UNIWERSYTET IM. ADAMA MICKIEWICZA W POZNANIU

WYDZIAŁ MATEMATYKI I INFORMATYKI

FUNCTIONES ET APPROXIMATIO
COMMENTARII MATHEMATICI

54.1 (2016)

WYDAWNICTWO NAUKOWE UAM

FUNCTIONES ET APPROXIMATIO
COMMENTARII MATHEMATICI

UNIWERSYTET IM. ADAMA MICKIEWICZA W POZNANIU
WYDZIAŁ MATEMATYKI I INFORMATYKI

FUNCTIONES ET APPROXIMATIO
COMMENTARII MATHEMATICI

54.1 (2016)

WYDAWNICTWO NAUKOWE

POZNAŃ 2016

Functiones et Approximatio
Commentarii Mathematici

Address: Faculty of Mathematics and Computer Science, Adam Mickiewicz University, ul. Umultowska 87, 61-614 Poznań, Poland.

CONTENTS

PART 1

Functiones et Approximatio
54.1 (2016), 7–17
doi: 10.7169/facm/2016.54.1.1

ON THE IWASAWA λ-INVARIANT OF THE CYCLOTOMIC $\mathbb{Z}_2$-EXTENSION OF $\mathbb{Q}(\sqrt{p})$, III

Takashi Fukuda, Keiichi Komatsu, Manabu Ozaki, Takae Tsuji

Abstract: In the preceding papers, two of authors developed criteria for Greenberg conjecture of the cyclotomic $\mathbb{Z}_2$-extension of $k = \mathbb{Q}(\sqrt{p})$ with prime number p. Criteria and numerical algorithm in [5], [3] and [6] enable us to show $\lambda_2(k) = 0$ for all p less than 10^5 except $p = 13841, 67073$. All the known criteria at present can not handle $p = 13841, 67073$. In this paper, we develop another criterion for $\lambda_2(k) = 0$ using cyclotomic units and Iwasawa polynomials, which is considered a slight modification of the method of Ichimura and Sumida. Our new criterion fits the numerical examination and quickly shows that $\lambda_2(\mathbb{Q}(\sqrt{p})) = 0$ for $p = 13841, 67073$. So we announce here that $\lambda_2(\mathbb{Q}(\sqrt{p})) = 0$ for all prime numbers p less that 10^5.

Keywords: Iwasawa invariant, cyclotomic unit, real quadratic field.

1. Introduction

Let $k = \mathbb{Q}(\sqrt{p})$ be a real quadratic field with prime number p and k_∞ the cyclotomic $\mathbb{Z}_2$-extension of k. It is very important to study Greenberg conjecture for k_∞/k, namely to consider whether the Iwasawa λ-invariant $\lambda_2(k) = \lambda(k_\infty/k)$ is zero or not. First approach on this problem was made by Ozaki and Taya [14] in which they proved that $\lambda_2(k) = 0$ if p satisfies $p \not\equiv 1 \pmod{16}$ or $2^{(p-1)/4} \not\equiv 1 \pmod{p}$. After Ozaki and Taya, the authors developed criteria for $\lambda_2(k) = 0$ when p satisfies $p \equiv 1 \pmod{16}$ and $2^{(p-1)/4} \equiv 1 \pmod{p}$ (cf. [5], [3], [6]). Our criteria are described by units in k_n, which is the intermediate field of k_∞/k with $[k_n : k] = 2^n$, and numerical calculations in k_n $(0 \leqslant n \leqslant 8)$ show that $\lambda_2(k) = 0$ for all prime number p less than 10^5 except $p = 13841, 67073$. All the known criteria accompanied with calculation in k_8 failed to show $\lambda_2(k) = 0$ for $p = 13841, 67073$. It seems necessary to calculate at least in k_{13} in order to show $\lambda_2(k) = 0$ using those criteria. Such a calculation is far beyond the ability of current computer.

2010 Mathematics Subject Classification: primary: 11R23; secondary: 11Y40

In this paper, we develop one more criterion using cyclotomic units, which is considered a slight modification of the method of Ichimura and Sumida [10], and verify that $\lambda_2(k) = 0$ for $p = 13841, 67073$ by using cyclotomic units and Iwasawa polynomials in k_8. Namely, we prove the following theorem:

Theorem 1.1. *We have $\lambda_2(\mathbb{Q}(\sqrt{p})) = 0$ for all prime number p less than 10^5.*

2. Preliminaries

From now on, we assume that p is a prime number satisfying $p \equiv 1 \pmod{16}$ and $2^{(p-1)/4} \equiv 1 \pmod{p}$. Let k_n be the n-th layer of the cyclotomic $\mathbb{Z}_2$-extension k_∞ of k as above, $\mathcal{O}_{k_n}$ the integer ring of k_n, $E_n = \mathcal{O}_{k_n}^\times$ the unit group of k_n, A_n the 2-part of the ideal class group of k_n, $\mathfrak{l}_n$ a prime ideal of k_n lying above 2. We put $\mathbb{B}_n = \mathbb{Q}(\cos\frac{2\pi}{2^{n+2}})$ and $\mathbb{B}_\infty = \cup_{n=0}^\infty \mathbb{B}_n$. Then $k_n = k\mathbb{B}_n$ and $k_\infty = k\mathbb{B}_\infty$. Moreover, let $\Delta = G(k_\infty/\mathbb{B}_\infty)$ the Galois group of k_∞ over $\mathbb{B}_\infty$ with a generator τ and $\Gamma = G(k_\infty/k)$ the Galois group of k_∞ over k with a topological generator γ.

Then we have $2\mathcal{O}_{k_n} = (\mathfrak{l}_n\mathfrak{l}_n^\tau)^{2^n}$. Let $k_{n\,\mathfrak{l}_n}$ be the completion of k_n at $\mathfrak{l}_n$ and put $c_n = 1 + 2\cos\frac{2\pi}{2^{n+2}}$. Then we have $k_{n\,\mathfrak{l}_n} = \mathbb{Q}_2(c_n)$, where $\mathbb{Q}_2$ is the 2-adic field. Let I'_n be the group of fractional ideals in k_n generated by ideals which are prime to 2. We put $E'_n = \{\, \alpha \in k_n \mid (\alpha) \in I'_n \,\}$ and $U_n = \mathcal{O}_{k_n\,\mathfrak{l}_n}^\times \times \mathcal{O}_{k_n\,\mathfrak{l}_n}^\times$.

We embed E'_n in U_n by the injective homomorphism $\varphi : E'_n \ni \alpha \mapsto (\alpha, \alpha^\tau) \in U_n$. We put $(\alpha,\alpha^\tau)^{\tau^*} = (\alpha^\tau, \alpha)$ for $(\alpha,\alpha^\tau) \in \varphi(E'_n)$. Since the topological closure $\overline{\varphi(E'_n)}$ of $\varphi(E'_n)$ is U_n, we can extend the mapping τ^* to U_n continuously.

Now we develop a quadratic version of [15, Theorem 3.3] by following the arguments in [9, §2]. We put $\mathbb{U} = \varprojlim U_n$, where the projective limit is taken with respect to the relative norms. Let $u = (u_n)_{n=1}^\infty$ be an element in $\varprojlim \mathcal{O}_{k_n\,\mathfrak{l}_n}^\times$. Then there exists a unique power series $f_u(X) \in \mathbb{Z}_2[[X]]$ satisfying

$$f_u(1 - \zeta_{2^{n+2}}) = u_n,$$

where ζ_m means $\exp(2\pi\sqrt{-1}/m)$. Let $D = (1-X)\frac{d}{dX}$ be a derivative operator on $\mathbb{Z}_2[[X]]$. We put $\Lambda = \mathbb{Z}_2[[T]]$ and let $1+T$ act on $\mathbb{U}$ as $\gamma \in \Gamma$. Let s be a primitive root modulo p and put $\xi = \sum_{i=1}^{(p-1)/2}(\zeta_p^{s^{2i}} - \zeta_p^{s^{2i+1}})$, which we regard as the image of the embedding $\mathcal{O}_k \hookrightarrow \mathcal{O}_{k_\mathfrak{l}} = \mathbb{Z}_2$. Then there exists a unique element $G_u(T)$ of Λ such that

$$D^\nu(\log f_u(X) - \tfrac{1}{2}\log f_u(1-(1-X)^2))|_{X=0} = G_u((1+4p)^\nu - 1)\xi.$$

We note that the correspondence $\mathbb{U}^{1-\tau^*} \ni (u, u^{-1}) \mapsto \frac{1}{2}G_u(T) \in \Lambda$ defines a Λ-isomorphism $\Psi : \mathbb{U}^{1-\tau^*} \longrightarrow \Lambda$. Now, we put

$$\eta_n = \zeta_{2^{n+2}}^{(p-1)/4} \prod_{i=1}^{(p-1)/2} \left(\zeta_{2^{n+2}}^{-1} - \zeta_p^{s^{2i}}\right),$$

and $\eta = (\eta_n)_{n=1}^\infty$. A straightforward calculation, which was presented in [6] for instance, shows that

$$\eta_n^2 = N_{\mathbb{Q}(\zeta_{2^{n+2}p})/k_n}\left(1 - \zeta_{2^{n+2}}\zeta_p\right).$$

From now on, we specify the topological generator γ of Γ by the relation

$$(\zeta_{2^{n+2}} + \zeta_{2^{n+2}}^{-1})^{\gamma} = \zeta_{2^{n+2}}^{1+4p} + \zeta_{2^{n+2}}^{-1-4p} \quad (n \geqslant 0)\,.$$

Then Iwasawa's construction of 2-adic L-function associated to k varies now into the following form.

Theorem 2.1. *Let χ be the non-trivial character modulo p associated to k and $\frac{1}{2}G(T)$ the image of the element $(\eta^{1-\tau}, \eta^{\tau-1})$ in $\mathbb{U}^{1-\tau^*}$ by the above isomorphism $\mathbb{U}^{1-\tau^*} \cong \Lambda$. Then we have*

$$G((1+4p)^{\nu} - 1) = -(1 - 2^{\nu-1})\frac{B_{\nu,\chi}}{\nu} \qquad \text{for } \ \nu \equiv 0 \pmod 2.$$

Here $B_{\nu,\chi}$ is a generalized Bernoulli number.

Since the Iwasawa μ-invariant $\mu_2(k) = \mu(k_\infty/k)$ is known to be zero by Ferrero-Washington [2], there exist a unique unit element $u(T) \in \Lambda^\times$ and a unique distinguished polynomial $g(T) \in \mathbb{Z}_2[[T]]$ such that

$$G(T) = 2u(T)g(T). \tag{2.1}$$

The distinguished polynomial $g(T)$, which is called Iwasawa polynomial, plays essential role in our arguments. We fix the notation $g(T)$ throughout the paper.

3. Criterion

In this section, we work in abelian extensions of $\mathbb{Q}$. So Leopoldt conjecture is valid in our situation (cf. [1]). Let L_∞ is the maximal unramified abelian 2-extension of k_∞ and M_∞ the maximal abelian 2-extension of k_∞ unramified outside 2. Then the Galois groups $I_\infty = G(M_\infty/L_\infty)$, $\mathfrak{X}_\infty = G(M_\infty/k_\infty)$ and $X_\infty = G(L_\infty/k_\infty)$ are finitely generated Λ-modules (cf. [12]). For a finitely generated Λ-module X, $\mathrm{ch}(X)$ denotes the characteristic polynomial of X. Then we have the following:

Lemma 3.1. *The tensor product $\mathfrak{X}_\infty \otimes_{\mathbb{Z}_2[\Delta]} \mathbb{Z}_2$ is pseudo-isomorphic to $\mathfrak{X}_\infty^{1-\tau}$, where τ acts on $\mathbb{Z}_2$ by $\tau a = -a$ for $a \in \mathbb{Z}_2$.*

Proof. Let ψ be a Δ-homomorphism of $\mathfrak{X}_\infty \otimes_{\mathbb{Z}_2[\Delta]} \mathbb{Z}_2$ to $\mathfrak{X}_\infty^{1-\tau}$ defined by $\psi(x \otimes a) = (x^a)^{1-\tau}$. Then ψ is surjective. Now, we assume $\psi(x \otimes a) = 1$. Then we have $(x^a)^{1-\tau} = 1$, which means $(x^a)^\tau = x^a$. Hence $x \otimes a = x^a \otimes 1 = (x^a)^\tau \otimes 1 = x^a \otimes (-1) = (x^a \otimes 1)^{-1}$, which shows $(x \otimes a)^2 = 1$. Since $\mathfrak{X}_\infty \otimes_{\mathbb{Z}_2[\Delta]} \mathbb{Z}_2$ is finitely generated $\mathbb{Z}_2$-module, the kernel of ψ is finite. ■

Hence we have the following (cf. [18, Theorem 6.2]):

Lemma 3.2. *We have $ch(\mathfrak{X}_\infty^{1-\tau}) = g(T)$.*

Moreover, we have the following:

Lemma 3.3. *Λ-modules $\mathfrak{X}_\infty^{1-\tau} \cap I_\infty$ and $I_\infty^{1-\tau}$ are pseudo-isomorphic. Namely, $ch(\mathfrak{X}_\infty^{1-\tau} \cap I_\infty) = ch(I_\infty^{1-\tau})$.*

Proof. Let x be an element in $\mathfrak{X}_\infty^{1-\tau} \cap I_\infty$. Since $x^\tau = x^{-1}$, we have $x^2 = x^{1-\tau}$, which means $x^2 \in I_\infty^{1-\tau}$. Since $I_\infty^{1-\tau} \subset \mathfrak{X}_\infty^{1-\tau} \cap I_\infty$ and since $\mathfrak{X}_\infty^{1-\tau} \cap I_\infty$ is a finitely generated $\mathbb{Z}_2$-module, the index $(\mathfrak{X}_\infty^{1-\tau} \cap I_\infty : I_\infty^{1-\tau})$ is finite. ■

Since $X_\infty^{1-\tau} = \mathfrak{X}_\infty^{1-\tau} I_\infty / I_\infty$ is isomorphic to $\mathfrak{X}_\infty^{1-\tau} / \mathfrak{X}_\infty^{1-\tau} \cap I_\infty$, we have the following:

Lemma 3.4. *We have*

$$g(T) = ch(X_\infty^{1-\tau}) ch(\mathfrak{X}_\infty^{1-\tau} \cap I_\infty).$$

Now, we put $E_n = \mathcal{O}_{k_n}^\times$. Then $\varphi(E_n) = \{ (\varepsilon, \varepsilon^\tau) \mid \varepsilon \in E_n \}$. Moreover, we put $\mathcal{E}_n = \overline{\varphi(E_n)} \subset U_n$ and $\mathcal{E} = \varprojlim \mathcal{E}_n$. Then I_∞ is isomorphic to $\mathbb{U}/\mathcal{E}$ by class field theory, which shows $I_\infty^{1-\tau}$ is isomorphic to $\mathbb{U}^{1-\tau}\mathcal{E}/\mathcal{E}$. Let $P(T)$ be a monic irreducible polynomial in Λ which divides $g(T)$ and put

$$Q(T) = \frac{g(T)}{P(T)}.$$

Assume that $P(T)$ divides $\mathrm{ch}(X_\infty^{1-\tau})$. Then $\mathrm{ch}(I_\infty^{1-\tau})$ divides $Q(T)$, which shows $(\mathbb{U}^{1-\tau})^{Q(T)} \subset \mathcal{E}$, because $\mathfrak{X}_\infty$ has no finite Λ-submodule (cf. [8, Theorem 1]). Since $P(T)$ and $\omega_n(T) = (1+T)^{2^n} - 1$ are mutually prime in Λ, which is a consequence of Leopoldt conjecture, there exist elements $q_n(T)$, $r_n(T) \in \Lambda$ with

$$P(T)q_n(T) + r_n(T)\omega_n(T) = 2^{a_n},$$

where a_n is a non-negative integer. Hence we have

$$(\eta_n^{1-\tau}, \eta_n^{\tau-1})^{q_n(T)} = \Psi^{-1}(u(T))^{P(T)Q(T)q_n(T)} \in \mathcal{E}_n^{2^{a_n}}$$

with $u(T)$ define by (2.1). Now we follow the arguments in [4] and [16] noting that Leopoldt conjecture is valid in our situation to establish the following theorem.

Theorem 3.5. *Assume that for any monic irreducible polynomial $P(T)$ dividing $g(T)$, there exists $n \geqslant 1$ which satisfies*

$$\eta_n^{(1-\tau)q(\gamma-1)} \notin E_n^{2^a}. \tag{3.1}$$

Here $q(T)$ is a polynomial in Λ and a is a non-negative integer satisfying

$$P(T)q(T) \equiv 2^a \pmod{\omega_n(T)}.$$

Then we have $\lambda_2(k) = 0$.

The condition (3.1) in Theorem 3.5 guarantees $P(T) \not| \mathrm{ch}(X_\infty^{1-\tau})$, from which we deduce $\lambda_2(k) = 0$. In the practical computations, we are often aware of an upper bound d of λ-invariant. If $P(T)$ satisfies $\deg P(T) > d$, then we immediately conclude $P(T) \not| \mathrm{ch}(X_\infty^{1-\tau})$ because $\deg \mathrm{ch}(X_\infty) \leqslant d$. Hence we are able to transform Theorem 3.5 to the following effective form.

Corollary 3.6. *Assume that $\lambda_2(k) \leqslant d$ with positive integer d. Moreover, assume that for any monic irreducible polynomial $P(T)$ dividing $g(T)$ which satisfies $\deg P(T) \leqslant d$, there exists $n \geqslant 1$ which satisfies*

$$\eta_n^{(1-\tau)q(\gamma-1)} \notin E_n^{2^a}. \tag{3.2}$$

Here $q(T)$ is a polynomial in Λ and a is a non-negative integer satisfying

$$P(T)q(T) \equiv 2^a \pmod{\omega_n(T)}. \tag{3.3}$$

Then we have $\lambda_2(k) = 0$.

We note here that we verify the condition (3.2) by a congruence relation. Namely, let α be an integer in k_n and ℓ a prime number which satisfies $\chi(\ell) = 1$, $\ell \equiv 1 \pmod{2^{n+2}}$ and $\ell \equiv 1 \pmod{2^a}$. Then ℓ splits completely in $k_n/\mathbb{Q}$ and we find $x = x_{\mathfrak{l}} \in \mathbb{Z}$ satisfying $\alpha \equiv x \pmod{\mathfrak{l}}$ for each prime ideal $\mathfrak{l}$ of k_n lying above ℓ. If we find ℓ and $\mathfrak{l}$ such that

$$x^{\frac{\ell-1}{2^a}} \not\equiv 1 \pmod{\ell},$$

then we see that

$$\alpha \notin k_n^{2^a}.$$

4. Bound of Iwasawa invariants

In this section, we discuss an upper bound of Iwasawa invariants in a general situation. Let F be a finite algebraic extension of $\mathbb{Q}$, ℓ a prime number and K a $\mathbb{Z}_\ell$-extension of F. Let F_n be the intermediate field of K/F with $[F_n : F] = \ell^n$ and denote by ℓ^{e_n} the ℓ-part of the class number of F_n. Then there exist integers $\lambda(K/F) \geqslant 0$, $\mu(K/F) \geqslant 0$ and $\nu(K/F)$ which satisfy

$$e_n = \lambda(K/F)n + \mu(K/F)\ell^n + \nu(K/F)$$

for all sufficiently large n (cf. [12]).

In some situations, a few practical values of e_n estimate explicitly upper bounds of $\lambda(K/F)$ and $\mu(K/F)$ and enables us to apply Corollary 3.6 to $k = \mathbb{Q}(\sqrt{p})$. A similar estimate is also given in [11, Lemma 5].

Theorem 4.1. *Notations being as above, assume that all the ramified primes in K/F are totally ramified. Furthermore we assume that inequality $e_{n+1} - e_n < \ell^{n+1} - \ell^n$ holds for some $n \geqslant 0$. Then we have $\lambda(K/F) \leqslant e_{n+1} - e_n$ and $\mu(K/F) = 0$.*

Proof. Let A_n be the ℓ-part of the ideal class group of F_n. Then $|A_n| = \ell^{e_n}$. Put $e_{n+1} - e_n = b$. Let $X = G(L_\infty/K)$ and $Y = G(L_\infty/KL_0) \subseteq X$, where L_∞ and L_0 are the maximal unramified abelian ℓ-extensions of K and F, respectively. Then $\Gamma = G(K/F)$ acts on X by inner automorphism. If we fix a topological generator γ of Γ and associate γ with $1 + T$, then we are able to regard X as a $\Lambda = \mathbb{Z}_\ell[[T]]$-module. We put

$$\nu_n = \frac{(1+T)^{\ell^n} - 1}{T}\ ,\ \nu_{n+1,n} = \nu_{n+1}/\nu_n.$$

Then we have the isomorphism

$$A_n \simeq X/\nu_n Y \tag{4.1}$$

from our assumption on the ramification in K/F and [12, Theorem 6]. It follows from (4.1) and our assumption on the class numbers that

$$|\nu_n Y/\nu_{n+1} Y| = \ell^b$$

Hence if we put $M = \nu_n Y$, then we have

$$|M/\nu_{n+1,n} M| = \ell^b. \tag{4.2}$$

Here we note that $\lambda(K/F) = \mathrm{rank}_{\mathbb{Z}_\ell} X = \mathrm{rank}_{\mathbb{Z}_\ell} M$ because $X/\nu_n Y \simeq A_n$ is finite. Also, the triviality of the μ-invariant of the Λ-module M implies that of $\mu(K/F)$ by the same reason. Therefore it is enough to show that $\dim_{\mathbb{F}_\ell} M/\ell M \leqslant b$, because $\mathrm{rank}_{\mathbb{Z}_\ell} M \leqslant \dim_{\mathbb{F}_\ell} M/\ell M$ holds in general and the finiteness of $M/\ell M$ implies the vanishing of the μ-invariant of M by Nakayama's lemma. Since $\mathbb{F}_\ell[[T]]$ is a discrete valuation ring and $M/\ell M$ is a finitely generated $\mathbb{F}_\ell[[T]]$-module, we have

$$M/\ell M \simeq \mathbb{F}_\ell[[T]]^{\oplus r} \oplus \left(\bigoplus_{i=1}^{s} \mathbb{F}_\ell[[T]]/(T^{a_i}) \right) \tag{4.3}$$

for some integers $r \geqslant 0$ and $a_1 \geqslant \ldots \geqslant a_s \geqslant 0$. Then we get

$$\begin{aligned} M/(\ell, \nu_{n+1,n})M &= M/(\ell, T^{\ell^{n+1}-\ell^n})M \\ &\simeq \left(\mathbb{F}_\ell[[T]]/(T^{\ell^{n+1}-\ell^n}) \right)^{\oplus r} \\ &\quad \oplus \left(\bigoplus_{i=1}^{s} \mathbb{F}_\ell[[T]]/(T^{\min\{a_i,\, \ell^{n+1}-\ell^n\}}) \right), \end{aligned} \tag{4.4}$$

because $\nu_{n+1,n} \equiv T^{\ell^{n+1}-\ell^n} \pmod{\ell}$. By using our assumption, (4.2) and (4.4), we derive

$$\begin{aligned} \ell^{n+1} - \ell^n > b &\geqslant \dim_{\mathbb{F}_\ell} (M/(\ell, \nu_{n+1,n})M) \\ &= r(\ell^{n+1} - \ell^n) + \sum_{i=1}^{s} \min\{a_i,\, \ell^{n+1} - \ell^n\}, \end{aligned} \tag{4.5}$$

from which we find immediately $r = 0$ and $a_i < \ell^{n+1} - \ell^n$ for all i. Therefore, we get inequality $\dim_{\mathbb{F}_\ell} M/\ell M = \sum_{i=1}^{s} a_i \leqslant b$ by (4.3) and (4.5), which implies the assertion of the theorem as mentioned above. ■

5. Calculation

In this section, we return to the case $\ell = 2$ and recall $\Lambda = \mathbb{Z}_2[[T]]$. Let $k = \mathbb{Q}(\sqrt{p}\,)$ with prime number p satisfying $p \equiv 1 \pmod{16}$ and $2^{(p-1)/4} \equiv 1 \pmod{p}$. Let k_n be the intermediate field of the cyclotomic $\mathbb{Z}_2$-extension of k with $[k_n : k] = 2^n$ and A_n the 2-part of the ideal class group of k_n. We put $|A_n| = 2^{e_n}$.

First of all, we explain how to compute e_n. Straightforward calculation using several software packages developed for number theory handles e_1, e_2 and e_3. But it fails to compute e_4 because the degree $[k_n : k] = 2^n$ increases rapidly. So a custom algorithm specialized to k is needed. Thanks to [6, Proposition 3.5], the integer a_r in the table in [3], which is expected to be equal to e_r, is now actually equal to e_r. Hence we can calculate e_n $(1 \leqslant n \leqslant 8)$ by using the method in [5].

Let χ be the character of k and ω the Teichmüller character modulo 4. Then $\chi^* = \omega\chi^{-1}$ is the character of $\mathbb{Q}(\sqrt{-p}\,)$. We define the integer s so that $p \equiv 1 \pmod{2^s}$ and $p \not\equiv 1 \pmod{2^{s+1}}$. Then the Stickelberger element ξ_n is defined by

$$\xi_n = \frac{1}{q_n} \sum_{\substack{a=1 \\ (a,q_n)=1}}^{q_n} a\chi^*(a)^{-1} \left(\frac{\mathbb{B}_n/\mathbb{Q}}{a}\right)^{-1} \in \mathbb{Z}_2[G(\mathbb{B}_n/\mathbb{Q})],$$

where $q_n = p2^{n+2}$ and $\left(\frac{\mathbb{B}_n/\mathbb{Q}}{a}\right)$ is the Artin symbol. It is known that $\frac{1}{2}\xi_n$ also has integral coefficients. So we associate $\left(\frac{\mathbb{B}_n/\mathbb{Q}}{1+q_0}\right)^{-1}$ with $\frac{1+T}{1+q_0}$ and construct the polynomial $G_n(T) \in \Lambda$ from $\frac{1}{2}\xi_n$. Weierstrass preparation theorem guarantees the decomposition

$$G_n(T) = u_n(T)g_n(T)$$

with the unit element $u_n(T) \in \Lambda$ and the distinguished polynomial $g_n(T) \in \Lambda$, where $g_n(T)$ is constructed explicitly by an algorithm in [17, Proposition 7.2]. Then we know the congruence relation

$$g(T) \equiv g_n(T) \pmod{2^{n-s+2}},$$

where $g(T)$ is the distinguished polynomial defined by (2.1).

Now we see

$$\begin{aligned}\frac{1}{2}\xi_n &= \frac{1}{2^{n+3}p}\sum_{\substack{a=1\\(a,2p)=1}}^{2^{n+2}p} a\chi^*(a)^{-1}\left(\frac{\mathbb{B}_n/\mathbb{Q}}{a}\right)^{-1}\\ &= \frac{1}{2^{n+3}p}\sum_{\substack{j=0\\(j,2)=1}}^{2^{n+2}-1}\sum_{i=0}^{p-1}(2^{n+2}i+j)\chi^*(2^{n+2}i+j)\left(\frac{\mathbb{B}_n/\mathbb{Q}}{2^{n+2}i+j}\right)^{-1}\\ &= \frac{1}{2p}\sum_{\substack{j=0\\(j,2)=1}}^{2^{n+2}-1}\left(\frac{\mathbb{B}_n/\mathbb{Q}}{j}\right)^{-1}\sum_{i=0}^{p-1} i\chi^*(2^{n+2}i+j)\\ &\quad+\frac{1}{2^{n+3}p}\sum_{j=0}^{2^{n+2}-1} j\left(\frac{\mathbb{B}_n/\mathbb{Q}}{j}\right)^{-1}\sum_{i=0}^{p-1}\chi^*(2^{n+2}i+j)\\ &= \frac{1}{2p}\sum_{\substack{j=0\\(j,2)=1}}^{2^{n+2}-1}\left(\frac{\mathbb{B}_n/\mathbb{Q}}{j}\right)^{-1}\sum_{i=0}^{p-1} i\chi^*(2^{n+2}i+j),\end{aligned}$$

because, for odd j, we have

$$\begin{aligned}\sum_{i=0}^{p-1}\chi^*(2^{n+2}i+j) &= \sum_{i=0}^{p-1}(-1)^{2^{n+1}i}(-1)^{\frac{j-1}{2}}\left(\frac{2^{n+2}i+j}{p}\right)\\ &= (-1)^{\frac{j-1}{2}}\sum_{a=0}^{p-1}\left(\frac{a}{p}\right)=0.\end{aligned}$$

Put $G=(\mathbb{Z}/2^{n+2}\mathbb{Z})^\times$ and $H=\langle\, 1+q_0+2^{n+2}\mathbb{Z}\,\rangle$. Then $G=H\cup(-H)$ and hence

$$\begin{aligned}G_n(T) = \frac{1}{2p}\sum_{j=0}^{2^n-1}\left(\frac{1+T}{1+q_0}\right)^j\sum_{i=0}^{p-1} i\Big\{&\chi^*(2^{n+2}i+((1+q_0)^j \bmod 2^{n+2}))\\ &+\chi^*(2^{n+2}i+(-(1+q_0)^j \bmod 2^{n+2}))\Big\},\end{aligned}$$

where $a \bmod 2^{n+2}$ means rational integer x satisfying

$$x\equiv a \pmod{2^{n+2}} \qquad \text{and} \qquad 0\leqslant x<2^{n+2}.$$

Now we show two examples, from which we derive Theorem 1.1. Let $p=13841$. Then $s=4$ and we see

$$\begin{aligned}g(T) &\equiv 44128+126772T+30644T^2+T^3 \pmod{2^{17}}\\ &\equiv (2616+T)(74772+28028T+T^2) \pmod{2^{17}} \qquad (5.1)\end{aligned}$$

from ξ_{19}. Proposition 2 in [13, Chapter II] with the fact $g_{19}(-2616) \equiv 0 \pmod{2^{17}}$, $g'_{19}(-2616) \not\equiv 0 \pmod{2^3}$ implies that $g(T)$ has a factor $P_1(T) = \alpha + T$ ($\alpha \in \mathbb{Z}_2$) with $\alpha \equiv 2616 \pmod{2^{13}}$ and (5.1) implies that $g(T)/P_1(T)$ is irreducible modulo 2^{13}. Hence $g(T)/P_1(T)$ is irreducible in Λ and we see

$$g(T) = P_1(T)P_2(T)$$

with irreducible polynomial $P_2(T)$ of degree two.

Now we get e_n as follows:

n	1	2	3	4	5	6	7	8
e_n	2	4	5	6	7	8	9	10

Hence it follows that $\lambda_2(k) \leqslant 1$ by Theorem 4.1 and it suffices to verify the condition (3.2) only for $P(T) = P_1(T)$ in order to prove $\lambda_2(k) = 0$. When $n = 10$, we see that $a = 13$ in the expression (3.3) and the condition (3.2) holds. Hence we have $\lambda_2(k) = 0$.

Next we treat $p = 67073$. In this case, $s = 9$. We calculate ξ_{28} and find that

$$g(T) = P_1(T)P_2(T)P_3(T),$$

where $P_1(T)$, $P_2(T)$ and $P_3(T)$ are monic irreducible polynomials with degree 1,2 and 124 respectively by factoring $g_{28}(T)$ modulo 2^{21} and using Hensel's lemma. We also see

$$\begin{aligned} P_1(T) &\equiv 1000 + T \pmod{2^{11}}, \\ P_2(T) &\equiv 1392 + 796T + T^2 \pmod{2^{11}}, \end{aligned}$$

and

n	1	2	3	4	5	6	7	8
e_n	3	6	9	12	14	16	18	20

Hence it follows that $\lambda_2(k) \leqslant 2$ by Theorem 4.1 and it suffices to verify the condition (3.2) only for $P(T) = P_1(T)$ and $P(T) = P_2(T)$ in order to prove $\lambda_2(k) = 0$. Actually we verify the condition (3.2) for $P_1(T)$ with $n = 8$ and for $P_2(T)$ with $n = 3$. So we conclude $\lambda_2(k) = 0$.

6. Comparison of criteria

We would like to compare criteria of $\lambda_2(k) = 0$. Most fundamental criterion is Theorem 2.1 in [3]. The condition (C) was first verified in our all practical calculations. Theorems 2.1 and 2.2 in [6] are considered the improvement of that in special situations. At the present time, we are abel to check these criteria in k_n ($1 \leqslant n \leqslant 8$). On the other hand, Corollary 3.6 is a criterion of different type. We are abel to check this criterion for larger n.

In the following table, we show n where we verified $\lambda_2(k) = 0$ under the calculations in k_n. The sign $\times$ means that the criterion can not be applied for such p. The inequality $\geqslant 13$ or $\geqslant 12$ means that we need at least $n = 13$ or $n = 12$ to apply [3, Theorem 2.1]. For p where the sign ? is marked, we failed to factorize Iwasawa polynomial $g(T)$ which has degree 2047, 1022 or 16383. So all the criteria should be considered complementary to each other.

p	[3, Theorem 2.1]	[6, Theorem 2.1]	[6, Theorem 2.2]	Corollary 3.6
1201	2	$\times$	$\times$	10
3361	5	$\times$	$\times$	3
12161	4	2	$\times$	11
13121	4	$\times$	2	6
13841	$\geqslant 13$	$\times$	$\times$	10
67073	$\geqslant 12$	$\times$	$\times$	8
14929	5	$\times$	4	2
15217	3	$\times$	$\times$	3
20353	1	$\times$	4	7
61297	8	$\times$	7	2
40961	1	2	$\times$	?
61441	2	$\times$	$\times$	?
65537	7	$\times$	$\times$	?

References

[1] A. Brumer, *On the units of algebraic number fields*, Mathematika **14** (1967), 121–124.

[2] B. Ferrero and L.C. Washington, *The Iwasawa invariant μ_p vanishes for abelian number fields*, Ann. of Math. **109** (1979), no. 2, 377–395.

[3] T. Fukuda, *Greenberg conjecture for the cyclotomic $\mathbb{Z}_2$-extension of $\mathbb{Q}(\sqrt{p}\,)$*, Interdisciplinary Information Sciences, **16-1** (2010), 21–32.

[4] T. Fukuda and K. Komatsu, *Ichimura-Sumida criterion for Iwasawa λ-invariants*, Proc. Japan Acad. Ser. A Math. Sci. **76** (2000), 111-115.

[5] T. Fukuda and K. Komatsu, *On the Iwasawa λ-invariant of the cyclotomic $\mathbb{Z}_2$-extension of $\mathbb{Q}(\sqrt{p}\,)$*, Math. Comp. **78** (2009), 1797–1808.

[6] T. Fukuda and K. Komatsu, *On the Iwasawa λ-invariant of the cyclotomic $\mathbb{Z}_2$-extension of $\mathbb{Q}(\sqrt{p}\,)$ II*, Funct. Approx. Comment. Math. **51** (2014), no. 1, 167–179.

[7] R. Greenberg, *On the Iwasawa invariants of totally real number fields*, Amer. J. Math. **98** (1976), 263–284.

[8] R. Greenberg, *On the structure of certain Galois groups*, Inv. math. **47** (1978), 85–99.

[9] C. Greither, *Class groups of abelian fields, and the main conjecture*, Ann. Inst. Fourier (Grenoble), **42**, (1992), 449-499.

[10] H. Ichimura and H. Sumida, *On the Iwasawa Invariants of certain real abelian fields II*, Inter. J. Math. **7** (1996), 721–744.

[11] H. Ichimura, S. Nakajima and H. Sumida-Takahashi, *On the Iwasawa lambda invariants of an imaginary abelian field of conductor* $3p^{n+1}$, J. Number Theory **133** (2013), 787–801.

[12] K. Iwasawa, *On* $\mathbb{Z}_\ell$*-extensions of algebraic number fields*, Ann. of Math. **98** (1973), 246–326.

[13] S. Lang, *Algebraic Number Theory*, Graduate Texts in Math. vol. 110, Springer, 1994.

[14] M. Ozaki and H. Taya, *On the Iwasawa* λ_2*-invariants of certain families of real quadratic fields*, Manuscripta Math. **94** (1997), no. 4, 437–444.

[15] T. Tsuji, *Semi-local units modulo cyclotomic units*, J. Number Theory **78** (1999), 1–26.

[16] T. Tsuji, *On the Iwasawa* λ*-invariants of real abelian fields*, Trans. Amer. Math. Soc. **355** (2003), 3699-3714.

[17] L.C. Washington, *Introduction to cyclotomic fields. Second edition*, Graduate Texts in Mathematics, 83, Springer-Verlag, New York, 1997.

[18] A. Wiles, *The Iwasawa conjecture for totally real fields*, Ann. Math. **131** (1990), 493–540.

Addresses: Takashi Fukuda: Department of Mathematics, College of Industrial Technology, Nihon University, 2-11-1 Shin-ei, Narashino, Chiba, Japan;
Keiichi Komatsu and Manabu Ozaki: Department of Mathematical Science, School of Science and Engineering, Waseda University, 3-4-1 Okubo, Shinjuku, Tokyo 169-8555, Japan;
Takae Tsuji: Department of Mathematics, Tokai University, 4-1-1 Kitakaname, Hiratsuka, Kanagawa, 259-1292, Japan.

E-mail: fukuda.takashi@nihon-u.ac.jp, kkomatsu@waseda.jp, ozaki@waseda.jp, tsuji@tokai-u.jp

Received: 7 November 2014; **revised:** 19 December 2015

Functiones et Approximatio
54.1 (2016), 19–23
doi: 10.7169/facm/2016.54.1.2

ON THE INVOLUTIONS OF THE RIORDAN GROUP

Masanari Kida

Abstract: We give an algebraic description of involutions in the Riordan group.
Keywords: Riordan group, involutions, eigenseries.

1. The Riordan group

Let F be a field of characteristic 0 and $F[[x]]$ the formal power series ring over F. The Riordan group is first introduced in [6]. We recall its definition. Let $N = F[[x]]^\times$ be the set of invertible formal power series over F. The set N forms a commutative group under multiplication. Also let $H = xF[[x]]^\times$ be the set of formal power series whose constant term is zero and whose coefficient of x is non-zero. The set H forms a non-commutative group under composition [1, Chapter 4 §4.7]. The identity element of H is x. The opposite group H^{op} of H acts on N from the left by substitution: namely, for $g(x) \in N$ and $f(x) \in H^{\mathrm{op}}$, we have

$$^{f}g(x) = g(f(x))$$

and if $f_1(x), f_2(x) \in H^{\mathrm{op}}$ and $\circ$ denotes the multiplication in H^{op}, then

$$^{f_1 \circ f_2}g(x) = g(f_2(f_1(x))).$$

By this action, we glue N and H^{op} together and form a left semi-direct product

$$\mathscr{R} = N \rtimes H^{\mathrm{op}}.$$

The group $\mathscr{R}$ is called the Riordan group and the multiplication of $(g_1(x), f_1(x))$, $(g_2(x), f_2(x)) \in \mathscr{R}$ is given by

$$\begin{aligned}(g_1(x), f_1(x))(g_2(x), f_2(x)) &= (g_1(x)\ {}^{f_1}g_2(x), f_2(f_1(x))) \\ &= (g_1(x)g_2(f_1(x)), f_2(f_1(x))).\end{aligned}$$

2010 Mathematics Subject Classification: primary: 05A15; secondary: 05A19, 05E18, 11B99

The identity element of $\mathscr{R}$ is $(1, x)$. The inverse of $(g_1(x), f_1(x)) \in \mathscr{R}$ is $\left(\frac{1}{g_1(\bar{f}_1(x))}, \bar{f}_1(x)\right)$, where $\bar{f}_1(x)$ is the compositional inverse of $f_1(x)$ in H^{op}, namely a power series satisfying $f_1(\bar{f}_1(x)) = \bar{f}_1(f_1(x)) = x$.

Although the Riordan group is usually defined by means of certain infinite matrices, we do not need such a description.

Recently the Riordan group has been used to obtain sequence identities. For example, in [7] the authors rewrote a combinatorially interesting element $(g, f) \in \mathscr{R}$ by a product of two elements to obtain sequence identities.

In this paper, we are interested in the action of $\mathscr{R}$ on $F[[x]]$. Let $G(x) \in F[[x]]$ be a formal power series and $(g(x), f(x)) \in \mathscr{R}$. We define

$$(g(x), f(x))G(x) = g(x)G(f(x)).$$

Hence elements of order 2 in the group $\mathscr{R}$ acts as involutions on $F[[x]]$. We call such an element of order 2 simply an involution in $\mathscr{R}$.

In his paper [5], Shapiro raised some problems on the involutions in $\mathscr{R}$, which can be stated in our notation as follows.

Problem 1.1. Is every involution a conjugate to $(1, -x)$?

Problem 1.2. Let $(f(x), g(x)) \in \mathscr{R}$ be an involution. Is there a simple condition for $g(x)$ in terms of $f(x)$?

These problems are solved by Cheon and Kim [2] in the category of analytic functions. In fact, they used a result on nonlinear functional equations. The aim of this paper is to give formal algebraic solutions to these problems (Propositions in the next section). The result and its proof are even simpler than Cheon and Kim's.

2. Involutions in the Riordan group

Let $\mathscr{R} = N \rtimes H = F[[x]]^{\times} \rtimes xF[[x]]^{\times}$ be the Riordan group as defined in the first section.

An easy computation shows that an element $(g(x), f(x)) \in \mathscr{R}$ has order 2 if and only if the following two identities hold:

$$f(f(x)) = x, \tag{2.1}$$

$$g(x)g(x)^f = 1. \tag{2.2}$$

The following description of $f(x)$ satisfying (2.1) is due to O'Farrell.

Lemma 2.1 ([4, Lemma 22]). *Let $f(x) \in H$. Suppose that $f(x) \neq x$. If $f(f(x)) = x$, then $f(x)$ is conjugate to $-x$ in H.*

Next we consider (2.2). Let $F((x))$ be the field of formal Laurent power series, which is a quotient field of $F[[x]]$ (see [1, Chapter 4 §4.9]).

The following proposition gives an answer to Problem 1.2.

Proposition 2.2. *Suppose that $f(x) \in H$ satisfies $f(f(x)) = x$ and $f(x) \neq x$. Then $g(x) \in N$ satisfies (2.2) if and only if there exists a non-zero formal Laurent power series $w(x) \in F((x))$ such that $g(x) = w(x)/w(f(x))$.*

Proof. First of all, note that the group H acts also on $F((x))^\times$ by substitution. Moreover an element of H defines an automorphism of the field $F((x))$. Hence, if $f(x) \in H$, then by Galois theory $F((x))$ is a quadratic extension over the fixed field $F((x))^{\langle f \rangle}$. An element $g(x)$ satisfying (2.2) is nothing but an element whose norm is 1 in the field extension $F((x))/F((x))^{\langle f \rangle}$. By Hilbert's theorem [1, Chapter 5 §11 Theorem 3], we have $g(x) = w(x)/w(x)^f$ for some $w(x) \in F((x))^\times$. The converse is obvious. ■

It is easy to see that two $w(x), w'(x) \in F((x))^\times$ give the same $g(x)$ if and only if they differ by an element in $F((x))^{\langle f \rangle}$. Hence there are infinitely possible $g(x)$ for a given $f(x)$.

The following proposition answers to Problem 1.1.

Proposition 2.3. *Assume that $f(x) \neq x$. An element $(g(x), f(x)) \in \mathscr{R}$ has order 2 if and only if it is conjugate to $(1, -x)$ in $\mathscr{R}$.*

Proof. Suppose that $(g(x), f(x)) \in \mathscr{R}$ has order 2. By Lemma 2.1, there exists $u(x) \in H = xF[[x]]^\times$ such that $f(x) = \bar{u}(-u(x))$. Also by Proposition 2.2, $g(x)$ can be written as $g(x) = w(x)/w(f(x))$ with some $w(x) \in F((x))^\times$. Consider an element

$$a = \left(\frac{1}{w(\bar{u}(x))}, \bar{u}(x) \right).$$

Then we have $a^{-1} = (w(x), u(x))$ and

$$\begin{aligned} a^{-1}(1, -x)a &= (w(x), -u(x)) \left(\frac{1}{w(\bar{u}(x))}, \bar{u}(x) \right) \\ &= (w(x)/w(f(x)), f(x)) \\ &= (g(x), f(x)) \end{aligned}$$

as desired. The converse is obvious. ■

Example 2.4. In our previous paper [3], by an analogy of modular form, we define an action of a lower triangular matrix

$$A_c = \begin{bmatrix} -1 & 0 \\ c & 1 \end{bmatrix} \in \mathrm{GL}_2(F)$$

on $G(x) \in F[[x]]$ of weight $k \in \mathbb{Z}$ by

$$G|_{[A]_k}(x) = (cx + 1)^{-k} G\left(\frac{-x}{cx + 1} \right). \tag{2.3}$$

This action can be interpreted in terms of involutions in $\mathscr{R}$. In fact, we have

$$[A_c]_k = \left(\frac{1}{(1+cx)^k}, \frac{-x}{1+cx} \right) \in \mathscr{R}.$$

For this $[A_c]_k$, we may take $u(x) = \frac{2x}{2+cx}$ and $w(x) = \left(1 + \frac{c}{2}x\right)^k$. There are many other choices.

Let $(g(x), f(x))$ be an involution in $\mathscr{R}$. A formal power series $G(x)$ is called an *eigenseries* of $(g(x), f(x))$ if it satisfies

$$(g(x), f(x))G(x) = \pm G(x).$$

The explicit description of involutions given in Proposition 2.3 enables us to prove an interesting result: any power series is an eigenseries of infinitely many involutions in $\mathscr{R}$.

Proposition 2.5. *Let $G(x)$ be any formal power series in $F[[x]]$. For any element $f(x) \in H$ of order 2 in H, there exist infinitely many $g(x) \in N$ such that $g(x)g(f(x)) = 1$ and that $G(x)$ is an eigenseries of involutions $(g(x), f(x)) \in \mathscr{R}$.*

Proof. By Lemma 2.1 we can write $f(x) = \bar{u}(-u(x))$ using some $u(x) \in H$. Let $e^+(x)$ (resp. $e^-(x)$) be any even (resp. odd) formal power series. We consecutively define

$$v(x) = e^{\pm}(u(x)), \qquad w(x) = G(x)/v(x), \qquad g(x) = w(x)/w(f(x)).$$

Then $g(x)$ clearly satisfies $g(x)g(f(x)) = 1$ and it is obvious that there are infinitely many such $g(x)$. Moreover we have

$$\begin{aligned} g(x)G(f(x)) &= \frac{w(x)}{w(f(x))} w(f(x))v(f(x)) \\ &= w(x)e^{\pm}(u(\bar{u}(-u(x)))) \\ &= w(x)e^{\pm}(-u(x)) \\ &= \pm w(x)e^{\pm}(u(x)) \\ &= \pm w(x)v(x) \\ &= \pm G(x). \end{aligned}$$

This completes the proof. ∎

In [3] we used the involutions $[A_c]_k$ to produce identities involving their eigenseries. These involutions have very rich eigenseries such as the generating functions of Bernoulli numbers, Fibonacci numbers, certain orthogonal polynomials and so on. While the above proposition indicates a possibility of extending our results in [3] to any series (or sequences), finding good simple involutions $(g(x), f(x)) \in \mathscr{R}$ seems to be inevitable to have a good theory. Our involutions $[A_c]_k$ in Example 2.4 are surely of this kind.

References

[1] N. Bourbaki, *Algebra II. Chapters 4–7*, Elements of Mathematics (Berlin), Springer-Verlag, Berlin, 2003, Translated from the 1981 French edition by P.M. Cohn and J. Howie.

[2] G.-S. Cheon and H. Kim, *Simple proofs of open problems about the structure of involutions in the Riordan group*, Linear Algebra Appl. **428** (2008), no. 4, 930–940.

[3] M. Kida and Y. Urata, *Involutions on generating functions*, J. of Integer Seq. **16** (2013), no. 1, Article 13.1.6.

[4] A.G. O'Farrell, *Composition of involutive power series, and reversible series*, Comput. Methods Funct. Theory **8** (2008), no. 1-2, 173–193.

[5] L. Shapiro, *Some open questions about random walks, involutions, limiting distributions, and generating functions*, Adv. in Appl. Math. **27** (2001), no. 2-3, 585–596, Special issue in honor of Dominique Foata's 65th birthday (Philadelphia, PA, 2000).

[6] L.W. Shapiro, S. Getu, W.J. Woan, and L.C. Woodson, *The Riordan group*, Discrete Appl. Math. **34** (1991), no. 1-3, 229–239, Combinatorics and theoretical computer science (Washington, DC, 1989).

[7] W. Wang and T. Wang, *Identities via Bell matrix and Fibonacci matrix*, Discrete Appl. Math. **156** (2008), no. 14, 2793–2803.

Address: Masanari Kida: Department of Mathematics, Tokyo University of Science, 1-3 Kagurazaka Shinjuku Tokyo 162-8601 Japan.

E-mail: kida@rs.tus.ac.jp

Received: 6 February 2015; **revised:** 21 October 2015

Functiones et Approximatio
54.1 (2016), 25–37
doi: 10.7169/facm/2016.54.2.3

SOME RESULTS ON EULER SUMS

Ce Xu, Jinfa Cheng

Abstract: In the paper, we develop an approach to evaluation of Euler sums that involve harmonic numbers and alternating harmonic numbers. We give explicit formulae for several classes of Euler sums in terms of Riemann zeta values and prove that the quadratic sums $S_{l^2,l}$ and cubic sums $S_{l^3,l}$ reduce to linear sums and polynomials in zeta values. The approach is based on constructive Power series and Cauchy product computations.

Keywords: Euler sums, Riemann zeta function, Cauchy product, power series.

1. Introduction

Harmonic numbers, alternating harmonic numbers and their generalizations are classically defined by

$$H_n=\sum_{j=1}^{n}\frac{1}{j},\qquad \zeta_n(k)=\sum_{j=1}^{n}\frac{1}{j^k},\qquad L_n(k)=\sum_{j=1}^{n}\frac{(-1)^{j-1}}{j^k}. \tag{1.1}$$

The subject of this paper is Euler sums, which are the infinite sums whose general term is a product of harmonic numbers and alternating harmonic numbers of index n and a power of n^{-1}. So, we consider the Euler sums of the form

$$\sum_{n=1}^{\infty}\frac{\prod\limits_{i=1}^{m_1}\zeta_n^{q_i}(k_i)\prod\limits_{j=1}^{m_2}L_n^{l_j}(h_j)}{n^p},\qquad \sum_{n=1}^{\infty}\frac{\prod\limits_{i=1}^{m_1}\zeta_n^{q_i}(k_i)\prod\limits_{j=1}^{m_2}L_n^{l_j}(h_j)(-1)^{n-1}}{n^p}, \tag{1.2}$$

where $m_1, m_2, q_i, k_i, h_j, l_j, p$ $(p\geqslant 2)$ are positive integer. If $\sum\limits_{i=1}^{m_1}(k_iq_i)+\sum\limits_{j=1}^{m_2}(h_jl_j)+p=C$ (C is a positive integer), then we call it C-order Euler sums. Apart from the actual evaluation of the series, one of the main questions that one sets out to

Supported by Nature Science Fund of Fujian Province (grant no. 2011J01021) and Fundamental Research Funds for the Central Universities (grant no. 20720150006)

2010 Mathematics Subject Classification: primary: 11L99; secondary: 11M06

solve is whether or not a given series can be expressed in terms of a linear rational combination of known constants. When this is the case, we say that the series is reducible to these values. It has been discovered in the course of the years that many Euler sums admit expressions involving finitely the zeta values, that is to say value of the Riemann zeta function,

$$\zeta(s)=\sum_{n=1}^{\infty}\frac{1}{n^s},\qquad Re(s)>1$$

with the positive integers.

For a pair (p,q) of positive integers with $p\geqslant 2$, the classical linear Euler sum is defined by

$$S_{p,q}=\sum_{n=1}^{\infty}\frac{1}{n^p}\sum_{k=1}^{n}\frac{1}{k^q}. \tag{1.3}$$

In 1742, Goldbach proposed to Euler the problem of expressing the $S_{p,q}$ in terms of values at positive integers of the Riemann zeta function $\zeta(s)$. Euler showed this problem in the case $p=1$ and gave a general formula for odd weight $p+q$ without any proof in 1775.

Let $\pi=(\pi_1,\ldots,\pi_k)$ be a partition of integer p into k summands, so that $p=\pi_1+\cdots+\pi_k$ and $\pi_1\leqslant\pi_2\leqslant\cdots\leqslant\pi_k$. The classical nonlinear Euler sum of index π,q is defined by (see [5])

$$S_{\pi,q}=\sum_{n=1}^{\infty}\frac{\zeta_n(\pi_1)\,\zeta_n(\pi_2)\cdots\zeta_n(\pi_k)}{n^q},$$

the quantity $\pi_1+\cdots+\pi_k+q$ being called the weight and the quantity k being the degree. As usual, repeated summands in partitions are indicated by powers, so that for instance

$$S_{1^2 2^3 4,q}=S_{112224,q}=\sum_{n=1}^{\infty}\frac{H_n^2\zeta_n^3(2)\,\zeta_n(4)}{n^q}.$$

The relationship between the values of the Riemann zeta function and Euler sums has been studied by many authors, for example see [1-5,7]. Philippe Flajolet and Bruno Salvy (see[5]) made use of contour integral to obtain some representation of $\sum\limits_{n=1}^{\infty}\frac{\zeta_n(q)}{n^p}$, $\sum\limits_{n=1}^{\infty}\frac{H_n^q}{n^p}$ by Riemann zeta function. In [1], David H. Bailey, Jonathan M. Borwein and Roland Girgensohn considered sums of the form $\sum\limits_{n=1}^{\infty}\frac{L_n^q(1)}{n^p}$, $\sum\limits_{n=1}^{\infty}\frac{L_n^q(1)}{n^p}(-1)^{n-1}$, where p and q are positive integers. In [7], Ping SUN made use of probabilistic and combinatiorial methods to obtain some representation of sums of the form $\sum\limits_{n=1}^{\infty}\frac{\prod\limits_{i=1}^{m_1}\zeta_n^{q_i}(k_i)}{n^p}$ by Riemann zeta function. But so far, no one has solved the following Euler sums,

$$\sum_{n=1}^{\infty}\frac{\zeta_n^2(3)}{n^3},\sum_{n=1}^{\infty}\frac{L_n(1)\,L_n(3)}{n+1}(-1)^{n-1},\sum_{n=1}^{\infty}\frac{L_n(1)\,\zeta_n(3)}{n+1}(-1)^{n-1}. \tag{1.4}$$

This paper develops an approach to the evaluation of Euler sums. The main purpose of this paper is to evaluation of some quadratic Euler sums that involve harmonic numbers and alternating harmonic numbers. We give explicit formulae for several classes of Euler sums in terms of Riemann zeta values and analytic value of (1.4) and establish the following important equations. For an integer $l \geqslant 2$, we have

$$S_{l^2,l} = \sum_{n=1}^{\infty} \frac{\zeta_n^2(l)}{n^l} = \sum_{n=1}^{\infty} \frac{\zeta_n(l)}{n^{2l}} + \frac{1}{3}\left(\zeta^3(l) - \zeta(3l)\right), \tag{1.5}$$

$$\sum_{n=1}^{\infty} \frac{L_n^2(l)(-1)^{n-1}}{n^l} = \sum_{n=1}^{\infty} \frac{L_n(l)}{n^{2l}} + \frac{1}{3}\left(L^3(l) - L(3l)\right), \tag{1.6}$$

where $\zeta(s) = \sum\limits_{n=1}^{\infty} \frac{1}{n^s}, L(s) = \sum\limits_{n=1}^{\infty} \frac{(-1)^{n-1}}{n^s}$. and we prove that the cubic sums $S_{l^3,l}$ reduce to linear sums and polynomials in zeta values.

From (1.5) we know that the quadratic sums $S_{l^2,l}$ reduce to linear sums and polynomials in zeta values. A general class of quadratic sums $S_{p_1p_2,q}$ $(1 < p_1, p_2, q \in Z)$ was studied by Flajolet and Salvy [5]. $S_{p_1p_2,q}\,(1 < p_1, p_2, q \in Z)$ are reducible to linear sums, but p_1, p_2, q should satisfy the condition $p_1 + p_2 + q$ is even.

2. Main theorems and the proof

Theorem 2.1. *For $l_1, l_2, m_1, m_2 \geqslant 2$ and $l_1, l_2, m_1, m_2 \in Z^+$, we have*

$$\begin{aligned}
\zeta^{m_1}(l_1)\zeta^{m_2}(l_2) = \sum_{k=1}^{\infty} \Bigg\{ & \sum_{j_1=1}^{m_1-1} \binom{m_1}{j_1} \frac{\zeta_k^{j_1}(l_1)}{(k+1)^{l_2m_2+(m_1-j_1)l_1}} \\
& + \sum_{j_2=1}^{m_2-1} \binom{m_2}{j_2} \frac{\zeta_k^{j_2}(l_2)}{(k+1)^{l_1m_1+(m_2-j_2)l_2}} \Bigg\} \\
& + \sum_{k=1}^{\infty} \left\{ \frac{\zeta_k^{m_2}(l_2)}{(k+1)^{m_1l_1}} + \frac{\zeta_k^{m_1}(l_1)}{(k+1)^{m_2l_2}} \right\} + \zeta(m_1l_1 + m_2l_2) \\
& + \sum_{k=1}^{\infty} \sum_{j_1=1}^{m_1-1} \sum_{j_2=1}^{m_2-1} \binom{m_1}{j_1} \binom{m_2}{j_2} \frac{\zeta_k^{j_1}(l_1)\zeta_k^{j_2}(l_2)}{(k+1)^{(m_1-j_1)l_1+(m_2-j_2)l_2}} \\
& + \sum_{k=1}^{\infty} \Bigg\{ \sum_{j_1=1}^{m_1-1} \binom{m_1}{j_1} \frac{\zeta_k^{j_1}(l_1)\zeta_k^{m_2}(l_2)}{(k+1)^{(m_1-j_1)l_1}} \\
& + \sum_{j_2=1}^{m_2-1} \binom{m_2}{j_2} \frac{\zeta_k^{j_2}(l_2)\zeta_k^{m_1}(l_1)}{(k+1)^{(m_2-j_2)l_2}} \Bigg\}.
\end{aligned} \tag{2.1}$$

Proof. First, constructing function $y=\sum\limits_{n=1}^{\infty}\zeta_n^{m_1}(l_1)\zeta_n^{m_2}(l_2)\,x^n\ (|x|<1)$. Using the definition of the harmonic numbers $\zeta_n(k)$ (1.1) we have

$$y=x+\sum_{n=1}^{\infty}\left(\zeta_n(l_1)+\frac{1}{(n+1)^{l_1}}\right)^{m_1}\left(\zeta_n(l_2)+\frac{1}{(n+1)^{l_2}}\right)^{m_2}x^{n+1}.$$

Using the Newton binomial expansion, we get

$$\begin{aligned}y=xy&+\sum_{n=1}^{\infty}\frac{x^n}{n^{l_1m_1+l_2m_2}}+\sum_{n=1}^{\infty}\left\{\frac{\zeta_n^{m_2}(l_2)}{(n+1)^{m_1l_1}}+\frac{\zeta_n^{m_1}(l_1)}{(n+1)^{m_2l_2}}\right\}x^{n+1}\\&+\sum_{n=1}^{\infty}\left\{\sum_{j_1=1}^{m_1-1}\binom{m_1}{j_1}\frac{\zeta_n^{j_1}(l_1)}{(n+1)^{l_2m_2+(m_1-j_1)l_1}}\right.\\&\left.+\sum_{j_2=1}^{m_2-1}\binom{m_2}{j_2}\frac{\zeta_n^{j_2}(l_2)}{(n+1)^{l_1m_1+(m_2-j_2)l_2}}\right\}x^{n+1}\\&+\sum_{n=1}^{\infty}\sum_{j_1=1}^{m_1-1}\sum_{j_2=1}^{m_2-1}\binom{m_1}{j_1}\binom{m_2}{j_2}\frac{\zeta_n^{j_1}(l_1)\,\zeta_n^{j_2}(l_2)}{(n+1)^{(m_1-j_1)l_1+(m_2-j_2)l_2}}x^{n+1}\\&+\sum_{n=1}^{\infty}\left\{\sum_{j_1=1}^{m_1-1}\binom{m_1}{j_1}\frac{\zeta_n^{j_1}(l_1)\,\zeta_n^{m_2}(l_2)}{(n+1)^{(m_1-j_1)l_1}}+\sum_{j_2=1}^{m_2-1}\binom{m_2}{j_2}\frac{\zeta_n^{j_2}(l_2)\,\zeta_n^{m_1}(l_1)}{(n+1)^{(m_2-j_2)l_2}}\right\}x^{n+1}.\end{aligned}$$

First, Move xy from the right to the left, then multiply both sides by $(1-x)^{-1}$. Using formula $(1-x)^{-1}=\sum\limits_{n=1}^{\infty}x^{n-1},\ x\in(-1,1)$ and Cauchy product formula, then equate the coefficient of x^{n+1} on both sides, we get

$$\begin{aligned}\zeta_{n+1}^{m_1}(l_1)\,\zeta_{n+1}^{m_2}(l_2)=&\sum_{k=1}^{n}\left\{\sum_{j_1=1}^{m_1-1}\binom{m_1}{j_1}\frac{\zeta_k^{j_1}(l_1)}{(k+1)^{l_2m_2+(m_1-j_1)l_1}}\right.\\&\left.+\sum_{j_2=1}^{m_2-1}\binom{m_2}{j_2}\frac{\zeta_k^{j_2}(l_2)}{(k+1)^{l_1m_1+(m_2-j_2)l_2}}\right\}\\&+\sum_{k=1}^{n}\left\{\frac{\zeta_k^{m_2}(l_2)}{(k+1)^{m_1l_1}}+\frac{\zeta_k^{m_1}(l_1)}{(k+1)^{m_2l_2}}\right\}+\zeta_{n+1}(m_1l_1+m_2l_2)\\&+\sum_{k=1}^{n}\sum_{j_1=1}^{m_1-1}\sum_{j_2=1}^{m_2-1}\binom{m_1}{j_1}\binom{m_2}{j_2}\frac{\zeta_k^{j_1}(l_1)\,\zeta_k^{j_2}(l_2)}{(k+1)^{(m_1-j_1)l_1+(m_2-j_2)l_2}}\\&+\sum_{k=1}^{n}\left\{\sum_{j_1=1}^{m_1-1}\binom{m_1}{j_1}\frac{\zeta_k^{j_1}(l_1)\,\zeta_k^{m_2}(l_2)}{(k+1)^{(m_1-j_1)l_1}}+\sum_{j_2=1}^{m_2-1}\binom{m_2}{j_2}\frac{\zeta_k^{j_2}(l_2)\,\zeta_k^{m_1}(l_1)}{(k+1)^{(m_2-j_2)l_2}}\right\}.\end{aligned}$$

Letting $n\to\infty$ gives (2.1). ■

Theorem 2.2. *For $l_1, l_2, m_2 \geqslant 2$ and $l_1, l_2, m_2 \in Z^+$, we have*

$$\begin{aligned}\zeta(l_1)\zeta^{m_2}(l_2) &= \sum_{k=1}^{\infty}\sum_{j_2=1}^{m_2-1}\binom{m_2}{j_2}\frac{\zeta_k^{j_2}(l_2)\,\zeta_k(l_1)}{(k+1)^{(m_2-j_2)l_2}} \\ &+ \sum_{k=1}^{\infty}\sum_{j_2=1}^{m_2-1}\binom{m_2}{j_2}\frac{\zeta_k^{j_2}(l_2)}{(k+1)^{(m_2-j_2)l_2+l_1}} \\ &+ \sum_{k=1}^{\infty}\frac{\zeta_k^{m_2}(l_2)}{(k+1)^{l_1}} + \zeta(l_1+m_2l_2) + \sum_{k=1}^{\infty}\frac{\zeta_k(l_1)}{(k+1)^{m_2l_2}}. \qquad (2.2)\end{aligned}$$

Proof. Similarly to Theorem 2.1, constructing function $y = \sum\limits_{n=1}^{\infty}\zeta_n(l_1)\zeta_n^{m_2}(l_2)\,x^n$ ($|x|<1$), we deduce that Theorem 2.2. ■

Theorem 2.3. *For $l_1, l_2, m_1, m_2 \geqslant 2$ with $l_1, l_2, m_1, m_2 \in Z^+$ and $|x| \leqslant 1$, we get*

$$\begin{aligned}\zeta_{n+1}^{m_1}(l_1,x)\,\zeta_{n+1}^{m_2}(l_2,x) &= \sum_{k=1}^{n}\frac{\zeta_k^{m_1}(l_1,x)\,x^{km_2}}{(k+1)^{m_2l_2}} \\ &+ \sum_{k=1}^{n}\sum_{j_2=1}^{m_2-1}\binom{m_2}{j_2}\frac{\zeta_k^{m_1}(l_1,x)\,\zeta_k^{j_2}(l_2,x)\,x^{k(m_2-j_2)}}{(k+1)^{(m_2-j_2)l_2}} \\ &+ \sum_{k=1}^{n}\frac{\zeta_k^{m_2}(l_2,x)\,x^{km_1}}{(k+1)^{m_1l_1}} + \sum_{k=1}^{n}\sum_{j_2=1}^{m_2-1}\binom{m_2}{j_2}\frac{\zeta_k^{j_2}(l_2,x)\,x^{k(m_1+m_2-j_2)}}{(k+1)^{m_1l_1+(m_2-j_2)l_2}} \\ &+ \sum_{k=1}^{n}\sum_{j_1=1}^{m_1-1}\binom{m_1}{j_1}\frac{\zeta_k^{m_2}(l_2,x)\,\zeta_k^{j_1}(l_1,x)\,x^{k(m_1-j_1)}}{(k+1)^{(m_1-j_1)l_1}} + \sum_{k=0}^{n}\frac{x^{k(m_1+m_2)}}{(k+1)^{m_1l_1+m_2l_2}} \\ &+ \sum_{k=1}^{n}\sum_{j_1=1}^{m_1-1}\sum_{j_2=1}^{m_2-1}\binom{m_1}{j_1}\binom{m_2}{j_2}\frac{\zeta_k^{j_1}(l_1,x)\,\zeta_k^{j_2}(l_2,x)\,x^{k(m_1+m_2-j_1-j_2)}}{(k+1)^{(m_1-j_1)l_1+(m_2-j_2)l_2}} \\ &+ \sum_{k=1}^{n}\sum_{j_1=1}^{m_1-1}\binom{m_1}{j_1}\frac{\zeta_k^{j_1}(l_1,x)\,x^{k(m_1+m_2-j_1)}}{(k+1)^{m_2l_2+(m_1-j_1)l_1}}. \qquad (2.3)\end{aligned}$$

If $m_1 = 1, m_2 \geqslant 2$, we obtain

$$\begin{aligned}\zeta_{n+1}(l_1,x)\,\zeta_{n+1}^{m_2}(l_2,x) &= \sum_{k=1}^{n}\frac{\zeta_k(l_1,x)\,x^{km_2}}{(k+1)^{m_2l_2}} \qquad (2.4) \\ &+ \sum_{k=1}^{n}\sum_{j_2=1}^{m_2-1}\binom{m_2}{j_2}\frac{\zeta_k(l_1,x)\,\zeta_k^{j_2}(l_2,x)\,x^{k(m_2-j_2)}}{(k+1)^{(m_2-j_2)l_2}} + \sum_{k=1}^{n}\frac{\zeta_k^{m_2}(l_2,x)\,x^{k}}{(k+1)^{l_1}} \\ &+ \sum_{k=1}^{n}\sum_{j_2=1}^{m_2-1}\binom{m_2}{j_2}\frac{\zeta_k^{j_2}(l_2,x)\,x^{k(1+m_2-j_2)}}{(k+1)^{l_1+(m_2-j_2)l_2}} + \sum_{k=0}^{n}\frac{x^{k(1+m_2)}}{(k+1)^{l_1+m_2l_2}}.\end{aligned}$$

where $\zeta_n(l_1,x) = 1 + \frac{x}{2^{l_1}} + \cdots + \frac{x^{n-1}}{n^{l_1}}, \zeta_n(l_2,x) = 1 + \frac{x}{2^{l_2}} + \cdots + \frac{x^{n-1}}{n^{l_2}}$.

Proof. Similarly to Theorem 2.1 and 2.2, constructing function

$$z=\sum_{n=1}^{\infty}\zeta_n^{m_1}\left(l_1,x\right)\zeta_n^{m_2}\left(l_2,x\right)y^n,$$

we deduce that Theorem 2.3. Obviously, Theorems 2.1 and 2.2 are special cases of Theorem 2.3. ■

Taking $m_1=m_2=2$ in (2.1), we obtain

Corollary 2.4. *For $l_1,l_2\geqslant 2$ and $l_1,l_2\in Z^+$, we have the relation*

$$\begin{aligned}\zeta^2\left(l_1\right)\zeta^2\left(l_2\right)=&\sum_{n=1}^{\infty}\left\{\frac{\zeta_n^2\left(l_2\right)}{\left(n+1\right)^{2l_1}}+\frac{\zeta_n^2\left(l_1\right)}{\left(n+1\right)^{2l_2}}\right\}\\&+2\sum_{n=1}^{\infty}\left\{\frac{\zeta_n\left(l_1\right)\zeta_n^2\left(l_2\right)}{\left(n+1\right)^{l_1}}+\frac{\zeta_n\left(l_1\right)}{\left(n+1\right)^{2l_2+l_1}}\right\}\\&+\zeta\left(2l_1+2l_2\right)+4\sum_{n=1}^{\infty}\frac{\zeta_n\left(l_1\right)\zeta_n\left(l_2\right)}{\left(n+1\right)^{l_2+l_1}}\\&+2\sum_{n=1}^{\infty}\left\{\frac{\zeta_n^2\left(l_1\right)\zeta_n\left(l_2\right)}{\left(n+1\right)^{l_2}}+\frac{\zeta_n\left(l_2\right)}{\left(n+1\right)^{2l_1+l_2}}\right\}.\end{aligned}\tag{2.5}$$

Let $m_1=m_2=2,l_1=l_2=l$ in (2.5), then

$$\zeta^4\left(l\right)=\zeta\left(4l\right)+6\sum_{n=1}^{\infty}\frac{\zeta_n^2\left(l\right)}{\left(n+1\right)^{2l}}+4\sum_{n=1}^{\infty}\frac{\zeta_n^3\left(l\right)}{\left(n+1\right)^{l}}+4\sum_{n=1}^{\infty}\frac{\zeta_n\left(l\right)}{\left(n+1\right)^{3l}}.\tag{2.6}$$

Taking $m_2=2$ in (2.2), we obtain

Corollary 2.5. *For $l_1,l_2\geqslant 2$ and $l_1,l_2\in Z^+$, we have*

$$\begin{aligned}\zeta\left(l_1\right)\zeta^2\left(l_2\right)=&\zeta\left(l_1+2l_2\right)+2\sum_{n=1}^{\infty}\frac{\zeta_n\left(l_1\right)\zeta_n\left(l_2\right)}{\left(n+1\right)^{l_2}}+2\sum_{n=1}^{\infty}\frac{\zeta_n\left(l_2\right)}{\left(n+1\right)^{l_1+l_2}}\\&+\sum_{n=1}^{\infty}\frac{\zeta_n^2\left(l_2\right)}{\left(n+1\right)^{l_1}}+\sum_{n=1}^{\infty}\frac{\zeta_n\left(l_1\right)}{\left(n+1\right)^{2l_2}}.\end{aligned}\tag{2.7}$$

Let $m_2=2,l_1=l_2=l$ in (2.7), we get

$$\zeta^3\left(l\right)=\zeta\left(3l\right)+3\sum_{n=1}^{\infty}\frac{\zeta_n^2\left(l\right)}{\left(n+1\right)^{l}}+3\sum_{n=1}^{\infty}\frac{\zeta_n\left(l\right)}{\left(n+1\right)^{2l}}.\tag{2.8}$$

Remark. Noting that the Riemann zeta function $\zeta^3\left(l\right)$, which can be rewritten as

$$\zeta^3\left(l\right)=1+\sum_{n=1}^{\infty}\left(\zeta_{n+1}^3\left(l\right)-\zeta_n^3\left(l\right)\right).\tag{2.9}$$

Then using the binomial theorem, we have

$$\zeta_{n+1}^{3}(l)=\zeta_{n}^{3}(l)+3\frac{\zeta_{n}^{2}(l)}{(n+1)^{l}}+3\frac{\zeta_{n}(l)}{(n+1)^{2l}}+\frac{1}{(n+1)^{3l}}. \tag{2.10}$$

Loading (2.10) in (2.9), we obtain (2.8).

From Theorem 2.3, let $m_2=2, l_1=l_2=l, n\to\infty$, we obtain

Corollary 2.6. *For $l\geqslant 2$, $l\in Z^{+}$ and $x\in[-1,1)$, we have*

$$Li_{l}^{3}(x)=3\sum_{n=1}^{\infty}\frac{\zeta_{n}^{2}(l,x)}{(n+1)^{l}}x^{n+3}+3\sum_{n=1}^{\infty}\frac{\zeta_{n}(l,x)}{(n+1)^{2l}}x^{2n+3}+Li_{3l}\left(x^{3}\right), \tag{2.11}$$

where $Li_{l}(x)=\sum\limits_{n=1}^{\infty}\frac{x^{n}}{n^{l}}$.

Taking $x=1, x=-1$ in (2.11) we obtain (1.5)(1.6). Taking $m_2=m-1, l_1=l_2=1, n\to\infty$ *in* (2.4) and combining $Li_{1}(x)=-\ln(1-x)$, we obtain

Corollary 2.7. *For $m\geqslant 2$, $l\in Z^{+}$ and $x\in[-1,1)$, we obtain*

$$\begin{aligned}&\ln^{m}\left(\frac{1}{1-x}\right)\\&=\left\{\sum_{n=1}^{\infty}\frac{x^{nm}}{n^{m}}+\sum_{j=1}^{m-1}\binom{m}{j}\sum_{n=1}^{\infty}\left(1+\frac{x}{2}+\cdots+\frac{x^{n-1}}{n}\right)^{j}\left(\frac{x^{n}}{n+1}\right)^{m-j}x^{m}\right\},\end{aligned} \tag{2.12}$$

where $x\in[-1,1)$.

In the same manner we obtain the more general identity

$$\begin{aligned}&Li_{l}^{m}(x)\\&=\left\{\sum_{n=1}^{\infty}\frac{x^{nm}}{n^{lm}}+\sum_{j=1}^{m-1}\binom{m}{j}\sum_{n=1}^{\infty}\left(1+\frac{x}{2^{l}}+\cdots+\frac{x^{n-1}}{n^{l}}\right)^{j}\left(\frac{x^{n}}{(n+1)^{l}}\right)^{m-j}x^{m}\right\}.\end{aligned} \tag{2.12'}$$

Lemma 2.8 ([6]). *For $l\geqslant 2$, $l\in Z^{+}$ and $x\in[-1,1)$, we have for $k\geqslant 0$,*

$$\sum_{n=k}^{\infty}S(n,k)\frac{t^{n}}{n!}=\ln^{k}\left(\frac{1}{1-t}\right)/k!, \tag{2.13}$$

where $S(n,k)$ is Stirling numbers of the first kind and

$$S(n,1)=(n-1)!, S(n,2)=(n-1)!H_{n-1}, S(n,3)=\frac{(n-1)!}{2!}\left[H_{n-1}^{2}-\zeta_{n}(2)\right],$$

$$S(n,4)=\frac{(n-1)!}{3!}\left[H_{n-1}^{3}-3H_{n-1}\zeta_{n}(2)+2\zeta_{n-1}(3)\right].$$

Taking $k=2,3,4$ in (2.13) yields

Corollary 2.9.

$$\ln^2(1-x)=2\sum_{n=1}^{\infty}\frac{H_n x^{n+1}}{n+1},\ln^3(1-x)=3\sum_{n=1}^{\infty}\frac{\left(\zeta_n(2)-H_n^2\right)x^{n+1}}{n+1},$$
$$\ln^4(1-x)=4\sum_{n=1}^{\infty}\frac{\left(H_n^3-3H_n\zeta_n(2)+2\zeta_n(3)\right)x^{n+1}}{n+1},$$

where $x\in[-1,1)$.

3. Representation of Euler sums by Riemann zeta function

Lemma 3.1 ([5]). *For an odd weight* $m=p+q$*, the Euler sums are reducible to zeta values,*

$$\begin{aligned}\sum_{n=1}^{\infty}\frac{\zeta_n(p)}{n^q}&=\zeta(m)\left(\frac{1}{2}-\frac{(-1)^p}{2}\binom{m-1}{p}-\frac{(-1)^p}{2}\binom{m-1}{q}\right)\\&+(-1)^p\sum_{k=1}^{[p/2]}\binom{m-2k-1}{q-1}\zeta(2k)\zeta(m-2k)+\frac{1-(-1)^p}{2}\zeta(p)\zeta(q)\\&+(-1)^p\sum_{k=1}^{[q/2]}\binom{m-2k-1}{p-1}\zeta(2k)\zeta(m-2k),\end{aligned}\tag{3.1}$$

where $\zeta(1)$ *should be interpreted as 0 wherever it occurs.*

Theorem 3.2. *For an odd weight* $m=3l$ (l *is a positive integer*)*, the Euler sums are reducible to zeta values,*

$$\begin{aligned}\sum_{n=1}^{\infty}\frac{\zeta_n^2(l)}{n^l}&=\frac{1}{3}\zeta^3(l)+\zeta(3l)\left(\frac{1}{6}-\frac{(-1)^l}{2}\binom{3l-1}{l}-\frac{(-1)^l}{2}\binom{3l-1}{2l}\right)\\&+(-1)^l\sum_{k=1}^{[l/2]}\binom{3l-2k-1}{2l-1}\zeta(2k)\zeta(3l-2k)+\frac{1-(-1)^l}{2}\zeta(l)\zeta(2l)\\&+(-1)^l\sum_{k=1}^{l}\binom{3l-2k-1}{l-1}\zeta(2k)\zeta(3l-2k).\end{aligned}\tag{3.2}$$

Proof. Taking $p=l,q=2l$ in (3.1) and combining (1.5) gives (3.2).

Taking $l=2$ in (1.5) and $l=3$ in (3.2), we have

$$\sum_{n=1}^{\infty}\frac{\zeta_n^2(2)}{n^2}=\sum_{n=1}^{\infty}\frac{\zeta_n(2)}{n^4}+\frac{1}{3}\left\{\zeta^3(2)-\zeta(6)\right\},\tag{3.3}$$

$$\sum_{n=1}^{\infty}\frac{\zeta_n^2(3)}{n^3}=\frac{253}{6}\zeta(9)+\frac{1}{3}\zeta^3(3)-21\zeta(2)\zeta(7)-6\zeta(4)\zeta(5). \tag{3.4}$$

From [7], we obtain

$$\sum_{n=1}^{\infty}\frac{\zeta_n(2)}{n^4}=-\frac{1}{3}\zeta(6)+\zeta^2(3). \tag{3.5}$$

Combining (3.3)(3.5) gives (3.3)′:

$$\sum_{n=1}^{\infty}\frac{\zeta_n^2(2)}{n^2}=\frac{19}{24}\zeta(6)+\zeta^2(3). \tag{3.3}'$$

In their paper, "Euler Sums and Contour Integral Representations", Philippe Flajolet and Bruno Salvy gave the following conclusion: If p_1+p_2+q is even, and $p_1>1, p_2>1, q>1$, the quadratic sums

$$S_{p_1p_2,q}=\sum_{n=1}^{\infty}\frac{\zeta_n(p_1)\zeta_n(p_2)}{n^q}$$

are reducible to linear sums (see Theorem 4.2 in the reference [5]). Hence we obtain from (2.6) and Theorem 4.2 in the reference [5] the following theorem:

Theorem 3.3. *For integer $l>1$, the cubic sums*

$$S_{l^3,l}=\sum_{n=1}^{\infty}\frac{\zeta_n^3(l)}{n^l}$$

are reducible to linear sums.

From Theorem 4.2 in the reference [5], let $p_1=p_2=2, q=4$. After a little simplification, we deduce that

$$\sum_{n=1}^{\infty}\frac{\zeta_n^2(2)}{n^4}=11S_{2,6}+\frac{457}{18}\zeta(8)+6\zeta(2)\zeta^2(3)-40\zeta(3)\zeta(5), \tag{3.6}$$

where $S_{2,6}=\sum\limits_{n=1}^{\infty}\frac{\zeta_n(2)}{n^6}$. Substituting (3.6) into (2.6) respectively, we obtain

$$\sum_{n=1}^{\infty}\frac{\zeta_n^3(2)}{n^2}=\frac{31}{2}S_{2,6}+\frac{3855}{96}\zeta(8)+9\zeta(2)\zeta^2(3)-60\zeta(3)\zeta(5). \tag{3.7}$$

In [5], Philippe Flajolet and Bruno Salvy proves (3.8),

$$\begin{gathered}\sum_{n=1}^{\infty}\frac{L_n(1)}{n^2}=\frac{\pi^2}{4}\ln 2-\frac{1}{4}\zeta(3), \qquad \sum_{n=1}^{\infty}\frac{H_n(-1)^{n-1}}{n^2}=\frac{5}{8}\zeta(3),\\ \sum_{n=1}^{\infty}\frac{L_n(1)(-1)^{n-1}}{n^2}=\frac{\pi^2}{4}\ln 2-\frac{5}{8}\zeta(3).\end{gathered} \tag{3.8}$$

It is easily seen that

$$\sum_{n=1}^{\infty}\frac{\zeta_n(m)(-1)^{n-1}}{n^s}+\sum_{n=1}^{\infty}\frac{L_n(s)}{k^m}$$
$$=\left(1-\frac{1}{2^{s-1}}\right)\zeta(m)\zeta(s)+\left(1-\frac{1}{2^{m+s-1}}\right)\zeta(m+s), \quad (3.9)$$

$$\sum_{n=1}^{\infty}\frac{L_n(m)(-1)^{n-1}}{n^s}+\sum_{n=1}^{\infty}\frac{L_n(s)(-1)^{k-1}}{k^m}$$
$$=\left(1-\frac{1}{2^{m-1}}\right)\left(1-\frac{1}{2^{s-1}}\right)\zeta(m)\zeta(s)+\zeta(m+s). \quad (3.10)$$

Substituting (3.8) into (3.9)(3.10), we get

$$\begin{aligned}\sum_{n=1}^{\infty}\frac{\zeta_n(2)(-1)^{n-1}}{n}&=\zeta(3)-\frac{\pi^2}{12}\ln 2,\\ \sum_{n=1}^{\infty}\frac{L_n(2)(-1)^{n-1}}{n}&=\frac{13}{8}\zeta(3)-\frac{\pi^2}{6}\ln 2.\end{aligned} \quad (3.11)$$

Taking $x=-1$ in Corollary 2.9, we have

$$\ln^3 2=\sum_{n=1}^{\infty}\frac{\zeta_n(2)-H_n^2}{n+1}(-1)^{n-1}. \quad (3.12)$$

Combining (3.11) and (3.12), we obtain

$$\sum_{n=1}^{\infty}\frac{H_n^2(-1)^{n-1}}{n}=\frac{3}{4}\zeta(3)+\frac{1}{3}(\ln 2)^3-\frac{\pi^2}{12}\ln 2. \quad (3.13)$$

Taking $l=1$ in (1.6) and combining (3.8), we have

$$\sum_{n=1}^{\infty}\frac{L_n^2(1)(-1)^{n-1}}{n}=\frac{1}{3}\ln^3 2+\frac{\pi^2}{4}\ln 2-\frac{1}{2}\zeta(3). \quad (3.14)$$

Taking $m=4,5$ and $x=-1$ in (2.12), we obtain

$$\begin{aligned}\ln^4(2)&=\zeta(4)+4\sum_{n=1}^{\infty}\frac{L_n(1)(-1)^n}{(n+1)^3}\\ &\quad+6\sum_{n=1}^{\infty}\frac{L_n^2(1)}{(n+1)^2}+4\sum_{n=1}^{\infty}\frac{L_n^3(1)(-1)^n}{(n+1)}, \quad (3.15)\\ \ln^5(2)&=\frac{15}{16}\zeta(5)+5\sum_{n=1}^{\infty}\frac{L_n(1)}{(n+1)^4}+10\sum_{n=1}^{\infty}\frac{L_n^2(1)(-1)^n}{(n+1)^3}\\ &\quad+10\sum_{n=1}^{\infty}\frac{L_n^3(1)}{(n+1)^2}+5\sum_{n=1}^{\infty}\frac{L_n^4(1)(-1)^n}{(n+1)}. \quad (3.16)\end{aligned}$$

Similarly to Theorem 2.1, constructing function $y = \sum_{n=1}^{\infty} L_n^2(1)\zeta_n(2)\,x^n$, $y = \sum_{n=1}^{\infty} L_n^2(1)L_n(2)\,x^n$, we have

$$\zeta(4) - \zeta(2)\ln^2 2 = \sum_{n=1}^{\infty} \frac{-L_n^2(1)}{(n+1)^2} - 2\sum_{n=1}^{\infty} \frac{(-1)^n L_n(1)\,\zeta_n(2)}{(n+1)} - 2\sum_{n=1}^{\infty} \frac{(-1)^n L_n(1)}{(n+1)^3} + \sum_{n=1}^{\infty} \frac{-\zeta_n(2)}{(n+1)^2}, \tag{3.17}$$

$$\frac{1}{2}\zeta(2)\ln^2 2 - \frac{7}{8}\zeta(4) = \sum_{n=1}^{\infty} \frac{L_n^2(1)(-1)^n}{(n+1)^2} + \sum_{n=1}^{\infty} \frac{2(-1)^n L_n(1)\,L_n(2)}{(n+1)} + \sum_{n=1}^{\infty} \frac{2L_n(1)}{(n+1)^3} + \sum_{n=1}^{\infty} \frac{L_n(2)}{(n+1)^2}. \tag{3.18}$$

From [5], Philippe Flajolet and Bruno Salvy gave the following formula (see Theorem 7.1 in the reference [5])

$$\sum_{n=1}^{\infty} \frac{L_n(1)}{n^s} = \zeta(s)\ln 2 - \frac{s}{2}\zeta(s+1) + L(s+1) + \frac{1}{2}\sum_{j=1}^{s} L(s-j+1)L(j), \qquad 1 < s \in Z. \tag{3.19}$$

where $L(s) = \sum_{n=1}^{\infty} \frac{(-1)^{n-1}}{n^s} = \left(1 - 2^{1-s}\right)\zeta(s)$. Let $s = 3, 4$ in (3.19), we get

$$\sum_{n=1}^{\infty} \frac{L_n(1)}{n^3} = \frac{7}{4}\zeta(3)\ln 2 - \frac{\pi^4}{288}, \tag{3.20}$$

$$\sum_{n=1}^{\infty} \frac{L_n(1)}{n^4} = \frac{15}{8}\ln 2\zeta(4) + \frac{3}{8}\zeta(2)\,\zeta(3) - \frac{17}{16}\zeta(5). \tag{3.21}$$

In [1], David H. Bailey, Jonathan M. Borwein and Roland Girgensohn gave the following formula by the experimental method (see Table 3 in the reference [1])

$$\sum_{n=1}^{\infty} \frac{L_n^2(1)}{(n+1)^2} = 6Li_4\left(\frac{1}{2}\right) + \frac{1}{4}\ln^4 2 - \frac{29}{8}\zeta(4) + \frac{3}{2}\zeta(2)\ln^2 2, \tag{3.22}$$

$$\sum_{n=1}^{\infty} \frac{L_n^2(1)(-1)^{n-1}}{(n+1)^2} = \frac{7}{4}\zeta(3)\ln 2 + \frac{37\pi^4}{1440} - \frac{\pi^2\ln^2 2}{3} - \frac{1}{6}\ln^4 2 - 4Li_4\left(\frac{1}{2}\right), \tag{3.23}$$

$$\sum_{n=1}^{\infty} \frac{L_n^2(1)}{(n+1)^3} = 4Li_5\left(\frac{1}{2}\right) - \frac{1}{30}\ln^5 2 - \frac{17}{32}\zeta(5) - \frac{11}{8}\zeta(4)\ln 2 + \frac{7}{4}\zeta(3)\ln^2 2 + \frac{1}{3}\zeta(2)\ln^3 2 - \frac{3}{4}\zeta(2)\,\zeta(3), \tag{3.24}$$

$$\sum_{n=1}^{\infty}\frac{L_n^2(1)(-1)^{n-1}}{(n+1)^3}=4\ln 2Li_4\left(\frac{1}{2}\right)+\frac{1}{6}\ln^5 2-\frac{79}{32}\zeta(5)+\frac{11}{8}\zeta(4)\ln 2$$
$$-\zeta(2)\ln^3 2+\frac{3}{8}\zeta(2)\zeta(3). \tag{3.25}$$

From [2] we know that

$$\sum_{n=1}^{\infty}\frac{L_n(1)(-1)^{n-1}}{n^3}=\frac{\pi^4}{60}+\frac{\pi^2\ln^2 2}{12}-\frac{1}{12}\ln^4 2-2Li_4\left(\frac{1}{2}\right). \tag{3.26}$$

Combining (3.15)-(3.18) and (3.20)-(3.26), we obtain

$$\sum_{n=1}^{\infty}\frac{L_n^3(1)(-1)^{n-1}}{(n+1)}=\frac{11\pi^2\ln^2 2}{24}+\frac{\ln^4 2}{24}+7Li_4\left(\frac{1}{2}\right)-\frac{15\pi^4}{288}, \tag{3.27}$$

$$\sum_{n=1}^{\infty}\frac{(-1)^{n-1}L_n(1)L_n(2)}{(n+1)}=\frac{5}{16}\zeta(4)-\frac{7}{8}\zeta(3)\ln 2-2\zeta(2)\ln^2 2. \tag{3.28}$$

$$\sum_{n=1}^{\infty}\frac{(-1)^{n-1}L_n(1)\zeta_n(2)}{(n+1)}=\frac{3}{4}\zeta(2)(\ln 2)^2+\frac{1}{24}(\ln 2)^4$$
$$+Li_4\left(\frac{1}{2}\right)-\frac{7}{16}\zeta(4), \tag{3.29}$$

$$\sum_{n=1}^{\infty}\frac{L_n^4(1)(-1)^{n-1}}{(n+1)}=\frac{11}{30}\ln^5 2-4\ln 2Li_4\left(\frac{1}{2}\right)-\frac{73}{2}\zeta(4)\ln 2+7\zeta(2)\ln^3 2$$
$$+\frac{5}{8}\zeta(2)\zeta(3)+\frac{709}{16}\zeta(5)-48Li_5\left(\frac{1}{2}\right). \tag{3.30}$$

Similarly, constructing function $y=\sum_{n=1}^{\infty}L_n^2(1)\zeta_n(3)x^n, y=\sum_{n=1}^{\infty}L_n^2(1)L_n(3)x^n$, we have

$$\zeta(5)-\zeta(3)\ln^2 2=2\sum_{n=1}^{\infty}\frac{(-1)^{n-1}L_n(1)\zeta_n(3)}{(n+1)}+2\sum_{n=1}^{\infty}\frac{(-1)^{n-1}L_n(1)}{(n+1)^4}$$
$$-\sum_{n=1}^{\infty}\frac{L_n^2(1)}{(n+1)^3}-\sum_{n=1}^{\infty}\frac{\zeta_n(3)}{(n+1)^2}, \tag{3.31}$$

$$\frac{15}{16}\zeta(5)-\frac{3}{4}\zeta(3)\ln^2 2=2\sum_{n=1}^{\infty}\frac{(-1)^{n-1}L_n(1)L_n(3)}{(n+1)}-2\sum_{n=1}^{\infty}\frac{L_n(1)}{(n+1)^4}$$
$$+\sum_{n=1}^{\infty}\frac{(-1)^{n-1}L_n^2(1)}{(n+1)^3}-\sum_{n=1}^{\infty}\frac{L_n(3)}{(n+1)^2}. \tag{3.32}$$

From Theorem 7.2 and 7.2 in the reference [5], we obtain

$$\begin{aligned}\sum_{n=1}^{\infty}\frac{(-1)^{n-1}L_n(1)}{n^4}&=\frac{15}{8}\zeta(4)\ln 2+\frac{3}{4}\zeta(2)\zeta(3)-\frac{59}{32}\zeta(5),\\ \sum_{n=1}^{\infty}\frac{L_n(3)}{n^2}&=\frac{1}{8}\zeta(2)\zeta(3)+\frac{41}{32}\zeta(5).\end{aligned}\tag{3.33}$$

Let $p=3,q=2$ in lemma 3.1, we get

$$\sum_{n=1}^{\infty}\frac{\zeta_n(3)}{n^2}=\frac{11}{2}\zeta(5)-2\zeta(2)\zeta(3).\tag{3.34}$$

Combining (3.21)(3.24)(3.25)(3.31)-(3.34) gives

$$\begin{aligned}\sum_{n=1}^{\infty}\frac{L_n(1)\zeta_n(3)(-1)^{n-1}}{(n+1)}&=2Li_5\left(\frac{1}{2}\right)-\frac{1}{60}\ln^5 2-\frac{23}{64}\zeta(5)+\frac{19}{16}\zeta(4)\ln 2\\&\quad+\frac{3}{8}\zeta(3)\ln^2 2+\frac{1}{6}\zeta(2)\ln^3 2-\frac{5}{8}\zeta(2)\zeta(3).\end{aligned}\tag{3.35}$$

$$\begin{aligned}\sum_{n=1}^{\infty}\frac{L_n(1)L_n(3)(-1)^{n-1}}{(n+1)}&=-2\ln 2Li_4\left(\frac{1}{2}\right)-\frac{1}{12}\ln^5 2+\frac{19}{16}\zeta(4)\ln 2\\&\quad+\frac{1}{2}\zeta(2)\ln^3 2+\frac{1}{4}\zeta(2)\zeta(3)-\frac{1}{8}\zeta(5)-\frac{3}{8}\zeta(3)\ln^2 2.\ \blacksquare\end{aligned}\tag{3.36}$$

Acknowledgements. The authors will be very grateful to the referee for his/her valuable suggestions.

References

[1] D.H. Bailey, J.M. Borwein, and R. Girgensohn, *Experimental evaluation of Euler sums*, Experimental Mathematics **3**(1) (1994), 17–30.

[2] D. Borwein, J.M. Borwein, and R. Girgensohn, *Explicit evaluation of Euler sums*, Proc. Edinburgh Math. **38** (1995), 277–294.

[3] J. Borwein, P. Borwein, R. Girgensohn, and S. Parnes, *A discussion*, Experimental Mathematics., 1995.

[4] M. Eie, C.-S. Wei, *Evaluations of some quadruple Euler sums of even weight*, Functiones et Approximatio **46**(1) (2012), 63–67.

[5] P. Flajolet and B. Salvy, *Euler sums and contour integral representations*, Experimental Mathematics **7**(1) (1998), 15–35.

[6] L. Comtet, *Advanced Combinatorics*, Boston: D Reidel Publishing Company, 1974.

[7] P. Sun, *The 6-order sums of Riemann zeta function*, Acta Mathematica Sinica, chinese Series ., **50**(2) (2007), 373–384.

Address: Ce Xu, Jinfa Cheng: School of Mathematical Sciences, Xiamen University, Fujian 361005, P. R. China.

E-mail: xuce1242063253@163.com, jfcheng@xmu.edu.cn

Received: 12 March 2015; **revised:** 19 September 2015

Functiones et Approximatio
54.1 (2016), 39–55
doi: 10.7169/facm/2016.54.1.4

MILNOR K-GROUPS ATTACHED TO ELLIPTIC CURVES OVER A p-ADIC FIELD

Toshiro Hiranouchi

Abstract: We study the Galois symbol map of the Milnor K-group attached to elliptic curves over a p-adic field. As by-products, we determine the structure of the Chow group for the product of elliptic curves over a p-adic field under some assumptions.

Keywords: Elliptic curves, Chow groups, Local fields.

1. Introduction

K. Kato and M. Somekawa introduced in [13] the Milnor type K-group $K(k; G_1, \ldots, G_q)$ attached to semi-abelian varieties $G_1, \ldots, G_q$ over a field k which is now called the *Somekawa K-group*. The group is defined by the quotient

$$K(k; G_1, \ldots, G_q) := \left(\bigoplus_{k'/k: \text{ finite}} G_1(k') \otimes_{\mathbb{Z}} \cdots \otimes_{\mathbb{Z}} G_q(k') \right) / R \tag{1}$$

where k' runs through all finite extensions over k and R is the subgroup which produces "the projection formula" and "the Weil reciprocity law" as in the Milnor K-theory. As a special case, for the multiplicative groups $G_1 = \cdots = G_q = \mathbb{G}_m$, the group $K(k; \overbrace{\mathbb{G}_m, \ldots, \mathbb{G}_m}^{q})$ is isomorphic to the ordinary Milnor K-group $K_q^M(k)$ of the field k ([13], Thm. 1.4). For general semi-abelian varieities $G_1, \ldots, G_q$, let $G_i[m]$ be the Galois module defined by the kernel of $G_i(\overline{k}) \stackrel{m}{\to} G_i(\overline{k})$ the multiplication by a positive integer m prime to the characteristic of k. Somekawa defined also the Galois symbol map

$$h : K(k; G_1, \ldots, G_q)/m \to H^q(k, G_1[m] \otimes \cdots \otimes G_q[m])$$

by the similar way as in the classical Galois symbol map $K_q^M(k)/m \to H^q(k, \mu_m^{\otimes q})$ on the Milnor K-group, where $\mu_m = \mathbb{G}_m[m]$ is the Galois module of all m-th

2010 Mathematics Subject Classification: primary: 11G07

roots of unity. He also presented a "conjecture" in which the map h is injective for arbitrary field k. For the case $G_1 = \cdots = G_q = \mathbb{G}_m$, the conjecture holds by the Milnor-Bloch-Kato conjecture, now is a theorem of Voevodsky, Rost, and Weibel ([17]). Although it holds in some special cases ([18], [19], and [9]), Spieß and Yamazaki disproved this for some tori ([14], Prop. 7).

The aim of this note is to show this "conjecture" for elliptic curves over a local field under some assumptions.

Theorem 1.1 (Thm. 4.1, Prop. 4.2). *Let k be a finite field extension of the p-adic field $\mathbb{Q}_p$ and n a positive integer.*

(i) *Let q be an integer $\geqslant 3$ and $E_1, \ldots, E_q$ be elliptic curves over k with $E_i[p] \subset E_i(k)$ for $i = 1, \ldots, q$. Assume that E_1 has good ordinary reduction or split multiplicative reduction, and E_i has good reduction or split multiplicative reduction for $i = 2, \ldots, q$. Then, we have*

$$K(k; E_1 \ldots, E_q)/p^n = 0.$$

(ii) *Let E_1, E_2 be elliptic curves over k with $E_i[p^n] \subset E_i(k)$ for $i = 1, 2$. Assume that E_1 has good ordinary reduction or split multiplicative reduction, and E_2 has good reduction or split multiplicative reduction. Then, the Galois symbol map*

$$h : K(k; E_1, E_2)/p^n \to H^2(k, E_1[p^n] \otimes E_2[p^n])$$

is injective.

The theorem above is known when E_i's have *semi-ordinary reduction*, that is, good ordinary or multiplicative reduction ([18], [9], see also [8]). Hence our main interest is in elliptic curves which have good supersingular reduction.

In our previous paper [3], we investigate the image of the Galois symbol map h. As byproducts, we obtain the structure of the Chow group $\mathrm{CH}_0(E_1 \times E_2)$ of 0-cycles as follows. By Corollary 2.4.1 in [9], we have

$$\mathrm{CH}_0(E_1 \times E_2) \simeq \mathbb{Z} \oplus E_1(k) \oplus E_2(k) \oplus K(k; E_1, E_2).$$

The Albanese kernel $T(E_1 \times E_2) := \mathrm{Ker}(\mathrm{alb} : \mathrm{CH}_0(E_1 \times E_2)^0 \to (E_1 \times E_2)(k))$ coincides with the Somekawa K-group $K(k; E_1, E_2)$, where $\mathrm{CH}_0(E_1 \times E_2)^0$ is the kernel of the degree map $\mathrm{CH}_0(E_1 \times E_2) \to \mathbb{Z}$. Mattuck's theorem [6] implies the following:

Corollary 1.2. *Let E_1 and E_2 be elliptic curves over k with good or split multiplicative reduction. Assume that E_1 does not have good supersingular reduction and $E_i[p^n] \subset E_i(k)$ for $i = 1, 2$. Then, we have*

$$\mathrm{CH}_0(E_1 \times E_2)/p^n \simeq \begin{cases} (\mathbb{Z}/p^n)^{2[k:\mathbb{Q}_p]+6}, & \text{if } E_1 \text{ and } E_2 \text{ have a same reduction type,} \\ (\mathbb{Z}/p^n)^{2[k:\mathbb{Q}_p]+7}, & \text{otherwise.} \end{cases}$$

Notation

Throughout this note, for an abelian group A and a positive integer m, let $A[m]$ be the kernel and A/m the cokernel of the map $m : A \to A$ defined by the multiplication by m. For a field F, we denote by F^{sep} the separable closure of F and $G_F := \mathrm{Gal}(F^{\mathrm{sep}}/F)$ the absolute Galois group of F. We also denote by $H^i(F, M) := H^i(G_F, M)$ the Galois cohomology group of G_F for a G_F-module M. The tensor product $A \otimes B$ for abelian groups A, B means $A \otimes_{\mathbb{Z}} B$.

For a finite field extension $K/\mathbb{Q}_p$, we denote by v_K the normalized valuation, $\mathfrak{m}_K$ the maximal ideal of the valuation ring $\mathcal{O}_K$, $\mathcal{O}_K^\times = U_K^0$ the group of units in $\mathcal{O}_K$ and $\mathbb{F}_K = \mathcal{O}_K/\mathfrak{m}_K$ the finite residue field.

Acknowledgments. This work was supported by KAKENHI 25800019. The author would like to thank the referee for pointing out mistakes of the proof of Theorem 3.6 in an earlier version of this article.

2. Mackey functors

Throughout this section, let k be a field of characteristic 0.

Mackey products

Definition 2.1. A *Mackey functor* A over k is a contravariant functor from the category of étale schemes over k to that of abelian groups equipped with a covariant structure for finite morphisms such that $A(X_1 \sqcup X_2) = A(X_1) \oplus A(X_2)$ and if

$$\begin{array}{ccc} X' & \xrightarrow{g'} & X \\ {\scriptstyle f'}\downarrow & & \downarrow{\scriptstyle f} \\ Y' & \xrightarrow{g} & Y \end{array}$$

is a Cartesian diagram, then the induced diagram

$$\begin{array}{ccc} A(X') & \xrightarrow{g'_*} & A(X) \\ {\scriptstyle f'^*}\uparrow & & \uparrow{\scriptstyle f^*} \\ A(Y') & \xrightarrow{g_*} & A(Y) \end{array}$$

commutes.

For a Mackey functor A, we denote by $A(K)$ its value $A(\mathrm{Spec}(K))$ for a field extension K over k.

Definition 2.2. For Mackey functors $A_1, \ldots, A_q$, their *Mackey product* $A_1 \otimes \cdots \otimes A_q$ is defined as follows: For any finite field extension K/k,

$$(A_1 \otimes \cdots \otimes A_q)(K) := \left(\bigoplus_{L/K:\,\text{finite}} A_1(L) \otimes \cdots \otimes A_q(L) \right) / R,$$

where R is the subgroup generated by elements of the following form:

(PF) For any finite field extensions $K \subset K_1 \subset K_2$, and if $x_{i_0} \in A_{i_0}(K_2)$ and $x_i \in A_i(K_1)$ for all $i \neq i_0$, then

$$j^*(x_1) \otimes \cdots \otimes x_{i_0} \otimes \cdots \otimes j^*(x_q) - x_1 \otimes \cdots \otimes j_*(x_{i_0}) \otimes \cdots \otimes x_q,$$

where $j = j_{K_2/K_1} : \mathrm{Spec}(K_2) \to \mathrm{Spec}(K_1)$ is the canonical map.

This product gives a monoidal structure in the abelian category of Mackey functors with unit $\mathbb{Z} : k' \mapsto \mathbb{Z}$. We write $\{x_1, \ldots, x_q\}_{K/k}$ for the image of $x_1 \otimes \cdots \otimes x_q \in A_1(K) \otimes \cdots \otimes A_q(K)$ in the product $(A_1 \otimes \cdots \otimes A_q)(k)$. For any field extension K/k, the canonical map $j = j_{K/k} : k \hookrightarrow K$ induces the pull-back

$$\mathrm{Res}_{K/k} := j^* : (A_1 \otimes \cdots \otimes A_q)(k) \longrightarrow (A_1 \otimes \cdots \otimes A_q)(K)$$

which is called the *restriction map*. If the extension K/k is finite, then the push-forward

$$N_{K/k} := j_* : (A_1 \otimes \cdots \otimes A_q)(K) \longrightarrow (A_1 \otimes \cdots \otimes A_q)(k)$$

is given by $N_{K/k}(\{x_1, \ldots, x_q\}_{L/K}) = \{x_1, \ldots, x_q\}_{L/k}$ on symbols and is called the *norm map*.

Let $G_1, \ldots, G_q$ be semi-abelian varieties over k. These form a Mackey functor by $K \mapsto G_i(K)$. The *Somekawa K-group* $K(k; G_1, \ldots, G_q)$ attached to $G_1, \ldots, G_q$ is defined by a quotient of $(G_1 \otimes \cdots \otimes G_q)(k)$ by the subgroup which produces "the Weil reciprocity law" (see for the precise definition, [13]).

Galois symbol map

For any positive integer m, we consider the isogeny $m : G_i \to G_i$ induced from the multiplication by m. The exact sequence

$$0 \to G_i[m] \to G_i(\overline{k}) \xrightarrow{m} G_i(\overline{k}) \to 0$$

of Galois modules gives an injection of Mackey functors

$$G_i/m \hookrightarrow H^1(-, G_i[m]),$$

where $G_i/m := \mathrm{Coker}(m)$ (in the category of Mackey functors) and $H^1(-, G_i[m])$ is also the Mackey functor given by $K \mapsto H^1(K, G_i[m])$. The cup products and the corestriction on the Galois cohomology groups give

$$G_1/m \otimes \cdots \otimes G_q/m \to H^q(-, G_1[m] \otimes \cdots \otimes G_q[m]). \tag{2}$$

This map factors through $K(-; G_1, \dots, G_q)/m$ ([13], Prop. 1.5). The induced homomorphism

$$K(k; G_1, \dots, G_q)/m \to H^q(k, G_1[m] \otimes \cdots \otimes G_q[m])$$

is called the *Galois symbol map*.

3. Higher unit groups

Throughout this section, we fix a finite field extension k of $\mathbb{Q}_p$ and *assume* that it contains $\mu_p := \mathbb{G}_m[p]$ the group of all p-th roots of unity.

Mackey functor defined by higher unit groups

Let K be a finite field extension of k and put $e_0(K) := v_K(p)/(p-1)$. The unit group $U_K^0 = \mathcal{O}_K^\times$ and the higher unit groups $U_K^i := 1 + \mathfrak{m}_K^i$ $(i \geqslant 1)$ induce a filtration $\{\overline{U}_K^i\}_{i \geqslant 0}$ of $K^\times/p$ which is given by

$$\overline{U}_K^i := \mathrm{Im}(U_K^i \hookrightarrow K^\times \twoheadrightarrow K^\times/p).$$

By abuse of notation, we still use $a \in \overline{U}_K^i$ for the residue class represented by a unit $a \in U_K^i$.

Lemma 3.1 (cf. [5], Lem. 2.1.3).

(a) *If* $0 \leqslant i < pe_0(K)$, *then*

$$\overline{U}_K^i/\overline{U}_K^{i+1} \simeq \begin{cases} \mathbb{F}_K, & \text{if } p \nmid i, \\ 1, & \text{if } p \mid i. \end{cases}$$

(b) *If* $i = pe_0(K)$, *then* $\overline{U}_K^{pe_0(K)}/\overline{U}_K^{pe_0(K)+1} \simeq \mathbb{Z}/p$.

(c) *If* $i > pe_0(K)$, *then* $\overline{U}_K^i = 1$.

Lemma 3.2 ([5], Lem. 2.1.5). *Let K be a finite field extension of k. For a positive integer i, and $a \in \overline{U}_K^i \smallsetminus \overline{U}_K^{i+1}$, we define an extension $L = K(\sqrt[p]{a})$ of K. For any $\sigma \in \mathrm{Gal}(L/K)$, put $i(\sigma) := v_L(\sigma(\varpi) - \varpi)$, where ϖ is a uniformizer of L.*

(a) *If* $1 \leqslant i < pe_0(K)$ *and* $p \nmid m$ *then L/K is a totally ramified extension of degree p and* $i(\sigma) = pe_0(K) - i + 1$ *for* $\sigma \in \mathrm{Gal}(L/K)$ *with* $\sigma \neq 1$.

(b) *If* $i = pe_0(K)$, *then L/K is an unramified extension of degree p.*

For any integer $i \geqslant 0$, we define a sub Mackey functor $\overline{U}^i$ of $\mathbb{G}_m/p := \mathrm{Coker}(p : \mathbb{G}_m \to \mathbb{G}_m)$ over k by

$$\overline{U}^i(K) := \overline{U}_K^{ie(K/k)}$$

for a field extension K/k with ramification index $e(K/k)$. For a finite field extension L/K over k and $j = j_{L/K} : \mathrm{Spec}(L) \to \mathrm{Spec}(K)$, the covariant map $N_{L/K} :=$

$j_* : \overline{U}^i(L) \to \overline{U}^i(K)$ is given by the norm homomorphism $N_{L/K} : L^\times \to K^\times$. We also denote by $\mathrm{Res}_{L/K}$ the contravariant map j^*. The Galois symbol map (2) induces the following isomorphisms:

Lemma 3.3 ([9], Lem. 4.2.1). *For integers $i, j \geqslant 0$ with $i + j \geqslant 2$, we have*

$$(\overline{U}^0)^{\otimes i} \otimes (\mathbb{G}_m/p)^{\otimes j} \xrightarrow{\simeq} \begin{cases} H^2(-, \mu_p^{\otimes 2}), & \text{if } i+j=2, \\ 0, & \text{otherwise.} \end{cases}$$

For integers $m, n \geqslant 0$, we define a map $h^{m,n} : \overline{U}^m \otimes \overline{U}^n \to H^2(-, \mu_p^{\otimes 2})$ of Mackey functors over k by the composition

$$h^{m,n} : \overline{U}^m \otimes \overline{U}^n \to \mathbb{G}_m/p \otimes \mathbb{G}_m/p \xrightarrow{\simeq} H^2(-, \mu_p^{\otimes 2}).$$

Here, the latter map is the Galois symbol map on $\mathbb{G}_m/p \otimes \mathbb{G}_m/p$ defined in (2) and is an isomorphism (Lem. 3.3). We also denote by

$$h^{-1,n} : \mathbb{G}_m/p \otimes \overline{U}^n \to \mathbb{G}_m/p \otimes \mathbb{G}_m/p \xrightarrow{\simeq} H^2(-, \mu_p^{\otimes 2})$$

by convention. For any finite field extension K/k, the map $h^{m,n}$ induces $h_K^{m,n} : \left(\overline{U}^m \otimes \overline{U}^n\right)(K) \to H^2(K, \mu_p^{\otimes 2})$.

As noted in (2), the Galois symbol map

$$h : \left(\mathbb{G}_m/p \otimes \mathbb{G}_m/p\right)(k) \to H^2(k, \mu_p^{\otimes 2})$$

is given by $h(\{a,b\}_{K/k}) = \mathrm{Cor}_{K/k}(h^1(a) \cup h^1(b))$ for a symbol $\{a,b\}_{K/k} \in \left(\mathbb{G}_m/p \otimes \mathbb{G}_m/p\right)(k)$, where $h^1 : \mathbb{G}_m/p(K) \to H^1(K, \mu_p)$ is the Kummer map. The corestriction $\mathrm{Cor}_{K/k}$ is bijective (e.g., [8], Lem. 5.8). The cup product $\cup : H^1(K, \mu_p) \otimes H^1(K, \mu_p) \to H^2(K, \mu_p^{\otimes 2})$ on the Galois cohomology groups is characterized by the Hilbert symbol $(\ ,\ )_K : K^\times/p \otimes K^\times/p \to \mu_p$ as in the following commutative diagram (cf. [11], Chap. XIV):

$$\begin{array}{ccc} H^1(K,\mu_p) \otimes H^1(K,\mu_p) & \xrightarrow{\cup} & H^2(K, \mu_p^{\otimes 2}) \\ \simeq \uparrow & & \downarrow \simeq \\ K^\times/p \otimes K^\times/p & \xrightarrow{(\ ,\ )_K} & \mu_p \end{array} \quad . \tag{3}$$

The image in $H^2(K, \mu_p^{\otimes 2})$ by the Hilbert symbol are calculated as follows (cf. [3], Lem. 3.1):

Lemma 3.4. *Let m, n be integers $\geqslant 0$.*

(i)

$$\#(K^\times/p, \overline{U}_K^n)_K = \begin{cases} p, & \text{if } n \leqslant pe_0(K), \\ 0, & \text{otherwise.} \end{cases}$$

(ii) *If $p \nmid m$ or $p \nmid n$, then*

$$\#(\overline{U}_K^m, \overline{U}_K^n)_K = \begin{cases} p, & \text{if } m+n \leqslant pe_0(K), \\ 0, & \text{otherwise.} \end{cases}$$

(iii) *If $p \mid m$ and $p \mid n$, then*

$$\#(\overline{U}_K^m, \overline{U}_K^n)_K = \begin{cases} p, & \text{if } m+n < pe_0(K), \\ 0, & \text{otherwise.} \end{cases}$$

Let π be a uniformizer of K. Since $\overline{U}_K^{pe_0(K)} \simeq \mathbb{Z}/p$ (Lem. 3.1), one can find a unit $\rho \in \mathcal{O}_K^\times$ such that $1+\rho\pi^{pe_0(K)}$ is a generator of $\overline{U}_K^{pe_0(K)}$. It is known that the Hilbert symbol $(\pi, 1+\rho\pi^{pe_0(K)})_K$ is a generator of $H^2(K, \mu_p^{\otimes 2})$ (e.g., [7], Cor. A.12).

Lemma 3.5.

(i) *Let i, j be positive integers with $i+j = pe_0(K)$. Assume $i \nmid p$. Then, for any unit $u \in \mathcal{O}_K^\times$, there exists $v \in \mathcal{O}_K^\times$ such that $(1+u\pi^i, 1+v\pi^j)_K \neq 0$.*

(ii) *Let i be an integer which is prime to p with $0 < i < pe_0(K)$. Then, there exists $u \in \mathcal{O}_K^\times$ such that $(1+u\pi^i, \pi)_K \neq 0$.*

(iii) *Let i, j be positive integers. Assume $p \nmid i$, $p \nmid (i+j)$, $i+j < pe_0(K)$, and $i+2j > pe_0(K)$. Then, for any $\eta \in \mu_{q-1} \subset \mathcal{O}_K^\times$ there exists $v \in \mathcal{O}_K^\times$ such that $(1+\eta\pi^i, 1+v\pi^j)_K \neq 0$, where $q = \#\mathbb{F}_K$.*

Proof. (i) As in [1], Lemma 4.1, we have the following equalities:

$$\begin{aligned}
&(1+u\pi^i, 1+\rho u^{-1}\pi^j)_K \\
&\quad = (1+u\pi^i(1+\rho u^{-1}\pi^j), 1+\rho u^{-1}\pi^j)_K \quad \text{(by Lem. 3.4)} \\
&\quad = -(1+u\pi^i(1+\rho u^{-1}\pi^j), -u\pi^i)_K \\
&\quad = -(1+\tfrac{\rho}{1+u\pi^i}\pi^{pe_0(K)}, -u\pi^i)_K \quad \text{(from the Steinberg relation)} \\
&\quad = -(1+\rho\pi^{pe_0(K)}, -u\pi^i)_K \quad \text{(by } 1+\rho\pi^{pe_0(K)} = 1+\tfrac{\rho}{1+u\pi^i}\pi^{pe_0(K)} \text{ in } \overline{U}_K^{pe_0(K)}) \\
&\quad = -i(1+\rho\pi^{pe_0(K)}, \pi)_K \quad \text{(by Lem. 3.4)} \\
&\quad = i(\pi, 1+\rho\pi^{pe_0(K)})_K.
\end{aligned}$$

This implies $(1+u\pi^i, 1+\rho u^{-1}\pi^j)_K \neq 0$ because of $p \nmid i$.

(ii) Since $((1-\pi^i)^i, \pi)_K = (1-\pi^i, \pi^i)_K = 0$, we have

$$\begin{aligned}
(1+\rho\pi^{pe_0(K)}, \pi)_K &= (1+\rho\pi^{pe_0(K)}, \pi)_K + ((1-\pi^i)^i, \pi)_K \\
&= ((1+\rho\pi^{pe_0(K)})(1-\pi^i)^i, \pi)_K.
\end{aligned}$$

The unit $(1+\rho\pi^{pe_0(K)})(1-\pi^i)^i \in U_K^i \smallsetminus U_K^{i+1}$ gives the required unit u.

(iii) From (ii), there exists $u \in \mathcal{O}_K^\times$ such that $(1+u\pi^{i+j}, \pi)_K \neq 0$. Put $v = (1+\eta\pi^i)u\eta^{-1} \in \mathcal{O}_K^\times$. The calculations of symbols as in (i) we have

$$\begin{aligned}(1+\eta\pi^i, 1+v\pi^j)_K &\\ &= (1+\eta\pi^i(1+v\pi^j), 1+v\pi^j)_K \quad (\text{by } i+2j > pe_0(K) \text{ and Lem. 3.4})\\ &= -(1+\eta\pi^i(1+v\pi^j), -\eta\pi^i)_K\\ &= -i(1+u\pi^{i+j}, \pi)_K \neq 0.\end{aligned}$$

■

Mackey products of higher unit groups

The rest of this section is devoted to show the following theorem.

Theorem 3.6. *Put $e_0 := e_0(k)$. Let n be an integer $\geqslant 0$ with $p \mid n$.*

(i) *The map $h^{-1,n}$ induces an isomorphism*

$$\mathbb{G}_m/p \otimes \overline{U}^n \xrightarrow{\simeq} \begin{cases} H^2(-, \mu_p^{\otimes 2}), & \text{if } n \leqslant pe_0,\\ 0, & \text{otherwise.}\end{cases}$$

(ii) *For $m = 0$ or pe_0, the map $h^{m,n}$ induces an isomorphism*

$$\overline{U}^m \otimes \overline{U}^n \xrightarrow{\simeq} \begin{cases} H^2(-, \mu_p^{\otimes 2}), & \text{if } m+n < pe_0,\\ 0, & \text{otherwise.}\end{cases}$$

Let n be a *positive* integer with $p \mid n$ and K/k a finite field extension with ramification index $e := e(K/k)$. From now on, we investigate the Galois symbol map

$$h := h_K^{0,n} : \left(\overline{U}^0 \otimes \overline{U}^n\right)(K) \to H^2(K, \mu_p^{\otimes 2}).$$

We basically follow the proof of Lemma 4.2.1 in [9] and proceed the steps below to show the injectivity of h:

Step 1. For any symbol of the form $\{a,b\}_{K/K} \in \left(\overline{U}^0 \otimes \overline{U}^n\right)(K)$, if $h(\{a,b\}_{K/K}) = 0$ then $\{a,b\}_{K/K} = 0$. (Prop. 3.7)

Step 2. The map h is injective on the subgroup of $\left(\overline{U}^0 \otimes \overline{U}^n\right)(K)$ generated by symbols of the form $\{a,b\}_{K/K}$. (Prop. 3.10)

Step 3. $\left(\overline{U}^0 \otimes \overline{U}^n\right)(K)$ is generated by symbols of the form $\{a,b\}_{K/K}$. (Prop. 3.11)

Proposition 3.7.

(i) *For any symbol $\{a,b\}_{K/K}$ in $\left(\overline{U}^0 \otimes \overline{U}^n\right)(K)$, if $h(\{a,b\}_{K/K}) = 0$, then we have $\{a,b\}_{K/K} = 0$.*

(ii) *For symbols of the form $\{a,b\}_{K/K}, \{a',b\}_{K/K}$ in $\left(\overline{U}^0 \otimes \overline{U}^n\right)(K)$ with $h(\{a,b\}_{K/K}) = h(\{a',b\}_{K/K})$, we have $\{a,b\}_{K/K} = \{a',b\}_{K/K}$.*

Proof. (i) Take a symbol $\{a,b\}_{K/K}$ in $\left(\overline{U}^0 \otimes \overline{U}^n\right)(K)$ and assume $h(\{a,b\}_{K/K}) = 0$. The symbol map is written by the Hilbert symbol $h(\{a,b\}_{K/K}) = (a,b)_K$ as in (3) and thus a is in the image of the norm $N_{L/K} : \overline{U}^0_L \to \overline{U}^0_K$ for $L = K(\sqrt[p]{b})$ ([2], Chap. IV, Prop. 5.1). Take $\alpha \in \overline{U}^0_L$ such that $N_{L/K}(\alpha) = a$. We obtain

$$\{a,b\}_{K/K} = \{N_{L/K}(\alpha), b\}_{K/K} = \{\alpha, \mathrm{Res}_{L/K}(b)\}_{L/K} = 0$$

by the condition (PF) in the definition of the Mackey product (Def. 2.2).

(ii) Suppose $h(\{a,b\}_{K/K}) = h(\{a',b\}_{K/K})$ and thus $h(\{a(a')^{-1},b\}_{K/K}) = 0$. From (i) we obtain $\{a(a')^{-1},b\}_{K/K} = 0$. Therefore we get $\{a,b\}_{K/K} = \{a',b\}_{K/K}$. ■

Now we *assume* $n < pe_0$ and introduce subgroups $S(K)$ and $T(K)$ of $\left(\overline{U}^0 \otimes \overline{U}^n\right)(K)$ as follows:

$S(K) :=$ subgroup generated by symbols of the form $\{a,b\}_{K/K}$ in $\left(\overline{U}^0 \otimes \overline{U}^n\right)(K)$,

$T(K) :=$ subgroup generated by symbols $\{a,b\}_{K/K} \in S(K)$ for $a \in \overline{U}_K^{pe_0(K)-ne-1}$.

Lemma 3.8. *Using the above notation, we have* $S(K) = T(K)$.

Proof. Define a filtration of $S(K)$ by

$$S^i(K) := \text{subgroup generated by symbols } \{a,b\}_{K/K} \in S(K) \text{ for } a \in \overline{U}^i_K.$$

By the very definition, we have $S(K) = S^0(K)$ and $T(K) = S^{pe_0(K)-ne-1}(K)$. It is enough to show $S^i(K) = S^{i+1}(K)$ for i with $0 \leqslant i < pe_0(K) - ne - 1$.

Fix a uniformizer π of K. Take a symbol $\xi = \{1 + u\pi^s, 1 + v\pi^t\}_{K/K} \in S^i(K)$ with $u, v \in \mathcal{O}_K^\times$, $s \geqslant i, t \geqslant ne$. To show $\xi \in S^{i+1}(K)$ we may assume $s = i$. We may also assume s and t are prime to p (Lemma 3.1) and $s+t \leqslant pe_0(K)$ (Lem. 3.4 and Lem. 3.7). From Proposition 3.7, Lemma 3.5(i) and Lemma 3.4 we have the following equalities:

$$\begin{aligned}
\xi &= \{1 + u\pi^i, 1 + v\pi^t\}_{K/K} \\
&= c\{1 + u\pi^i, 1 + v'\pi^{pe_0(K)-i}\}_{K/K} \quad \text{(for some } c \text{ and } v' \in \mathcal{O}_K^\times\text{)} \\
&= c\{1 + \eta\pi^i, 1 + v'\pi^{pe_0(K)-i}\}_{K/K} \quad \text{(for } u = \eta u_1 \in \mathcal{O}_K^\times \\
&\qquad\qquad\qquad\qquad\qquad\qquad \text{with } \eta \in \mu_{q-1}(K) \text{ and } u_1 \in U_K^1\text{)},
\end{aligned}$$

where $q := \#\mathbb{F}_K$. Since $i = s$ is prime to p and we have inequalities

$$i + 2(pe_0(K) - i - 1) > pe_0(K) + ne - 1 \geqslant pe_0(K) + p - 1$$

(recall $p \mid n$ and $n > 0$), one can apply Lemma 3.5(iii) so that there exists a non-zero symbol $\{1 + \eta\pi^i, 1 + v''\pi^{pe_0(K)-i-1}\}_{K/K}$ for some unit $v'' \in \mathcal{O}_K^\times$. From

Proposition 3.7(ii) we have

$$\{1+\eta\pi^i, 1+v'\pi^{pe_0(K)-i}\}_{K/K} \\ = c'\{1+\eta\pi^i, 1+v''\pi^{pe_0(K)-i-1}\}_{K/K} \quad (\text{for some } c' \in \mathbb{Z}).$$

Now we suppose $p \nmid i+1$. From Proposition 3.5(i) again we have

$$\{1+\eta\pi^i, 1+v''\pi^{pe_0(K)-i-1}\}_{K/K} \\ = c''\{1+u'\pi^{i+1}, 1+v''\pi^{pe_0(K)-i-1}\}_{K/K} \quad (\text{for some } u' \in \mathcal{O}_K^\times \text{ and some } c'').$$

Thus $\xi \in S^{i+1}(K)$. In the case of $p \mid i+1$, we have $\overline{U}_K^{pe_0(K)-(i+1)} = \overline{U}_K^{pe_0(K)-(i+2)}$ (Lem. 3.1). Therefore, the same computations as above give

$$\{1+\eta\pi^i, 1+v''\pi^{pe_0(K)-i-1}\}_{K/K} \\ = \{1+\eta\pi^i, 1+v'''\pi^{pe_0(K)-i-2}\}_{K/K} \quad (\text{for some } v''' \in \mathcal{O}_K^\times) \\ = c''\{1+u'\pi^{i+2}, 1+v'''\pi^{pe_0(K)-i-2}\}_{K/K} \quad (\text{for some } u' \in \mathcal{O}_K^\times \text{ and some } c'').$$

Hence we obtain $S^i(K) = S^{i+1}(K)$. ■

Define a bilinear map of $\mathbb{F}_p$-vector spaces

$$\Phi : \mathbb{F}_K \times \mathbb{F}_K \to S(K); (a,b) \mapsto \{1+\widetilde{a}\pi^{pe_0(K)-ne-1}, 1+\widetilde{b}\pi^{ne+1}\}_{K/K},$$

where $\widetilde{a}, \widetilde{b} \in \mathcal{O}_K$ are lifts of a, b respectively. The map Φ is well-defined (Lem. 3.4, Prop. 3.7(i)). Take a non-zero single symbol $\{a,b\}_{K/K} \in T(K)$ with $a \in \overline{U}_K^{pe_0(K)-ne-1}, b \in \overline{U}_K^{ne+1} = \overline{U}^n(K)$. If $a \in \overline{U}_K^{pe_0(K)-ne}$ or $b \in \overline{U}_K^{ne+2}$, then $(a,b)_K = 0$ (Lem. 3.4) and this contradicts with $\{a,b\}_{K/K} \neq 0$ by Lemma 3.7(i). Thus $a \in \overline{U}_K^{pe_0(K)-ne-1} \setminus \overline{U}_K^{pe_0(K)-ne}, b \in \overline{U}_K^{ne+1} \setminus \overline{U}_K^{ne+2}$ and there exist $\overline{a}, \overline{b} \in \mathbb{F}_K$ such that $\{a,b\}_{K/K} = \Phi(\overline{a}, \overline{b})$. From Lemma 3.8, any single symbol in $S(K)$ can be written as $\Phi(a,b)$ for some $a, b \in \mathbb{F}_K$ so that any non-zero element in $S(K)$, that is, a finite sum of symbols, can be written as $\sum_i \Phi(a_i, b_i)$ for some $a_i, b_i \in \mathbb{F}_K$. We also define

$$\Psi := h \circ \Phi : \mathbb{F}_K \times \mathbb{F}_K \to H^2(K, \mu_p^{\otimes 2}).$$

Lemma 3.9. *If $\Psi(a,b) = \Psi(c,d)$ for $a,b,c,d \in \mathbb{F}_K$, then $\Phi(a,b) = \Phi(c,d)$.*

Proof. Put $\alpha = \Psi(a,b) = \Psi(c,d)$ and we may assume $\alpha \neq 0$ by Proposition 3.7(i).

If $\{b,d\} \subset \mathbb{F}_K$ are linearly dependent in $\mathbb{F}_K$ (as an $\mathbb{F}_p$-vector space), then $sb = d$ for some $s \in \mathbb{F}_p$ ($s \neq 0$). From $\Psi(a,b) = \Psi(c,d) = s\Psi(c,b) = \Psi(sc,b)$, we have $\Phi(a,b) = \Phi(sc,b) = \Phi(c,d)$ by Proposition 3.7(ii).

When $\{b,d\} \subset \mathbb{F}_K$ are linearly independent, we define non-zero homomorphisms $\psi_b, \psi_d : \mathbb{F}_K \to H^2(K, \mu_p^{\otimes 2})$ by $\psi_b(x) = \Psi(x,b), \psi_d(x) = \Psi(x,d)$. These are linearly independent. In fact, if we assume $\psi_b = s\psi_d$ for some constant s then, for any $x \in \mathbb{F}_K$, $\psi_b(x) = s\psi_d(x)$ and thus $\Psi(x, b-sd) = 0$. Take a generator

$1+\rho\pi^{pe_0(K)} \in \overline{U}_K^{pe_0(K)}$ with $\rho \in \mathcal{O}_K^\times$ and denote the reduction of ρ to $\mathbb{F}_K$ by $r \in \mathbb{F}_K$. Since $u := b - sd \neq 0$, the calculations of symbols as in the proof of Lemma 3.5(i) give

$$0 = \Psi(ru^{-1}, u) = (1+\rho\widetilde{u}^{-1}\pi^{pe_0(K)-ne-1}, 1+\widetilde{u}\pi^{ne+1})_K = (1+\rho\pi^{pe_0(K)}, \pi)_K.$$

This contradicts with $(1+\rho\pi^{pe_0(K)}, \pi)_K \neq 0$. Thus ψ_b and ψ_d are linearly independent. One can find $x \in \mathbb{F}_K$ such that $\psi_b(x) = \psi_d(x) = \alpha$. Putting $y := d$, we have

$$\alpha = \Psi(a,b) = \Psi(x,b) = \Psi(x,y) = \Psi(c,y) = \Psi(c,d).$$

From these equalities and Proposition 3.7(i), we obtain

$$\Phi(a,b) - \Phi(c,d) = \Phi(a-x,b) + \Phi(x,b-y) + \Phi(x-c,y) + \Phi(c,y-d) = 0. \quad \blacksquare$$

Proposition 3.10. *Let K be a finite field extension of k, and n an integer with $p \mid n$ and $0 < n < pe_0(K)$. Then, the Galois symbol map h is injective on $S(K)$.*

Proof. Take a non-zero symbol $\Phi(a_0, b_0) \in S(K)$. By Proposition 3.7(i), it is enough to show that $S(K)$ is generated by the symbol $\Phi(a_0, b_0)$. Since $\Psi(a_0, b_0)$ is a generator of $H^2(K, \mu_p^{\otimes 2})$, for any non-zero element $\xi = \sum_{i=1}^n \Phi(a_i, b_i) \in S(K)$, there exists c_i such that $\Psi(a_i, b_i) = c_i \Psi(a_0, b_0)$ for each i. By Lemma 3.9, $\Phi(a_i, b_i) = \Phi(c_i a_0, b_0) = c_i \Phi(a_0, b_0)$ for all i and hence $\xi = (\sum_{i=1}^n c_i)\Phi(a_0, b_0)$. $\blacksquare$

Proposition 3.11. *Let K be a finite field extension of k, and n an integer with $p \mid n$ and $0 < n < pe_0(K)$. Then, we have $S(K) = \left(\overline{U}^0 \otimes \overline{U}^n\right)(K)$.*

Proof. Take a symbol $\{a,b\}_{L/K} \in \left(\overline{U}^0 \otimes \overline{U}^n\right)(K)$ and we have to prove that the symbol $\{a,b\}_{L/K}$ is in $S(K)$.

(a) Reduce to the case of a Galois extension L/K: First we assume that this claim holds for all Galois extensions, namely, for any finite extension K/k and any symbol $\{a', b'\}_{K'/K} \in \left(\overline{U}^0 \otimes \overline{U}^n\right)(K)$ where K'/K is a finite Galois extension, we have $\{a', b'\}_{K'/K} \in S(K)$.

Let M be the Galois closure of L/K. The Galois symbol maps are compatible with norm maps as in the following commutative diagram:

$$\begin{array}{ccc} \left(\overline{U}^0 \otimes \overline{U}^n\right)(M) & \xrightarrow{h_M^{0,n}} & H^2(M, \mu_p^{\otimes 2}) \\ \Big\downarrow{\scriptstyle N_{M/L}} & & \Big\downarrow{\scriptstyle \mathrm{Cor}_{M/L}} \\ \left(\overline{U}^0 \otimes \overline{U}^n\right)(L) & \xrightarrow{h_L^{0,n}} & H^2(L, \mu_p^{\otimes 2}). \end{array}$$

Since the corestriction map $\mathrm{Cor}_{M/L} : H^2(M, \mu_p^{\otimes 2}) \to H^2(L, \mu_p^{\otimes 2})$ on the Galois cohomology groups is bijective ([8] Lem. 5.8) and the Galois symbol map $h_M^{0,n}$ are

surjective (Lem. 3.4), one can find a symbol $\{\alpha,\beta\}_{M/M} \in S(M)$ such that

$$\begin{aligned} h_L^{0,n}(\{a,b\}_{L/L}) &= \mathrm{Cor}_{M/L} \circ h_M^{0,n}(\{\alpha,\beta\}_{M/M}) \\ &= h_L^{0,n} \circ N_{M/L}(\{\alpha,\beta\}_{M/M} = h_L^{0,n}(\{\alpha,\beta\}_{M/L}). \end{aligned}$$

Since M/L is Galois, $\{\alpha,\beta\}_{M/L} \in S(L)$ and thus $\{a,b\}_{L/L} = \{\alpha,\beta\}_{M/L}$ by Prop. 3.10. From the equalities

$$\{a,b\}_{L/K} = N_{L/K}(\{a,b\}_{L/L}) = N_{L/K}(\{\alpha,\beta\}_{M/L}) = \{\alpha,\beta\}_{M/K}$$

and the extension M/K is Galois, we obtain $\{a,b\}_{L/K} \in S(K)$. Therefore, without loss of generality, we may suppose L/K is a finite Galois extension and show $\{a,b\}_{L/K} \in S(K)$.

(b) *The case* $p \nmid e(L/K)$. In this extension, the norm map $N_{L/K} : \overline{U}_L^0 \to \overline{U}_K^0$ is surjective. There exist $\gamma \in \overline{U}_L^0$ and $d \in \overline{U}_K^{ne}$ such that $\{N_{L/K}(\gamma), d\}_{K/K}$ is a generator of $S(K)$. By the projection formula (PF), we have

$$\{N_{L/K}(\gamma), d\}_{K/K} = \{\gamma, \mathrm{Res}_{L/K}(d)\}_{L/K} = N_{L/K}(\{\gamma, \mathrm{Res}_{L/K}(d)\}_{L/L}).$$

Since the symbol $\{\gamma, \mathrm{Res}_{L/K}(d)\}_{L/L}$ is also a generator of $S(L)$, we obtain

$$\{a,b\}_{L/K} = N_{L/K}(\{a,b\}_{L/L}) = N_{L/K}(i\{\gamma, \mathrm{Res}_{L/K}(d)\}_{L/L}) = i\{N_{L/K}(\gamma), d\}_{K/K}$$

for some i. Hence $\{a,b\}_{L/K}$ is in $S(K)$.

(c) *The case* $p \mid e(L/K)$. By taking the maximal tamely ramified extension $K \subset K' \subset L$ in L/K, we have $\{a,b\}_{L/K} = N_{K'/K}(\{a,b\}_{L/K'})$. From the above arguments (b) again, we may assume that L/K is totally ramified Galois extension with $[L:K] = p^s$.

Take a finite sub extension K' of K_p/K, where K_p is the fixed field of the p-Sylow subgroup of G_k and put $L' = LK'$. As in (b), there exists $\alpha \in \overline{U}_{L'}^0$ such that $N_{L'/L}(\alpha) = a$. Therefore,

$$\begin{aligned} \{a,b\}_{L/K} &= \{N_{L'/L}(\alpha), b\}_{L/K} \\ &= \{\alpha, \mathrm{Res}_{L'/L}(b)\}_{L'/K} \\ &= N_{K'/K}\{\alpha, \mathrm{Res}_{L'/L}(b)\}_{L'/K'}. \end{aligned}$$

Choosing K' large enough, we may also assume $e(K/k) > 1$.

We prove $\{a,b\}_{L/K} \in S(K)$ for a finite extension K/k with $e(K/k) > 1$ and L/K is a totally ramified Galois extension with $[L:K] = p^s$ by induction on s.

If $s = 0$, there is nothing to show. So we assume $s > 0$. There exists an intermediate field M of L/K such that L/M is a cyclic extension of degree p. (The subfield M exists since the Galois group $\mathrm{Gal}(L/K)$ is solvable.) There exists an element $d \in \overline{U}^n(M) = \overline{U}_M^{ne(M/k)}$ such that $\Sigma = M(\sqrt[p]{d})$ is a totally ramified nontrivial extension of M and $\Sigma \neq L$. In fact, if the element d is in $\overline{U}_M^i \smallsetminus \overline{U}_M^{i+1}$

$(ne(M/k) < i < pe_0(M), p \nmid i)$ then the upper ramification subgroups of $G := \mathrm{Gal}(\Sigma/M)$ ([11], Chap. IV) is known to be

$$G = G^0 = G^1 = \cdots = G^{pe_0(M)-i} \supset G^{pe_0(M)-i+1} = \{1\}$$

(Lem. 3.2, see also [11], Chap. V, Sect. 3). Hence we can choose d such that the ramification break of Σ/M is different[1] from that of L/M. Using the element d, there exists $c \in \overline{U}^0_M$ such that $\{c, d\}_{M/M} \neq 0$. By local class field theory, we have $U^0_M = N_{L/M}U^0_L \cdot N_{\Sigma/M}U^0_\Sigma$. Therefore, one can find $\gamma \in U^0_L$ and $\gamma' \in U^0_\Sigma$ with $c = N_{K/M}(\gamma)N_{\Sigma/M}(\gamma')$. Since $\{N_{\Sigma/M}(\gamma'), d\}_{M/M} = \{\gamma', \mathrm{Res}_{\Sigma/M}(d)\}_{\Sigma/M} = 0$, we obtain

$$\begin{aligned}\{c, d\}_{M/M} &= \{N_{\Sigma/M}(\gamma'), d\}_{M/M} + \{N_{L/M}(\gamma), d\}_{M/M} \\ &= N_{L/M}(\{\gamma, \mathrm{Res}_{L/M}(d)\}_{L/L}).\end{aligned}$$

In particular, $\{\gamma, \mathrm{Res}_{L/M}(d)\}_{K/K} \neq 0$. Therefore, there exists i such that

$$\begin{aligned}\{a, b\}_{L/K} &= N_{L/K}(\{a, b\}_{L/L}) \\ &= N_{M/K} \circ N_{L/M}(\{\gamma^i, \mathrm{Res}_{L/M}(d)\}_{L/L}) \\ &= N_{M/K}(\{\gamma^i, \mathrm{Res}_{L/M}(d)\}_{L/M}) \\ &= N_{M/K}(\{N_{L/M}(\gamma^i), d\}_{M/M}) \\ &= \{N_{L/M}(\gamma^i), d\}_{M/K}.\end{aligned}$$

By the induction hypothesis, the last symbol $\{N_{L/M}(\gamma^i), d\}_{M/K}$ is in $S(K)$. ■

Proof of Thm. 3.6. The proof of (i) is basically same as in (ii) and much easier so that we show the assertion (ii) only. For any finite extension K/k with ramification index e, we prove that the Galois symbol map gives isomorphisms

$$h := h^{m,n}_K : \left(\overline{U}^m \otimes \overline{U}^n\right)(K) \xrightarrow{\simeq} \begin{cases} H^2(K, \mu_p^{\otimes 2}), & \text{if } m + n < pe_0, \\ 0, & \text{otherwise.} \end{cases} \tag{4}$$

(a) The case $m = pe_0$: We show $\left(\overline{U}^{pe_0} \otimes \overline{U}^n\right)(K) = 0$. For any symbol $\{a, b\}_{L/K}$ in $\left(\overline{U}^{pe_0} \otimes \overline{U}^n\right)(K)$, we have $N_{L/K}(\{a, b\}_{L/L}) = \{a, b\}_{L/K}$. Thus it is enough to show $\{a, b\}_{K/K} = 0$ with $a \neq 1$. Since the extension $L = K(\sqrt[p]{a})$ is unramified and of degree p (Lem. 3.2), the norm map $N_{L/K} : \overline{U}^n(L) \to \overline{U}^n(K)$ is surjective ([11], Chap. V, Sect. 2, Prop. 3). By the projection formula (PF),

$$\{a, b\}_{K/K} = \{a, N_{L/K}(\beta)\}_{K/K} = \{\mathrm{Res}_{L/K}(a), \beta\}_{L/K} = 0$$

for some $\beta \in \overline{U}^n(L)$.

(b) The case $m = 0$ and $n \geqslant pe_0$: From the norm arguments, it is enough to show $\{a, b\}_{K/K} = 0$ for any symbol $\{a, b\}_{K/K} \in (\overline{U}^0 \otimes \overline{U}^n)(K)$. Since $e_0(K) = e_0 e$

and $\overline{U}^n(K) = \overline{U}_K^{ne}$, Lemma 3.4 implies $h(\{a,b\}_{K/K}) = 0$. The required assertion $\{a,b\}_{K/K} = 0$ follows from Proposition 3.7(i).

(c) The case $m = 0$ and $n < pe_0$: From Lemma 3.3, we may assume $n > 0$. Lemma 3.4(iii) implies that $h = h_K^{0,n}$ is surjective. Since h is injective on $S(K)$ (Prop. 3.10) and we have $S(K) = (\overline{U}^0 \otimes \overline{U}^n)(K)$ (Prop. 3.11), the symbol map h is injective. ■

4. Galois symbol map for elliptic curves

Let k be a finite field extension of $\mathbb{Q}_p$ and put $e_0 = v_k(p)/(p-1)$ as in the last section.

Theorem 4.1. *Let n be an integer $\geqslant 1$. Let E_1, E_2 be elliptic curves over k with $E_i[p^n] \subset E_i(k)$ for $i = 1, 2$. Assume that E_1 has good ordinary reduction or split multiplicative reduction, and E_2 has good reduction or split multiplicative reduction. Then the Galois symbol map*

$$h_{p^n} : K(k; E_1, E_2)/p^n \to H^2(k, E_1[p^n] \otimes E_2[p^n])$$

is injective.

Proof. Consider the following diagram with exact rows:

$$\begin{array}{ccccc} K(k;E_1,E_2)/p^{n-1} & \longrightarrow & K(k;E_1,E_2)/p^n & \longrightarrow & K(k;E_1,E_2)/p \\ \downarrow{\scriptstyle h_{p^{n-1}}} & & \downarrow{\scriptstyle h_{p^n}} & & \downarrow{\scriptstyle h_p} \\ H^2(k,E_1[p^{n-1}]\otimes E_2[p^{n-1}]) & \longrightarrow & H^2(k,E_1[p^n]\otimes E_2[p^n]) & \longrightarrow & H^2(k,E_1[p]\otimes E_2[p]). \end{array}$$

The assumption $E_i[p^n] \subset E_i(k)$ implies the injectivity of the left lower map $H^2(k, E_1[p^{n-1}] \otimes E_2[p^{n-1}]) \to H^2(k, E_1[p^n] \otimes E_2[p^n])$. By induction on n, the assertion follows from the case of $n = 1$. More strongly we show that the Galois symbol map on the Mackey product

$$h : (E_1 \otimes E_2)(k)/p \to H^2(k, E_1[p] \otimes E_2[p])$$

is injective.

We recall the following results on the image of the Kummer map $h^1 : E(k) \to H^1(k, E[p])$ for an elliptic curve E over k ([5], see also [15], Rem. 3.2). Assume $E[p] \subset E(k)$ and choose an isomorphism of the Galois modules $E[p] \simeq (\mu_p)^{\oplus 2}$ which maps $E[p]^0$ onto the first factor μ_p, where $E[p]^0$ is the subgroup of $E[p]$ consisting of $\overline{k}$-valued points of the maximal connected finite flat p-torsion subgroup scheme of the Néron model of E. From the isomorphism, we can identify $H^1(k, E[p])$ and $(k^\times/p)^{\oplus 2}$. On the latter group $k^\times/p$, the higher unit groups $U_k^m = 1 + \mathfrak{m}_k^m$ induce a filtration $\overline{U}_k^m := \mathrm{Im}(U_k^m \to k^\times/p)$ as noted in the last section.

In terms of this filtration, the image of $h^1 : E(k)/p \hookrightarrow H^1(k, E[p]) = (k^\times/p)^{\oplus 2}$ is written precisely as follows (cf. [15]):

$$\mathrm{Im}(h^1) = \begin{cases} \overline{U}_k^{p(e_0-t_0)} \oplus \overline{U}_k^{pt_0}, & \text{if } E \text{ has good reduction,} \\ k^\times/p \oplus 1, & \text{if } E \text{ has split multiplicative reduction,} \end{cases} \tag{5}$$

where $t_0 := t_0(E) \in \mathbb{Z}$ with $0 < t_0 \leqslant e_0$ (It is calculated from the theory of the canonical subgroup of Katz-Lubin, cf. [3], Thm. 3.5).

Fix isomorphisms of Galois modules $E_1[p] \simeq \mu_p^{\oplus 2}$ and $E_2[p] \simeq \mu_p^{\oplus 2}$ as above. From the isomorphisms we can identify $H^1(-, E_1[p]) \simeq (\mathbb{G}_m/p)^{\oplus 2}$ and $H^1(-, E_2[p]) \simeq (\mathbb{G}_m/p)^{\oplus 2}$.

(a) *E_1 has split multiplicative reduction*: Consider the case that E_1 has split multiplicative reduction. We also assume that E_2 has good reduction. The other case on E_2 is treated in the same way and much easier. From (5), the Kummer maps on E_1 and E_2 induces isomorphisms

$$E_1/p \xrightarrow{\simeq} \mathbb{G}_m/p, \qquad E_2/p \xrightarrow{\simeq} \overline{U}^{p(e_0-t_0)} \oplus \overline{U}^{pt_0},$$

where $t_0 := t_0(E_2)$. Therefore $E_1/p \otimes E_2/p \simeq (\mathbb{G}_m/p \otimes \overline{U}^{p(e_0-t_0)}) \oplus (\mathbb{G}_m/p \otimes \overline{U}^{pt_0})$. The Galois symbol map h commutes with the maps $h^{-1,p(e_0-t_0)}$ and h^{-1,pt_0} defined in the last section and the injectivity of h follows from Theorem 3.6(i).

(b) *E_1 has good ordinary reduction*: Next we assume that E_1 has good ordinary reduction and E_2 has good reduction. In this case also, by (5), we have

$$E_1/p \xrightarrow{\simeq} \overline{U}^0 \oplus \overline{U}^{pe_0}, \qquad E_2/p \xrightarrow{\simeq} \overline{U}^{p(e_0-t_0)} \oplus \overline{U}^{pt_0},$$

where $t_0 := t_0(E_2)$. We have to show that the induced Galois symbol maps on

$$\overline{U}^0 \otimes \overline{U}^{p(e_0-t_0)}, \quad \overline{U}^0 \otimes \overline{U}^{pt_0}, \quad \overline{U}^{pe_0} \otimes \overline{U}^{p(e_0-t_0)}, \quad \text{and} \quad \overline{U}^{pe_0} \otimes \overline{U}^{p(e_0-t_0)}$$

are injective. This follows from Theorem 3.6(ii). ∎

Proposition 4.2. *Let n be an integer $\geqslant 1$ and q an integer $\geqslant 3$. Let $E_1, \ldots, E_q$ be elliptic curves over k. Assume that $E_i[p] \subset E_i(k)$ for $1 \leqslant i \leqslant 3$, E_1 has good ordinary reduction or split multiplicative reduction, and E_i has good reduction or split multiplicative reduction for $i = 2, 3$. Then, we have*

$$K(k; E_1, \ldots, E_q)/p^n = 0.$$

Proof. By considering the exact sequence

$$(E_1 \otimes E_2 \otimes E_3)(k)/p^{n-1} \to (E_1 \otimes E_2 \otimes E_3)(k)/p^n \to (E_1 \otimes E_2 \otimes E_3)(k)/p,$$

it is enough to show $(E_1 \otimes E_2 \otimes E_3)(k)/p = 0$. We show only the case E_1 has good ordinary reduction and E_i has good reduction for each $i = 2, 3$. As in the above proof of Theorem 4.1, we have

$$E_1/p \xrightarrow{\simeq} \overline{U}^0 \oplus \overline{U}^{pe_0}, \qquad E_i/p \xrightarrow{\simeq} \overline{U}^{p(e_0-t_0(E_i))} \oplus \overline{U}^{pt_0(E_i)} \qquad (i = 2, 3),$$

By Theorem 3.6,

$$\overline{U}^0 \otimes \overline{U}^{p(e_0 - t_0(E_2))} \simeq \overline{U}^0 \otimes \overline{U}^{pt_0(E_2)} \simeq \mathbb{G}_m/p \otimes \mathbb{G}_m/p.$$

Hence the assertion follows from Lemma 3.3. ■

Remark 4.3. From the same arguments in the proof of Theorem 4.1, we obtain the injectivity of the Galois symbol map

$$h : K(k; \mathbb{G}_m, E)/p^n \to H^2(k, \mathbb{G}_m[p^n] \otimes E[p^n])$$

under the assumption $E[p^n] \subset E(k)$ for $n \geqslant 1$. As in [3] we can determine the image of the above h and have

$$K(k; \mathbb{G}_m, E)/p^n \simeq \begin{cases} \mathbb{Z}/p^n, & \text{if } E \text{ has multiplicative reduction,} \\ (\mathbb{Z}/p^n)^{\oplus 2}, & \text{if } E \text{ has good reduction.} \end{cases}$$

It is known that the Somekawa K-group $K(k; \mathbb{G}_m, E)$ is isomorphic to the homology group $V(E)$ of the complex

$$K_2(k(E)) \xrightarrow{\oplus \partial_P} \bigoplus_{P \in E\text{: closed points}} k(P)^\times \xrightarrow{\sum N_{k(P)/k}} k^\times.$$

By the class field theory of curves over local field ([10], [20]), we have $V(E)/p^n \simeq \pi_1(E)^{\mathrm{ab,geo}}_{\mathrm{tor}}/p^n$. Therefore, the above computations give the structure of $\pi_1(E)^{\mathrm{ab}}$.

References

[1] S. Bloch and K. Kato, *p-adic étale cohomology*, Inst. Hautes Études Sci. Publ. Math. (1986), 107–152.

[2] I. B. Fesenko and S. V. Vostokov, *Local fields and their extensions*, second ed., Translations of Mathematical Monographs, vol. 121, American Mathematical Society, Providence, RI, 2002, With a foreword by I. R. Shafarevich.

[3] T. Hiranouchi and S. Hirayama, *On the cycle map for products of elliptic curves over a p-adic field*, Acta Arith. **157** (2013), no. 2, 101–118.

[4] B. Kahn, *Nullité de certains groupes attachés aux variétés semi-abéliennes sur un corps fini; application*, C. R. Acad. Sci. Paris Sér. I Math. **314** (1992), no. 13, 1039–1042.

[5] M. Kawachi, *Isogenies of degree p of elliptic curves over local fields and Kummer theory*, Tokyo J. Math. **25** (2002), 247–259.

[6] A. Mattuck, *Abelian varieties over p-adic ground fields*, Ann. of Math. (2) **62** (1955), 92–119.

[7] J. Milnor, *Introduction to algebraic K-theory*, Princeton University Press, Princeton, N.J., 1971, Annals of Mathematics Studies, No. 72.

[8] J. Murre and D. Ramakrishnan, *Local Galois symbols on $E \times E$*, Motives and algebraic cycles, Fields Inst. Commun., vol. 56, Amer. Math. Soc., Providence, RI, 2009, pp. 257–291.

[9] W. Raskind and M. Spiess, *Milnor K-groups and zero-cycles on products of curves over p-adic fields*, Compositio Math. **121** (2000), 1–33.
[10] S. Saito, *Class field theory for curves over local fields*, J. Number Theory **21** (1985), no. 1, 44–80.
[11] J.-P. Serre, *Corps locaux*, Hermann, Paris, 1968, Deuxième édition, Publications de l'Université de Nancago, No. VIII.
[12] J. H. Silverman, *The arithmetic of elliptic curves*, Graduate Texts in Mathematics, vol. 106, Springer-Verlag, New York, 1986.
[13] M. Somekawa, *On Milnor K-groups attached to semi-abelian varieties*, K-Theory **4** (1990), no. 2, 105–119.
[14] M. Spiess and T. Yamazaki, *A counterexample to generalizations of the Milnor-Bloch-Kato conjecture*, J. K-Theory **4** (2009), no. 1, 77–90.
[15] T. Takemoto, *Zero-cycles on products of elliptic curves over p-adic fields*, Acta Arith. **149** (2011), no. 3, 201–214.
[16] J. Tate, *Relations between K_2 and Galois cohomology*, Invent. Math. **36** (1976), 257–274.
[17] C. Weibel, *The norm residue isomorphism theorem*, J. Topol. **2** (2009), 346–372.
[18] T. Yamazaki, *On Chow and Brauer groups of a product of Mumford curves*, Math. Ann. **333** (2005), 549–567.
[19] T. Yamazaki, *Milnor K-group attached to a torus and Birch-Tate conjecture*, Internat. J. Math. **20** (2009), no. 7, 841–857.
[20] T. Yoshida, *Finiteness theorems in the class field theory of varieties over local fields*, J. Number Theory **101** (2003), no. 1, 138–150.

Address: Toshiro Hiranouchi: Department of Mathematics, Graduate School of Science, Hiroshima University 1-3-1 Kagamiyama, Higashi-Hiroshima, 739-8526 Japan.

E-mail: hira@hiroshima-u.ac.jp

Received: 10 March 2015; **revised:** 19 August 2015

Functiones et Approximatio
54.1 (2016), 57–63
doi: 10.7169/facm/2016.54.1.5

MULTIPLES OF SQUARES IN SHORT INTERVALS

Joël Rivat, Igor E. Shparlinski

Abstract: We use the theory of exponent pairs and Vaaler polynomials to show that any interval of the form $[x, x + x^{1/2}]$ contains an integral multiple $m^2 r \in [x, x + x^{1/2}]$ of a perfect square m^2 with an integer $m > x^{0.281286}$.

Keywords: multiples of squares, short intervals, exponential sums.

1. Introduction

Clearly any interval of the form $[x, x + 2x^{1/2} + 1]$ with $x \geqslant 1$ contains a perfect integer square, while some shorter intervals do not. Furthermore, any interval of the form $[x, x + y]$ with real positive x and y contains an integral multiple $m^2 r$ of a perfect square m^2 with a positive integer $m \leqslant \lfloor y^{1/2} \rfloor$.

Here, in a wide range of relative sizes of sufficiently large positive x and y we show that any interval of the form $[x, x + y]$ contains an integral multiple $m^2 r$ of a perfect square m^2 with an integer $m = y^{\gamma + o(1)}$ with some fixed $\gamma > 1/2$. In particular, in the most interesting "borderline" case when $y = x^{1/2 + o(1)}$ one can take $\gamma = 346/615 = 0.5626\ldots$.

Our main tool is the theory of *exponent pairs*, we refer to [1, Chapter 3], [3, Sections 7.3 and 17.4], [5, Chapter 8] and [6, Chapter 3] for an exact definition, properties and examples of exponent pairs. Note that in the terminology of [5], which we accept here, an exponent pair (κ, λ) corresponds to the exponent pair $(\kappa, \lambda + 1/2)$ in the terminology of [1, 3, 6].

Throughout the paper, any implied constants in symbols O and $\ll$ may depend on the real positive parameter ε and are absolute otherwise. We recall that the notations $U = O(V)$ and $U \ll V$ are all equivalent to the statement that $|U| \leqslant cV$ holds with some constant $c > 0$. We also use $U \asymp V$ to denote that $U \ll V \ll U$. For a real $A \geqslant 1$ and an integer a we write $a \sim A$ to express that $A \leqslant a \leqslant 2A$.

2010 Mathematics Subject Classification: primary: 11N25

Theorem 1. *For real numbers x and y with $x^{1/2} > y > 1$ the interval $[x, x+y]$ contains an integral multiple $m^2 r \in [x, x+y]$ of a perfect square m^2 with an integer*

$$m = x^{-\alpha+o(1)} y^{\beta},$$

as $x \to \infty$, provided that $x^{\alpha} \leqslant y^{\beta}$, where

$$\alpha = \frac{2\kappa}{3+2\lambda-2\kappa} \qquad \text{and} \qquad \beta = \frac{2+2\kappa}{3+2\lambda-2\kappa},$$

for an arbitrary exponent pair (κ, λ).

We now immediately derive:

Corollary 2. *For an integer $N \geqslant 1$, for any fixed ϑ with $\alpha/\beta \leqslant \vartheta \leqslant 1$ there are integers*

$$1 \leqslant r \leqslant N^{1-2\beta\vartheta+2\alpha+o(1)} \qquad \text{and} \qquad 0 \leqslant s \leqslant N^{\vartheta}$$

as $N \to \infty$, such that $r(N+s)$ is a perfect square, where α and β are as in Theorem 1.

Indeed, we apply Theorem 1 with $x = N$ and $y = N^{\vartheta}$, thus the condition $x^{\alpha} \leqslant y^{\beta}$ is satisfied. Then, for m and r as in Theorem 1, we define s by the condition $s = m^2 r - N$, thus $r(N+s) = (mr)^2$. Furthermore, we have

$$x - N = 0 \leqslant s \leqslant x + y - N = N^{\vartheta}$$

and

$$1 \leqslant r \leqslant (x + x^{\vartheta})/m^2 \ll x/m^2 = x \left(x^{-\alpha+o(1)} y^{\beta}\right)^{-2} = N^{1-2\beta\vartheta+2\alpha+o(1)}.$$

Clearly, the result of Corollary 2 is nontrivial only for $\vartheta \leqslant 1/2$.

We remark that a somewhat related question about multiples of squares in short intervals, motivated by application to computer arithmetic, has been studied by Hanrot, Rivat, Tenenbaum and Zimmermann [2] via similar techniques.

2. Fractional parts and exponential sums

As usual, we define the function $\psi(u) = u - \lfloor u \rfloor - 1/2$, where $\lfloor u \rfloor$ is the integer part of a real u. By a result of Vaaler [7], see also [1, Theorem A.6].

Lemma 3. *For any integer $H \geqslant 1$ there is a trigonometric polynomial*

$$\psi_H(u) = \sum_{1 \leqslant |h| \leqslant H} \frac{a_h}{-2i\pi h} \mathbf{e}(hu)$$

for coefficients $a_h \in [0,1]$ and such that

$$|\psi(u) - \psi_H(u)| \leqslant \frac{1}{2H+2} \sum_{|h| \leqslant H} \left(1 - \frac{|h|}{H+1}\right) \mathbf{e}(hu).$$

As we have mentioned we combine Lemma 3 with the bounds of exponential sums based on the theory of exponent pairs, see [1, Chapter 3] or [5, Chapter 8]. In our case we apply it to the monomial functions $f(z) = A/z^2$ with $A \geqslant 1$ so that the condition [5, Equation (8.55)] is satisfied (with $F = A/N^2$). More precisely, we have:

Lemma 4. *Let (κ, λ) be an exponent pair. For any $A \geqslant M \geqslant N \geqslant 1$ with $N \sim M$ and such that $A \geqslant M^3$, we have*

$$\sum_{M \leqslant m < N} \mathbf{e}\left(\frac{A}{m^2}\right) \ll A^{\kappa + o(1)} M^{1/2 + \lambda - 3\kappa}$$

where the implied constant depends only on κ and λ.

Proof. First we note that for $f(z) = A/z^2$ on the interval $z \in [M, 2M]$ we have

$$F/M^{-j} \ll |f^{(j)}(z)| \ll F/M^{-j}$$

where $F = A/M^2$. Furthermore, for $\Lambda = FM^{-1} = A/M^{-3}$ we have $\Lambda \geqslant 1$, so the condition [5, Equation (8.56)] holds and thus by [5, Equation (8.55)] we have

$$\sum_{M \leqslant m < N} \mathbf{e}\left(\frac{A}{m^2}\right) \ll \Lambda^{\kappa} M^{1/2 + \lambda} A^{o(1)}.$$

After simple calculations we obtain the result. ∎

We also recall that given an exponent pair (κ, λ) one can produce a series of other pairs by applying, the so-called $\mathcal{A}$- and $\mathcal{B}$-processes, which in the terminology of [5, Section 8.4] can be written as

$$\mathcal{A}(\kappa, \lambda) = \left(\frac{\kappa}{2\kappa + 2}, \frac{\lambda + 1/2}{2\kappa + 2}\right) \qquad \text{and} \qquad \mathcal{B}(\kappa, \lambda) = (\lambda, \kappa)\,. \tag{1}$$

3. Proof of Theorem 1

For $1 \leqslant y \leqslant x$ and $M \in \mathbb{N}$ we consider the sum

$$S(x, y, M) = \sum_{m \sim M} \left(\left\lfloor \frac{x + y}{m^2} \right\rfloor - \left\lfloor \frac{x}{m^2} \right\rfloor\right).$$

Clearly, the positivity $S(x, y, M) > 0$ implies that there is $m \sim M$ with

$$m^2 \left(\left\lfloor \frac{x}{m^2} \right\rfloor + 1\right) \in [x, x + y].$$

Using the function $\psi(u)$ we write

$$S(x, y, M) = \sum_{m \sim M} \frac{y}{m^2} - \sum_{m \sim M} \left(\psi\left(\frac{x + y}{m^2}\right) - \psi\left(\frac{x}{m^2}\right)\right).$$

Using the Vaaler polynomials given in Lemma 3, for any integer $H \geqslant 1$ we can write

$$\left| S(x,y,M) - y \sum_{m \sim M} \frac{1}{m^2} \right| \leqslant E(x+y,M,H) + E(x,M,H) + |F(x,y,M,H)|,$$

where

$$E(z,M,H) = \sum_{m \sim M} \left| \psi\left(\frac{z}{m^2}\right) - \psi_H\left(\frac{z}{m^2}\right) \right|$$

and

$$F(x,y,M,H) = \sum_{m \sim M} \left(\psi_H\left(\frac{x+y}{m^2}\right) - \psi_H\left(\frac{x}{m^2}\right) \right).$$

We see from Lemma 3 that

$$E(z,M,H) \leqslant \frac{M}{2H+2} + \frac{1}{2H+2} \sum_{1 \leqslant |h| \leqslant H} \left(1 - \frac{|h|}{H+1}\right) \sum_{m \sim M} \mathbf{e}\left(\frac{hz}{m^2}\right) \tag{2}$$

and also

$$F(x,y,M,H) = \sum_{1 \leqslant |h| \leqslant H} \frac{a_h}{-2i\pi h} \sum_{m \sim M} \left(\mathbf{e}\left(\frac{hy}{m^2}\right) - 1 \right) \mathbf{e}\left(\frac{hx}{m^2}\right). \tag{3}$$

We have

$$\begin{aligned}
\left(\mathbf{e}\left(\frac{hy}{(m+1)^2}\right) - 1 \right) - \left(\mathbf{e}\left(\frac{hy}{m^2}\right) - 1 \right) &= \mathbf{e}\left(\frac{hy}{(m+1)^2}\right) - \mathbf{e}\left(\frac{hy}{m^2}\right) \\
&= \mathbf{e}\left(\frac{hy}{m^2}\right) \left(\mathbf{e}\left(\frac{hy}{(m+1)^2} - \frac{hy}{m^2}\right) - 1 \right) \\
&= \mathbf{e}\left(\frac{hy}{m^2}\right) \left(\mathbf{e}\left(\frac{-hy(2m+1)}{m^2(m+1)^2}\right) - 1 \right) \\
&= O\left(\frac{|h|y}{M^3}\right).
\end{aligned}$$

Hence, by partial summation, we derive from (3) that

$$F(x,y,M,H) \ll \frac{y}{M^2} \sum_{1 \leqslant |h| \leqslant H} \max_{N \sim M} \left| \sum_{M \leqslant m < N} \mathbf{e}\left(\frac{hx}{m^2}\right) \right|. \tag{4}$$

So, assuming that

$$M \leqslant x^{1/3}, \tag{5}$$

we see from (2), (4) and Lemma 4 that for any exponent pair (κ, λ) we have

$$S(x,y,M) - \frac{y}{2M} \ll \frac{M}{H} + \left(\frac{1}{H} + \frac{y}{M^2}\right) \sum_{1 \leqslant |h| \leqslant H} (|h|\, x)^{\kappa}\, M^{1/2+\lambda-3\kappa}.$$

Let us assume that we are in the interesting case $M \geqslant y^{1/2}$. We then fix some sufficiently small $\varepsilon > 0$ and set

$$H = \left\lceil \frac{M^2}{y} x^{\varepsilon} \right\rceil .$$

We then obtain

$$\begin{aligned} S(x,y,M) - \frac{y}{2M} &\ll \frac{y}{M} x^{-\varepsilon} + x^{(1+\kappa)\varepsilon} \left(\frac{x}{y}\right)^{\kappa} M^{1/2+\lambda-\kappa} \\ &\ll \frac{y}{M} x^{-\varepsilon} + x^{2\varepsilon} \left(\frac{x}{y}\right)^{\kappa} M^{1/2+\lambda-\kappa}. \end{aligned}$$

So we see that

$$S(x,y,M) - \frac{y}{2M} \ll \frac{y}{M} x^{-\varepsilon}$$

under the following sufficient condition:

$$\left(xy^{-1}\right)^{\kappa} M^{1/2+\lambda-\kappa} \ll \frac{y}{M} x^{-3\varepsilon}$$

that is,

$$M^{3/2+\lambda-\kappa} \ll x^{-\kappa} y^{1+\kappa} x^{-2\varepsilon}.$$

Since $\varepsilon > 0$ is arbitrary, we can take

$$M = x^{-\alpha+o(1)} y^{\beta}$$

to guarantee that $S(x,y,M) > 0$.

It remains to note that for the above choice of M, for $y \leqslant x^{1/2}$ we have

$$M \leqslant x^{-\alpha+\beta/2+o(1)} = x^{(1-\kappa)/(3+2\lambda-2\kappa)+o(1)}.$$

As we always have $\lambda, \kappa > 0$, the condition (5) holds and the result now follows.

4. Comments

Clearly, Theorem 1 improves the trivial result with $m \asymp y^{1/2}$ provided that

$$y > x^{4\kappa/(1+6\kappa-2\lambda)+\varepsilon}$$

for some fixed ε.

For $y = x^{1/2+o(1)}$ the result of Theorem 1 becomes

$$m = x^{(1-\kappa)/(3+2\lambda-2\kappa)+o(1)}.$$

Thus, for the classical exponent pair $(\kappa, \lambda) = (1/6, 1/6)$, which can be obtained from the pair $(1/2, 0)$ given by [5, Corollay 8.13] with the help of the transformations (1) as $\mathcal{AB}(0, 1/2) = (1/6, 1/6)$ we obtain $m = x^{5/18+o(1)}$. Alternatively, the

same value of m can also be obtained for $(\kappa, \lambda) = (2/7, 1/14) = \mathcal{BA}^2\mathcal{B}(0, 1/2)$. Notice that for using $(\kappa, \lambda) = (1/6, 1/6)$ it is sufficient to apply [1, Theorem 2.9], thus avoiding the use of the theory of exponent pairs. However using more complicated exponent pairs one can get slightly better results. For example, the pair $(9/56, 9/56)$, see [5, Equation (8.68)] (which cannot be obtained from $(0, 1/2)$ via the $\mathcal{A}$- and $\mathcal{B}$-processes) gives $m = x^{47/168+o(1)}$, while $(2/9, 1/9) = \mathcal{BAB}\mathcal{AB}\mathcal{A}^2\mathcal{B}(0, 1/2)$ gives $m = x^{7/25+o(1)}$. Furthermore, with a more complicated the choice

$$(\kappa, \lambda) = \left(\frac{32}{205}, \frac{32}{205}\right) \tag{6}$$

given by Huxley [4] for $y = x^{1/2+o(1)}$ we obtain

$$m = x^{173/615+o(1)}.$$

Note that the numerical differences between these estimates are really minor

$$\frac{5}{18} = 0.2777\ldots, \qquad \frac{47}{168} = 0.2797\ldots,$$
$$\frac{7}{25} = 0.2800\ldots, \qquad \frac{173}{615} = 0.2813\ldots.$$

It is quite possible that some other choices of (κ, λ) lead to a stronger bound. In fact, the algorithm given in [1, Chapter 5] may lead to an optimal choice within the pairs obtained via the $\mathcal{A}$- and $\mathcal{B}$-processes; we however do not expect any substantial numerical improvements. Indeed, by [6, Conjecture 2, Chapter 3], $(\varepsilon, \varepsilon)$ is an exponent pair for any $\varepsilon > 0$. This leads to $m = x^{1/3+o(1)}$ which is the limit of our approach.

Clearly, for any sufficiently large z there are at most

$$\sum_{m \geqslant M} \frac{z}{m^2} \ll z/M$$

multiples of squares $m^2 r \leqslant z$. Thus for any $y < z^{1/2}$ there is $x \in [z/2, z]$ such that the interval $[x, x + y]$ does not contain a multiple of m^2 for any $m \geqslant cy$, where $c > 0$ is an absolute constant.

We also remark, that taking

$$\vartheta = \frac{1 + 2\alpha}{1 + 2\beta}$$

in Corollary 2 balances the bounds on r and s and with the choice (6) leads to the bound $r, s \leqslant N^{743/1563+o(1)}$. This also suggests the following:

Question 5. *Given an integer N, obtain an upper bound on smallest values of positive integers u and v such that the linear transformation $uN + v$ is a perfect square.*

Note that Question 5 can be reformulated as a question about finding a bound U as a function of N so the congruence

$$m^2 \equiv v \pmod{N}$$

has a solution in positive integers $m \leqslant \sqrt{NU}$ and $v \leqslant U$. Using bounds of incomplete Gaussian sums, it is easy to show that one can take $U = N^{2/3+o(1)}$. It is certainly interesting to improve this bound.

We note that the same method works for multiples of higher powers. It can also be extended to multiples of many other functions such as, for example, $m(m+1)$. This flexibility of our approach may also be its main weakness as it does not use the arithmetic structure of squares.

Furthermore, it is not clear how to obtain a nontrivial result for the polynomial analogue of our question. Namely, given a monic polynomial $f \in \mathbb{F}_q[X]$ of degree d over a finite field $\mathbb{F}_q$ of q elements and a positive integer e, we ask what is the largest degree m of a polynomial g such that $\deg(f - g^2h) \leqslant e$ for some $h \in \mathbb{F}_q[X]$.

References

[1] S.W. Graham and G. Kolesnik, *Van der Corput's method of exponential sums*, Cambridge Univ. Press, 1991.

[2] G. Hanrot, J. Rivat, G. Tenenbaum and P. Zimmermann, *Density results on floating-point invertible numbers*, Theoret. Comput. Sci. **291** (2003), 135–141.

[3] M.N. Huxley, *Area, lattice points and exponential sums*, Oxford Univ. Press, 1996.

[4] M.N. Huxley, *Exponential sums and the Riemann zeta function, V*, Proc. London Math. Soc. **90** (2005), no. 1, 1–41.

[5] H. Iwaniec and E. Kowalski, *Analytic number theory*, Amer. Math. Soc., Providence, RI, 2004.

[6] H.L. Montgomery, *Ten lectures on the interface between analytic number theory and harmonic analysis*, Amer. Math. Soc., Providence, RI, 1994.

[7] J.D. Vaaler, *Some extremal functions in Fourier analysis*, Bull. Amer. Math. Soc. **12** (1985) 183–215.

Addresses: Joël Rivat: Institut de Mathématiques de Marseille, Université d'Aix-Marseille, 13288 Marseille, France;
Igor E. Shparlinski: Department of Pure Mathematics, University of New South Wales, Sydney, NSW 2052, Australia.

E-mail: joel.rivat@univ-amu.fr, igor.shparlinski@unsw.edu.au

Received: 19 April 2015; **revised:** 14 May 2015

Functiones et Approximatio
54.1 (2016), 65–72
doi: 10.7169/facm/2016.54.1.6

FINITE MORDELL-TORNHEIM MULTIPLE ZETA VALUES

Ken Kamano

Abstract: We investigate a finite analogue of the Mordell-Tornheim multiple zeta values (the finite Mordell-Tornheim multiple zeta values). These values can be expressed by a linear combination of finite multiple zeta values, and its rules are described by the shuffle product. As a corollary, we give a certain relation among finite multiple zeta values.

Keywords: Mordell-Tornheim multiple zeta values; finite multiple zeta values.

1. Introduction

The multiple zeta values are defined by

$$\zeta(k_1,\dots,k_r) := \sum_{\substack{m_1>\cdots>m_r>0\\ m_i\in\mathbb{Z}}} \frac{1}{m_1^{k_1}\cdots m_r^{k_r}}$$

for positive integers $k_1,\dots,k_r$ with $k_1 \geqslant 2$. The numbers $k := k_1+\cdots+k_r$ and r are called the weight and the depth of $\zeta(k_1,\dots,k_r)$, respectively. The case of depth 2 was studied by Euler, and general cases have been studied by many authors from 1990's. Many linear relations among multiple zeta values are known, and one of the goals of the study of multiple zeta values is to determine all such relations.

For positive integers $k_1,\dots,k_{r+1}$, the Mordell-Tornheim multiple zeta values are defined by

$$\zeta^{MT}(k_1,\dots,k_r;k_{r+1}) := \sum_{m_1,\dots,m_r\geqslant 1} \frac{1}{m_1^{k_1}\cdots m_r^{k_r}(m_1+\cdots+m_r)^{k_{r+1}}}. \tag{1}$$

These types of sums were first studied by Tornheim [10] and Mordell [6] and many relations are given. Tsumura proved that the value $\zeta^{MT}(k_1,\dots,k_r;k_{r+1})$ can be expressed as a rational linear combination of products of the Mordell-Tornheim multiple zeta values of lower depth than r, when its depth r and weight

2010 Mathematics Subject Classification: primary: 11M32

$k_1 + \cdots + k_{r+1}$ are of different parity. Note that Tornheim [10] proved this result for the case $r = 2$. Matsumoto [7] considered the function (1) as an $(r+1)$-variable complex function and proved that this function can be meromorphically continued to the whole $\mathbb{C}^{r+1}$ space.

Recently, Kaneko-Zagier introduced a finite analogue of multiple zeta values, called *finite multiple zeta values* (cf. [4]). Let $\mathcal{A} := \prod_p \mathbb{Z}/p\mathbb{Z} \,/ \bigoplus_p \mathbb{Z}/p\mathbb{Z}$ where p runs over all primes. The ring $\mathcal{A}$ naturally becomes $\mathbb{Q}$-algebra.

For positive integers $k_1, \ldots, k_r$, finite multiple zeta values are defined by

$$\zeta_{\mathcal{A}}(k_1, \ldots, k_r) := \left(\sum_{\substack{p > m_1 > \cdots > m_r > 0 \\ m_i \in \mathbb{Z}}} \frac{1}{m_1^{k_1} \cdots m_r^{k_r}} \right)_p \in \mathcal{A}.$$

From now on, we denote $(a_p)_p \in \mathcal{A}$ simply by a_p. Hence the definition above is written as

$$\zeta_{\mathcal{A}}(k_1, \ldots, k_r) = \sum_{\substack{p > m_1 > \cdots > m_r > 0 \\ m_i \in \mathbb{Z}}} \frac{1}{m_1^{k_1} \cdots m_r^{k_r}}.$$

Similar to the usual multiple zeta values, there are many relations among finite multiple zeta values. For example, the following identities are known.

Proposition 1.1 ([3]). *For any positive integers $k_1, \ldots, k_r$ and k, the following identities hold:*

1. $\zeta_{\mathcal{A}}(k, \ldots, k) = 0$,
2. $\zeta_{\mathcal{A}}(k_1, \ldots, k_r) = (-1)^{k_1 + \cdots + k_r} \zeta_{\mathcal{A}}(k_r, \ldots, k_1)$,
3. $\sum_{\sigma \in \mathfrak{S}_r} \zeta_{\mathcal{A}}(k_{\sigma(1)}, \ldots, k_{\sigma(r)}) = 0$ *where $\mathfrak{S}_r$ is the symmetric group of degree r.*

For other relations, see [2], [3], [8] and [9].

As a finite analogue of the Mordell-Tornheim multiple zeta values, we define the *finite Mordell-Tornheim multiple zeta values* by

$$\zeta_{\mathcal{A}}^{MT}(k_1, \ldots, k_r; k_{r+1}) := \sum_{\substack{m_1, \ldots, m_r > 0 \\ m_1 + \cdots + m_r < p}} \frac{1}{m_1^{k_1} \cdots m_r^{k_r} (m_1 + \cdots + m_r)^{k_{r+1}}} \in \mathcal{A}$$

for positive integers $k_1, \ldots, k_{r+1}$. It is clear that $\zeta_{\mathcal{A}}^{MT}(k_1, 0; k_3) = \zeta_{\mathcal{A}}(k_3, k_1)$.

Following Hoffman [2], we introduce the algebraic setup of finite multiple zeta values. Let $\mathfrak{H} := \mathbb{Q}\langle x, y \rangle$ be the non-commutative polynomial ring over $\mathbb{Q}$ in two indeterminates x and y, and $\mathfrak{H}^1$ its subring $\mathbb{Q} + \mathfrak{H}y$. The shuffle product ш on $\mathfrak{H}$ is a $\mathbb{Q}$-bilinear map $\mathfrak{H} \times \mathfrak{H} \to \mathfrak{H}$ satisfying

$$w ш 1 = 1 ш w = w, \qquad (u_1 w_1) ш (u_2 w_2) = u_1 (w_1 ш (u_2 w_2)) + u_2 ((u_1 w_1) ш w_2) \quad (2)$$

for $w, w_i \in \mathfrak{H}$ and $u_i = x$ or y $(i = 1, 2)$. We denote $x^{k-1}y$ by z_k for $k \geqslant 1$, and define the $\mathbb{Q}$-linear map $Z_{\mathcal{A}} : \mathfrak{H}^1 \to \mathcal{A}$ satisfying $Z_{\mathcal{A}}(z_{k_1} z_{k_2} \cdots z_{k_r}) = \zeta_{\mathcal{A}}(k_1, k_2, \ldots, k_r)$. For example, $Z_{\mathcal{A}}(x^2yxy) = Z_{\mathcal{A}}(z_3 z_2) = \zeta_{\mathcal{A}}(3, 2)$.

The finite Mordell-Tornheim multiple zeta values have the following expression.

Theorem 1.2. *For integers $k_1, \dots, k_r \geqslant 1$ and $l \geqslant 0$, the following identity holds:*

$$\zeta_{\mathcal{A}}^{MT}(k_1, \dots, k_r; l) = Z_{\mathcal{A}}(x^l(z_{k_1} ш \cdots ш z_{k_r})). \tag{3}$$

As a main result of the paper, we will prove this type of relation in a more general setting (see Theorem 2.1) and Theorem 1.2 is its special case. The right-hand side of (3) can be expressed by a linear combination of finite multiple zeta values, hence the finite Mordell-Tornheim multiple zeta values can be expressed by a linear combination of finite multiple zeta values.

2. Finite Mordell-Tornheim multiple zeta values and their generalization

For non-negative integers $k_1, \dots, k_i, l_i, \dots, l_r$ with $1 \leqslant i \leqslant r$, we define the function

$$T_{\mathcal{A}}((k_1, \dots, k_i); (l_i, \dots, l_r)) := \sum_{\substack{m_1, \dots, m_r \geqslant 1 \\ m_1 + \cdots + m_r \leqslant p-1}} \frac{1}{m_1^{k_1} \cdots m_i^{k_i} N_i^{l_i} N_{i+1}^{l_{i+1}} \cdots N_r^{l_r}} \in \mathcal{A},$$

where $N_k := m_1 + \cdots + m_k$ for $1 \leqslant k \leqslant r$. This function contains finite multiple zeta values and the finite Mordell-Tornheim multiple zeta values. Indeed, $T_{\mathcal{A}}((k_1); (0, l_2, \dots, l_r)) = \zeta_{\mathcal{A}}(l_r, \dots, l_2, k_1)$ and $T_{\mathcal{A}}((k_1, \dots, k_r); (l_r)) = \zeta_{\mathcal{A}}^{MT}(k_1, \dots, k_r; l_r)$.

The following is the main result of the present paper. Note that this theorem includes Theorem 1.2 because $T_{\mathcal{A}}((k_1, \dots, k_r); (l_r)) = \zeta_{\mathcal{A}}^{MT}(k_1, \dots, k_r; l_r)$ in the case $i = r$.

Theorem 2.1. *Let i and r be integers with $1 \leqslant i \leqslant r$. For integers $k_1, \dots, k_i \geqslant 1$, $l_i \geqslant 0$ and $l_{i+1}, \dots, l_r \geqslant 1$, we have*

$$T_{\mathcal{A}}((k_1, \dots, k_i); (l_i, \dots, l_r)) = Z_{\mathcal{A}}(z_{l_r} \cdots z_{l_{i+1}} x^{l_i}(z_{k_1} ш \cdots ш z_{k_i})).$$

In particular, the value $T_{\mathcal{A}}((k_1, \dots, k_i); (l_i, \dots, l_r))$ can be expressed by a linear combination of finite multiple zeta values of weight $\sum_{s=1}^{i} k_s + \sum_{t=i}^{r} l_t$.

Proof. We prove the theorem by induction on $k_1 + \cdots + k_i$. We first consider the case $(k_1, \dots, k_i) = (1, \dots, 1)$. By using the partial fraction decomposition

$$\frac{1}{m_1 \cdots m_i} = \frac{1}{m_1 + \cdots + m_i} \sum_{1 \leqslant c \leqslant i} \frac{1}{\underbrace{m_1 \cdots m_i}_{\text{remove } c\text{-th}}}, \tag{4}$$

we have

$$\begin{aligned}
T_{\mathcal{A}}((1,\dots,1);(l_i,\dots,l_r)) &= \sum_{\substack{m_1,\dots,m_r\geqslant 1\\ m_1+\cdots+m_r\leqslant p-1}} \frac{1}{m_1\cdots m_i N_i^{l_i}\cdots N_r^{l_r}} \\
&= \sum_{\substack{m_1,\dots,m_r\geqslant 1\\ m_1+\cdots+m_r\leqslant p-1}} \sum_{1\leqslant c\leqslant i} \frac{1}{\underbrace{m_1\cdots m_i}_{1531:\text{remove } c\text{-th}}} \frac{1}{N_i^{l_i+1}N_{i+1}^{l_{i+1}}\cdots N_r^{l_r}} \\
&= \sum_{\substack{m_1,\dots,m_r\geqslant 1\\ m_1+\cdots+m_r\leqslant p-1}} \frac{i}{m_1\cdots m_{i-1}} \frac{1}{N_i^{l_i+1}N_{i+1}^{l_{i+1}}\cdots N_r^{l_r}}.
\end{aligned}$$

By repeating this procedure, we have

$$\begin{aligned}
&T_{\mathcal{A}}((1,\dots,1);(l_i,\dots,l_r)) \\
&\quad = i! \sum_{\substack{m_1,\dots,m_r\geqslant 1\\ m_1+\cdots+m_r\leqslant p-1}} \frac{1}{m_1(m_1+m_2)\cdots(m_1+\cdots+m_{i-1})} \frac{1}{N_i^{l_i+1}N_{i+1}^{l_{i+1}}\cdots N_r^{l_r}} \\
&\quad = i!\zeta_{\mathcal{A}}(l_r,\cdots,l_{i+1},l_i+1,\underbrace{1,\cdots,1}_{i-1}).
\end{aligned}$$

On the other hand, since $\underbrace{z_1 ш \cdots ш z_1}_{i} = i!\, z_1^i$, we have

$$\begin{aligned}
Z_{\mathcal{A}}(z_{l_r}\cdots z_{l_{i+1}}x^{l_i}(\underbrace{z_1 ш \cdots ш z_1}_{i}) &= i! Z_{\mathcal{A}}(z_{l_r}\cdots z_{l_{i+1}}z_{l_i+1}\underbrace{z_1\cdots z_1}_{i-1})) \\
&= i!\zeta_{\mathcal{A}}(l_r,\cdots,l_{i+1},l_i+1,\underbrace{1,\cdots,1}_{i-1}).
\end{aligned}$$

Hence the assertion holds for the case $(k_1,\dots,k_i)=(1,\dots,1)$.

Next we assume that the assertion holds for all $(k_1,\dots,k_i)$ with $k_1+\cdots+k_i=k$. Let $(k_1,\dots,k_i)\in\mathbb{N}^i$ with $k_1+\cdots+k_i=k+1$. Without loss of generality, we may assume that $(k_1,\dots,k_i)=(k_1,\dots,k_j,1,\dots,1)$ where $k_1,\dots,k_j\geqslant 2$ for some j. Then, by (4) again,

$$\begin{aligned}
&T_{\mathcal{A}}((k_1,\dots,k_i);(l_i,\dots,l_r)) \\
&\quad = \sum_{\substack{m_1,\dots,m_r\geqslant 1\\ m_1+\cdots+m_r\leqslant p-1}} \frac{1}{m_1^{k_1-1}\cdots m_i^{k_i}N_i^{l_i+1}N_{i+1}^{l_{i+1}}\cdots N_r^{l_r}} + \cdots \\
&\qquad + \sum_{\substack{m_1,\dots,m_r\geqslant 1\\ m_1+\cdots+m_r\leqslant p-1}} \frac{1}{m_1^{k_1}\cdots m_j^{k_j-1}m_{j+1}\cdots m_i N_i^{l_i+1}N_{i+1}^{l_{i+1}}\cdots N_r^{l_r}} \\
&\qquad + (i-j) \sum_{\substack{m_1,\dots,m_r\geqslant 1\\ m_1+\cdots+m_r\leqslant p-1}} \frac{1}{m_1^{k_1}\cdots m_j^{k_j}m_{j+1}\cdots m_{i-1}N_i^{l_i+1}N_{i+1}^{l_{i+1}}\cdots N_r^{l_r}}.
\end{aligned}$$

We use the notation $z_1^{\text{ш}r} = \underbrace{z_1 \text{ш} \cdots \text{ш} z_1}_{r}$. Then, by the inductive assumption, we have

$$\begin{aligned} T_{\mathcal{A}}((k_1,\dots,k_i);(l_i,\dots,l_r)) \\ &= Z_{\mathcal{A}}(z_{l_r}\cdots z_{l_{i+1}}x^{l_i+1}(z_{k_1-1}\text{ш}\cdots\text{ш}z_{k_j}\text{ш}z_1^{\text{ш}(i-j)})) \\ &\quad + \cdots + Z_{\mathcal{A}}(z_{l_r}\cdots z_{l_{i+1}}x^{l_i+1}(z_{k_1}\text{ш}\cdots\text{ш}z_{k_j-1}\text{ш}z_1^{\text{ш}(i-j)})) \\ &\quad + (i-j)Z_{\mathcal{A}}(z_{l_r}\cdots z_{l_{i+1}}z_{l_i+1}(z_{k_1}\text{ш}\cdots\text{ш}z_{k_j}\text{ш}z_1^{\text{ш}(i-j-1)})). \end{aligned}$$

On the other hand, by (2), we have

$$\begin{aligned} Z_{\mathcal{A}}(z_{l_r}\cdots z_{l_{i+1}}x^{l_i}(z_{k_1}\text{ш}\cdots\text{ш}z_{k_i})) \\ &= Z_{\mathcal{A}}(z_{l_r}\cdots z_{l_{i+1}}x^{l_i+1}(z_{k_1-1}\text{ш}\cdots\text{ш}z_{k_j}\text{ш}z_1^{\text{ш}(i-j)})) \\ &\quad + \cdots + Z_{\mathcal{A}}(z_{l_r}\cdots z_{l_{i+1}}x^{l_i+1}(z_{k_1}\text{ш}\cdots\text{ш}z_{k_j-1}\text{ш}z_1^{\text{ш}(i-j)})) \\ &\quad + (i-j)Z_{\mathcal{A}}(z_{l_r}\cdots z_{l_{i+1}}x^{l_i}y(z_{k_1}\text{ш}\cdots\text{ш}z_{k_j}\text{ш}z_1^{\text{ш}(i-j-1)})). \end{aligned}$$

Therefore the assertion holds for $(k_1,\dots,k_i)$ and this completes the proof. ■

Remark 2.2. This method can be applied for the classical Mordell-Tornheim multiple zeta values. For example, one can prove the identity

$$\zeta^{MT}(k_1,\dots,k_r;l) = Z(x^l(z_{k_1}\text{ш}\cdots\text{ш}z_{k_r})) \qquad (k_1,\dots,k_r,l\geqslant 1). \tag{5}$$

Here $Z:\mathfrak{H}^0\to\mathbb{R}$ is the $\mathbb{Q}$-linear map satisfying $Z(z_{k_1}\cdots z_{k_r}) = \zeta(k_1,\dots,k_r)$ where $\mathfrak{H}^0 := \mathbb{Q}+x\mathfrak{H}y$. Bradley and Zhou [1, Theorem 1.1] proved that $\zeta^{MT}(k_1,\dots,k_r;l)$ can be written in the form of a linear combination of the usual multiple zeta values. Equation (5) can be regarded as an explicit expression of their result.

Remark 2.3. Kuba [5] introduced a finite analogue T_N of the Mordell-Tornheim multiple zeta values as

$$T_N := \sum_{\substack{m_1+m_2\leqq N\\ m_1,m_2\geqslant 1}} \frac{1}{m_1^{k_1}m_2^{k_2}(m_1+m_2)^{k_3}} \qquad (k_1,k_2,k_3\geqslant 1)$$

for any positive integer N. He proved an identity which expresses T_N in terms of finite analogue of multiple zeta values ([5, Theorem 5]). In our setting ($N=p-1$), his result can be written in the following form:

$$\begin{aligned} \zeta_{\mathcal{A}}^{MT}(k_1,k_2;l) = &\sum_{i=k_2}^{k_1+k_2-1}\binom{i-1}{k_2-1}\zeta_{\mathcal{A}}(l+i,k_1+k_2-i) \\ &+ \sum_{j=k_1}^{k_1+k_2-1}\binom{j-1}{k_1-1}\zeta_{\mathcal{A}}(l+j,k_1+k_2-j) \end{aligned} \tag{6}$$

for $k_1, k_2 \geqslant 1$ and $l \geqslant 0$. This equation also follows from our Theorem 1.2 because it hold that

$$z_{k_1} \text{ш} z_{k_2} = \sum_{i=k_2}^{k_1+k_2-1} \binom{i-1}{k_2-1} z_i z_{k_1+k_2-i} + \sum_{j=k_1}^{k_1+k_2-1} \binom{j-1}{k_1-1} z_j z_{k_1+k_2-j}.$$

3. Relations for finite multiple zeta values

In this section, we give some linear relations among finite multiple zeta values by using Theorem 2.1. First we give the following lemma, which is an analogue of Proposition 1.1 (ii).

Lemma 3.1. *For integers $k_1, \dots, k_r, l \geqslant 0$, the following identity holds:*

$$\zeta_{\mathcal{A}}^{MT}(k_1, \dots, k_r; l) = (-1)^{k_1+l} \zeta_{\mathcal{A}}^{MT}(l, k_2, \dots, k_r; k_1). \tag{7}$$

Proof. By changing the variables as $m_1 \mapsto p - m_1 - \cdots - m_r$ in the summation, we have

$$\begin{aligned}
\zeta_{\mathcal{A}}^{MT}(k_1, \dots, k_r; l) &= \sum_{\substack{m_1,\dots,m_r \geqslant 1 \\ m_1+\cdots+m_r \leqslant p-1}} \frac{1}{m_1^{k_1} \cdots m_r^{k_r} (m_1 + \cdots + m_r)^l} \\
&= \sum_{\substack{m_1,\dots,m_r \geqslant 1 \\ m_1+\cdots+m_r \leqslant p-1}} \frac{1}{(p - m_1 - \cdots - m_r)^{k_1} m_2^{k_2} \cdots m_r^{k_r} (p - m_1)^l} \\
&= \sum_{\substack{m_1,\dots,m_r \geqslant 1 \\ m_1+\cdots+m_r \leqslant p-1}} \frac{(-1)^{k_1+l}}{m_1^l m_2^{k_2} \cdots m_r^{k_r} (m_1 + \cdots + m_r)^{k_1}} \\
&= (-1)^{k_1+l} \zeta_{\mathcal{A}}^{MT}(l, k_2, \dots, k_r; k_1).
\end{aligned}$$

■

Theorem 3.2. *Let r be a positive integer. For positive integers $k_1, \dots, k_r$, the following identities hold:*

$$Z_{\mathcal{A}}(x^l(z_{k_1} \text{ш} \cdots \text{ш} z_{k_r})) = (-1)^{k_1+l} Z_{\mathcal{A}}(x^{k_1}(z_l \text{ш} z_{k_2} \text{ш} \cdots \text{ш} z_{k_r})) \qquad (l \geqslant 1). \tag{8}$$

$$Z_{\mathcal{A}}(z_{k_1} \text{ш} \cdots \text{ш} z_{k_r}) = (-1)^{k_1} Z_{\mathcal{A}}(z_{k_1}(z_{k_2} \text{ш} \cdots \text{ш} z_{k_r})). \tag{9}$$

Both sides of (8) and (9) can be expressed in terms of finite multiple zeta values, hence these equations give linear relations among finite multiple zeta values.

Proof of Theorem 3.2. By Lemma 3.1, we have

$$\zeta_{\mathcal{A}}^{MT}(k_1, \dots, k_r; l) = (-1)^{k_1+l} \zeta_{\mathcal{A}}^{MT}(l, k_2, \dots, k_r; k_1)$$

for positive integers $k_1, \dots, k_r, l$. Equation (8) is obtained by Theorem 1.2.

To prove (9), we consider

$$\begin{aligned}
\zeta_{\mathcal{A}}^{MT}(k_1, \dots, k_r; 0) &= (-1)^{k_1} \zeta_{\mathcal{A}}^{MT}(0, k_2, \dots, k_r; k_1) \\
&= (-1)^{k_1} T_{\mathcal{A}}((k_2, \dots, k_r); (0, k_1)),
\end{aligned}$$

which is also obtained by Lemma 3.1. Then (9) is obtained by Theorem 2.1. ■

Remark 3.3. Equation (9) can be immediately follows from the equation (2.3) in [4].

In the last of this paper, we give some examples.

For $(k_1,\dots,k_r)=(k_1,k_2,\dots,k_{r-t},\overbrace{1,\dots,1}^{t})$ $(k_{r-t}\geqslant 2)$, we define $u_{k_1,\dots,k_r}=t+1$. For example, $u_{2,3}=1$, $u_{3,1}=2$ and $u_{1,1,1}=4$. Then the following identity holds:

Proposition 3.4. *For positive integers k, l and r, it holds that*

$$(-1)^l\sum_{m_1+\cdots+m_r=k+r}u_{m_1,\dots,m_r}\zeta_{\mathcal{A}}(l+1,m_1,\dots,m_r)$$
$$=(-1)^k\sum_{m_1+\cdots+m_r=l+r}u_{m_1,\dots,m_r}\zeta_{\mathcal{A}}(k+1,m_1,\dots,m_r).$$

Proof. Let $Y_r(k,l):=Z_{\mathcal{A}}(x^l(z_k\text{ш}y^{r-1}))$. Since

$$\begin{aligned}z_k\text{ш}y^{r-1}&=\sum_{i_1+\cdots+i_r=k+r-1}u_{i_2,\dots,i_r}x^{i_1-1}yx^{i_2-1}y\cdots x^{i_r-1}y\\&=\sum_{i_1+\cdots+i_r=k+r-1}u_{i_2,\dots,i_r}z_{i_1}z_{i_2}\cdots z_{i_r},\end{aligned}$$

we have

$$\begin{aligned}Y_r(k,l)&=\sum_{i_1+\cdots+i_r=k+r-1}u_{i_2,\dots,i_r}\zeta_{\mathcal{A}}(l+i_1,i_2,\dots,i_r)\\&=\sum_{\substack{i_1+\cdots+i_r=k+l+r-1\\ i_1\geqslant l+1}}u_{i_2,\dots,i_r}\zeta_{\mathcal{A}}(i_1,i_2,\dots,i_r).\end{aligned}$$

Hence it holds that

$$Y_r(k+1,l)-Y_r(k,l+1)=\sum_{i_2+\cdots+i_r=k+r-1}u_{i_2,\dots,i_r}\zeta_{\mathcal{A}}(l+1,i_2,\dots,i_r).$$

By putting $k_1=k$ and $k_2=\cdots=k_r=1$ in (8), we have $Y_r(k,l)=(-1)^{k+l}Y_r(l,k)$. Therefore

$$\sum_{i_2+\cdots+i_r=k+r-1}u_{i_2,\dots,i_r}\zeta_{\mathcal{A}}(l+1,i_2,\dots,i_r)$$
$$=(-1)^{k+l}\sum_{i_2+\cdots+i_r=l+r-1}u_{i_2,\dots,i_r}\zeta_{\mathcal{A}}(k+1,i_2,\dots,i_r).$$

By replacing $r-1$ by r, we obtain the result. ■

Acknowledgements. The author is grateful to Professor Seidai Yasuda for his helpful advice about Theorem 1.2. The author would also like to thank Professor Kohji Matsumoto, Professor Hirofumi Tsumura and Professor Yasushi Komori for their comments about Remark 2.2.

References

[1] D.M. Bradley and X. Zhou, *On Mordell-Tornheim sums and multiple zeta values*, Ann. Sci. Math. Québec **34** (2010), 15–23.
[2] M. Hoffman, *The algebra of multiple harmonic series*, J. Algebra **194** (1997), 477–495.
[3] M. Hoffman, *Quasi-symmetric functions and mod p multiple harmonic sums*, preprint.
[4] M. Kaneko, *Finite multiple zeta values* (in Japanese), RIMS Kôkyûroku Bessatsu, to appear.
[5] M. Kuba, *On evaluations of infinite double sums and Tornheim's double series*, Sémin. Lothar. Comb. **58** (2008), Article B58d.
[6] L.J. Mordell, *On the evaluation of some multiple series*, J. London Math. Soc. **33** (1958), 368–371.
[7] K. Matsumoto, *On the analytic continuation of various multiple zeta-functions*, Number theory for the millennium, II (Urbana, IL, 2000), 417–440, A K Peters, Natick, MA, 2002.
[8] S. Saito and N. Wakabayashi, *Sum formula for finite multiple zeta values*, J. Math. Soc. Japan, to appear.
[9] S. Saito and N. Wakabayashi, *The Bowman-Bradley type theorem for finite multiple zeta values*, preprint.
[10] L. Tornheim, *Harmonic double series*, Amer. J. Math. **72** (1950), 303–314.
[11] H. Tsumura, *On Mordell-Tornheim zeta values*, Proc. Amer. Math. Soc. **133** (2005), 2387–2393.

Address: Ken Kamano: Department of Mathematics, Osaka Institute of Technology, 5-16-1, Omiya, Asahi, Osaka 535-8585, Japan.

E-mail: ken.kamano@oit.ac.jp

Received: 6 January 2015; **revised:** 7 May 2015

Functiones et Approximatio
54.1 (2016), 73–93
doi: 10.7169/facm/2016.54.1.7

THE MULTIPLICATIVE ORDERS OF CERTAIN GAUSS FACTORIALS, II

John B. Cosgrave, Karl Dilcher

Abstract: We study the multiplicative orders of $\left(\frac{n-1}{M}\right)_n!$ (mod n) for odd prime powers $n = p^\alpha$, $p \equiv 1 \pmod{M}$, where the Gauss factorial $N_n!$ denotes the product of all integers up to N that are relatively prime to n. Departing from previously obtained results on the connection between the order for p^α and for $p^{\alpha+1}$, we obtain new criteria for exceptions to a general pattern, with particular emphasis on the cases $M = 3$, $M = 4$ and $M = 6$. In the process we also obtain some results of independent interest. Most results are based on generalizations of binomial coefficient congruences of Gauss, Jacobi, and Hudson and Williams.

Keywords: Gauss-Wilson theorem, factorials, Gauss factorials, binomial coefficient congruences.

1. Introduction

The factorial-like product of integers,

$$N_n! = \prod_{\substack{1 \leqslant j \leqslant N \\ \gcd(j,n)=1}} j, \tag{1.1}$$

defined for positive integers N and n, plays an important role in number theory, for instance in the definition of Morita's p-adic Gamma function (see, e.g., [1, p. 277]). We call this product a *Gauss factorial*, a terminology suggested by the *Gauss-Wilson theorem* which states that for any integer $n \geqslant 2$ we have

$$(n-1)_n! \equiv \begin{cases} -1 \pmod{n} & \text{for} \quad n = 2, 4, p^\alpha, \text{ or } 2p^\alpha, \\ 1 \pmod{n} & \text{otherwise,} \end{cases} \tag{1.2}$$

where p is an odd prime and α is a positive integer. In the previous papers [2], [4], and [5] we studied the Gauss factorials $(\frac{n-1}{M})_n!$, $M \geqslant 1$, $n \equiv 1 \pmod{M}$. For

Research supported in part by the Natural Sciences and Engineering Research Council of Canada

2010 Mathematics Subject Classification: primary: 11A07; secondary: 11B65

$M = 1$ this is just the Gauss-Wilson theorem (1.2), and the case $M = 2$ and p prime was first considered by Lagrange in 1773 (see [8, p. 275]). Later Mordell [13] completely determined the multiplicative orders (modulo p), and the present authors [2] extended this to arbitrary positive integers n. While much can be said about the case of general $M \geqslant 2$ and n having two or more distinct prime factors congruent to 1 modulo M (see [5] and [6]), a particularly interesting and challenging case occurs when $n = p^\alpha$, $p \equiv 1 \pmod{M}$. In fact, it is the purpose of this paper to continue our study in [4] of the multiplicative orders of

$$\left(\tfrac{p^\alpha-1}{M}\right)_{p^\alpha}! \pmod{p^\alpha}, \qquad p \equiv 1 \pmod{M}, \qquad M \geqslant 2. \tag{1.3}$$

While everything is known when $M = 2$, and a number of results for general M were obtained in [4], this paper will be mainly devoted to the cases $M = 3, 4$, and 6. This is not because they are "next in line", but rather, the theory of Jacobi sums makes it possible to obtain particular results, and explain special phenomena, that do not apparently occur in other cases.

Given a fixed integer $M \geqslant 2$ and prime $p \equiv 1 \pmod{M}$, our main objects of study will be the multiplicative orders

$$\gamma_\alpha^M(p) := \operatorname{ord}_{p^\alpha}\left(\left(\tfrac{p^\alpha-1}{M}\right)_{p^\alpha}!\right) \tag{1.4}$$

for varying integers $\alpha \geqslant 1$. Clearly $(\frac{p^\alpha-1}{M})_{p^\alpha}! = (\frac{p^\alpha-1}{M})_p!$; in what follows we will therefore replace the subscript p^α in the Gauss factorial by p.

Since the case $M = 2$ is completely determined, we consider mainly $M \geqslant 3$. We illustrate the sequence of orders for $\alpha = 1, 2, \ldots$ with two examples for $M = 3$.

Example 1. When $p = 7$, we have $\frac{p-1}{3} = 2$ and the Gauss factorial is just the ordinary factorial, namely 2. We immediately see that $\gamma_1^3(7) = 3$. Using computer algebra, we furthermore find $\gamma_2^3(7) = 21$, $\gamma_3^3(7) = 147$, and writing $\gamma := \gamma_1^3(7)$, it appears that we obtain the sequence $\gamma, \gamma p, \gamma p^2, \gamma p^3, \ldots$

Example 2. When $p = 13$, we have $\frac{p-1}{3} = 4$ and once again the Gauss factorial is the ordinary factorial, $4! \equiv 11 \pmod{13}$. It is now easy to verify that $\gamma_1^3(13) = 12$. Furthermore, computer algebra yields $\gamma_2^3(13) = 12$ also, while we get $\gamma_3^3(13) = 12 \cdot 13$, and it appears that in this case the sequence $\{\gamma_\alpha^M(p)\}$, $\alpha = 1, 2, \ldots$, is of the form $\gamma, \gamma, \gamma p, \gamma p^2, \ldots$, in contrast to the first example.

These two examples are special cases of one of the main results in [4], namely Proposition 2.2, which relates the order $\gamma_{\alpha+1}^M(p)$ with $\gamma_\alpha^M(p)$, for $\alpha \geqslant 1$:

Theorem 1 ([4]). *Let $M \geqslant 2$ be an integer, let $p \equiv 1 \pmod{M}$ be a prime, and for $\alpha \geqslant 1$ let $\gamma_\alpha^M(p)$ be defined as in* (1.4). *If $p \equiv 1 \pmod{2M}$, then*

$$\gamma_{\alpha+1}^M(p) = p\gamma_\alpha^M(p) \qquad \text{or} \qquad \gamma_{\alpha+1}^M(p) = \gamma_\alpha^M(p). \tag{1.5}$$

If $p \equiv M + 1 \pmod{2M}$, then

$$\gamma_{\alpha+1}^M(p) = \begin{cases} p\gamma_\alpha^M(p) \quad \text{or} \quad \gamma_\alpha^M(p) & \text{when} \quad \gamma_\alpha^M(p) \equiv 0 \pmod 4, \\ \frac{1}{2}p\gamma_\alpha^M(p) \quad \text{or} \quad \frac{1}{2}\gamma_\alpha^M(p) & \text{when} \quad \gamma_\alpha^M(p) \equiv 2 \pmod 4, \\ 2p\gamma_\alpha^M(p) \quad \text{or} \quad 2\gamma_\alpha^M(p) & \text{when} \quad \gamma_\alpha^M(p) \equiv 1 \pmod 2. \end{cases} \tag{1.6}$$

Numerical experiments show that almost always the first alternative in the various cases in Theorem 1 holds, with very few exceptions such as the case of Example 2. For the sake of completeness we display an excerpt of Table 3 in [4] as Table 1 below.

Table 1: Exceptional ($\alpha = 1$) primes $p < 2 \cdot 10^6$ for $3 \leqslant M \leqslant 10$.

M	p
3	13, 181, 2 521, 76 543, 489 061
4	29 789
5	71
6	13, 181, 2 521, 76 543, 489 061
10	11

All these exceptional primes occur at $\alpha = 1$. We have not found any for $\alpha \geqslant 2$, and will return to this point in the next section. It was a major part of [4], and will also be so in the present paper, to establish criteria and characterizations for the exceptionality of these primes. While this paper will be mainly devoted to the special cases $M = 3$, 4 and 6, we begin by quoting a general criterion from [4]. We first need some definitions.

For any prime p, the *Wilson quotient* is defined by

$$w(p) := \frac{(p-1)! + 1}{p}. \tag{1.7}$$

By Wilson's theorem, $w(p)$ is obviously an integer; often the Wilson quotient is considered modulo p. Next, for any positive integer $M \geqslant 2$ and prime $p \equiv 1 \pmod{M}$ we define the sum

$$S^M(p) := \sum_{j=1}^{\frac{p-1}{M}} \frac{1}{j}. \tag{1.8}$$

For $M = 2$, 3, 4 and 6 there are well-known evaluations of such sums modulo p in terms of Fermat quotients; see, e.g., [12] or [3]. Finally, for given $\alpha \geqslant 1$, $M \geqslant 2$ and $p \equiv 1 \pmod{M}$ we define $V_\alpha^M(p)$ by

$$\left(\left(\tfrac{p^\alpha - 1}{M} \right)_p ! \right)^{\gamma_\alpha^M(p)} \equiv 1 + V_\alpha^M(p) p^\alpha \pmod{p^{\alpha+1}}, \tag{1.9}$$

where $\gamma_\alpha^M(p)$ is the order defined in (1.4). We are now ready to state the following supplementary result to Theorem 1, which can be found as the final part of Proposition 4.2 in [4].

Theorem 2. *With M, p and α as in Theorem 1, the first alternative in each case of* (1.5), (1.6) *holds if and only if*

$$T_\alpha^M(p) := V_\alpha^M(p) + \tfrac{1}{M} \gamma_\alpha^M(p) \big(w(p) - S^M(p) \big) \not\equiv 0 \pmod{p}. \tag{1.10}$$

While it is not our intention to repeat the proof of this result and of Theorem 1, we would like to put the expression $T_\alpha^M(p)$ into perspective. Let us take, for instance, $M = 3$. Then by definition of the order we obviously have, for a given $\alpha \geqslant 1$,

$$\left(\left(\frac{p^\alpha-1}{3}\right)_p!\right)^{\gamma_\alpha^3(p)} \equiv 1 \pmod{p^\alpha}.$$

Much less obvious is the congruence

$$\left(\left(\frac{p^{\alpha+1}-1}{3}\right)_p!\right)^{\gamma_\alpha^3(p)} \equiv 1 + T_\alpha^3(p)p^\alpha \pmod{p^{\alpha+1}}; \tag{1.11}$$

the general case of this lies at the heart of the proof of both Theorems 1 and 2. Indeed, the congruence (1.11) shows that in the case when $T_\alpha^3(p) \equiv 0 \pmod{p}$, by the definition (1.4) we have $\gamma_{\alpha+1}^3(p) = \gamma_\alpha^3(p)$. On the other hand, when $T_\alpha^3(p) \not\equiv 0 \pmod{p}$, we raise both sides of the congruence (1.11) to the power p, and we see that in this case $\gamma_{\alpha+1}^3(p) = p\gamma_\alpha^3(p)$. All this, of course, is consistent with Theorems 1 and 2.

The condition (1.10) was used to find the entries in Table 1 for all $p < 2 \cdot 10^6$, using the computer algebra system Maple. In the cases $M = 3$, 4 and 6, aided by the connection between the sums $S^M(p)$ and Fermat quotients, we were able to extend the computations to $p < 10^8$; this was later extended at our request by Yves Gallot [9] to $4 \cdot 10^8$. On the other hand, due to the obvious difficulty of computing $V_\alpha^M(p)$ for $\alpha = 2$, we were able to search for "$\alpha = 2$ exceptional primes" only for $p < 10^4$, without finding any. See, however, the remarks following Theorem 3 below.

The above results, quoted from [4], may serve as motivation for the new results in the present paper. In particular, in the cases $M = 3$, 4 and 6 we will

– give a new and much faster test for exceptional primes, which will also lead to some new theoretical results;

– further investigate the coincidence of exceptional primes for $M = 3$ and $M = 6$.

However, we begin with a matter that is related to Theorem 1 and Example 2.

2. Descending exceptionality

Considering Examples 1 and 2 with $M = 3$, it is conceivable that there exists a prime $p \equiv 1 \pmod 3$ such that $\gamma_1^3(p) = \gamma$, $\gamma_2^3(p) = p\gamma$, and $\gamma_3^3(p) = p\gamma$ also, for some integer γ. In this section we show that this, and related behaviour of more general orders, cannot happen. We first introduce some terminology.

Definition 1. For a fixed integer $M \geqslant 2$, a prime $p \equiv 1 \pmod M$ will be called α-*exceptional for* M if for the integer $\alpha \geqslant 1$ the second alternative in the appropriate case in (1.5) or (1.6) holds, or equivalently, if $T_\alpha^M(p) \equiv 0 \pmod p$; see (1.10).

Thus, all the primes listed in Table 1 are 1-exceptional for the appropriate M. The following result shows that the levels of exceptionality are strongly related with each other.

Theorem 3. *Let $M \geqslant 2$ be fixed. If, for an integer $\alpha \geqslant 2$, a prime $p \equiv 1 \pmod{M}$ is α-exceptional for M, then it is also $(\alpha-1)$-exceptional for M.*

We see that Examples 1 and 2 are consistent with this result which applies vacuously to these situations. On the other hand, this theorem shows that the hypothetical situation at the beginning of this section cannot occur since the 2-exceptionality of p would imply its 1-exceptionality. In other words, the only possible sequence of orders is (in the case of (1.5)) of the form

$$\gamma, \gamma, \ldots, \gamma, \gamma p, \gamma p^2, \gamma p^3, \ldots \qquad \text{or} \qquad \gamma, \gamma, \gamma, \ldots,$$

with the appropriate adjustments in the situations of (1.6). As mentioned before, we have not found any prime that is 2-exceptional for some $M \geqslant 3$. It is now a routine computation to check that none of the entries in Table 1 (and in Table 3 in [4]) are 2-exceptional.

For $M = 2$, on the other hand, *every* odd prime is α-exceptional for all $\alpha \geqslant 1$, which is again consistent with Theorem 3. This follows immediately from Theorem 2 in [2] and is related to the fact that $\gamma_\alpha^2(p)$ can only be 1, 2 or 4.

For the proof of Theorem 3 we need the following easy lemma.

Lemma 1. *Let p be an odd prime and $\alpha \geqslant 2$ an integer. Then the congruence $X^p \equiv 1 \pmod{p^\alpha}$ implies $X \equiv 1 \pmod{p^{\alpha-1}}$.*

Proof. When $X = 1$, the lemma is trivially true; we therefore assume that $X \neq 1$. By the first congruence we have $X^p \equiv 1 \pmod{p}$, and in particular $X \not\equiv 0 \pmod{p}$. Fermat's little theorem then gives $X^{p-1} \equiv 1 \pmod{p}$, and upon subtracting we get $X^p - X^{p-1} = (X-1)X^{p-1} \equiv 0 \pmod{p}$, which implies $X \equiv 1 \pmod{p}$.

Now let $a \in \mathbb{N}$ be such that $X = 1 + mp^a$ with an integer $m \not\equiv 0 \pmod{p}$. Then a binomial expansion gives

$$X^p = 1 + pmp^a + \sum_{j=2}^{p-1} \binom{p}{j} m^j p^{ja} + m^p p^{pa}. \tag{2.1}$$

Since $p \mid \binom{p}{j}$ for $1 \leqslant j \leqslant p-1$ and then $1 + ja \geqslant a + 2$ for all $j \geqslant 2$ and $a \geqslant 1$, the middle sum in (2.1) is divisible by p^{a+2}. Similarly, since p is odd, we have $pa \geqslant 3a \geqslant a + 2$ for $a \geqslant 1$, so that $p^{a+2} \mid p^{pa}$. Hence (2.1) gives

$$X^p \equiv 1 + mp^{a+1} \pmod{p^{a+2}},$$

which, by our hypothesis, means that $a \geqslant \alpha - 1$. It follows that $X \equiv 1 \pmod{p^{\alpha-1}}$, as desired. ∎

We note that the condition in Lemma 1 that p be an odd prime is necessary. Indeed, we have $3^2 \equiv 1 \pmod{2^3}$, but $3 \not\equiv 1 \pmod{2^2}$.

Proof of Theorem 3. If p is α-exceptional, then the expression in (1.10) vanishes modulo p. To obtain a contradiction, we assume that p is *not* $(\alpha-1)$-exceptional, where $\alpha \geqslant 2$. Then by definition, the first alternatives in (1.5) and (1.6) hold, with α replaced by $\alpha - 1$. In particular, since p is odd, we have in all cases $\gamma_\alpha^M(p) \equiv 0 \pmod{p}$. By our first statement above, which concerned the term in (1.10), this means that

$$V_\alpha^M(p) \equiv 0 \pmod{p}.$$

But then, the definition (1.9) of $V_\alpha^M(p)$ implies

$$\left(\left(\frac{p^\alpha - 1}{M} \right)_p ! \right)^{\gamma_\alpha^M(p)} \equiv 1 \pmod{p^{\alpha+1}}. \tag{2.2}$$

By our assumption that p is not $(\alpha-1)$-exceptional, we have once again

$$\gamma_\alpha^M(p) = \delta p \gamma_{\alpha-1}^M(p), \qquad \delta = \tfrac{1}{2}, 1, \text{or } 2.$$

We now use this relation and apply Lemma 1 to (2.2), obtaining

$$\left(\left(\frac{p^\alpha - 1}{M} \right)_p ! \right)^{\delta\gamma_{\alpha-1}^M(p)} \equiv 1 \pmod{p^\alpha}.$$

However, this contradicts the fact that, by the definition of the order, the smallest exponent giving $1 \pmod{p^\alpha}$ is $\gamma_\alpha^M(p) = p \cdot (\delta\gamma_{\alpha-1}^M(p))$. The proof is now complete. ∎

3. Some fundamental congruences for $M = 3$ and 6

In this section we derive a number of congruences that will be required in the following sections. Before we can state and prove our results, we need some facts related to the representation of a prime $p \equiv 1 \pmod 6$ in the form $p = a^2 + 3b^2$. It is known that this representation is unique up to signs, but the signs of a and b are crucial here and require some explanation (see [1, pp. 103–106]):

Let g be a primitive root modulo p and χ_6 a character modulo p of order 6 with $\chi_6(g) = e^{2\pi i/6} = (1 + i\sqrt{3})/2$. Then we fix the signs of a and b by the congruences

$$a \equiv -1 \pmod 3 \qquad \text{and} \qquad 3b \equiv (2g^{(p-1)/3} + 1)a \pmod{p}.$$

With the integers a and b thus determined, we define two closely related pairs r, s and u, v of integers as follows. Let $Z = \operatorname{ind}_g 2$, the index of $2 \pmod p$ with respect to g. Then

$$r = 2a, \quad s = 2b; \quad u = 2a, \quad v = 2b \quad (Z \equiv 0 \pmod 3), \tag{3.1}$$
$$r = -a - 3b, \ s = a - b; \quad u = -a + 3b, \ v = -a - b \quad (Z \equiv 1 \pmod 3), \tag{3.2}$$
$$r = -a + 3b, \ s = -a - b; \ u = -a - 3b, \ v = a - b \quad (Z \equiv 2 \pmod 3). \tag{3.3}$$

We mention in passing that the integers r, s and u, v also satisfy sums-of-squares identities, namely

$$4p = r^2 + 3s^2 \qquad \text{and} \qquad 4p = u^2 + 3v^2, \qquad r \equiv u \equiv 1 \pmod 3 \tag{3.4}$$

We are now ready to state our results. In [3, Theorem 8] a well-known congruence of Jacobi for binomial coefficients, namely

$$\binom{\frac{2(p-1)}{3}}{\frac{p-1}{3}} \equiv -r \pmod p, \tag{3.5}$$

was extended as follows: For any integer $\alpha \geqslant 1$ and for any prime $p \equiv 1 \pmod 6$ and integer r as defined in (3.1)–(3.3) we have

$$\frac{\left(\frac{2(p^{\alpha+1}-1)}{3}\right)_p!}{\left(\left(\frac{p^{\alpha+1}-1}{3}\right)_p!\right)^2} \equiv -J_\alpha(p) \pmod{p^{\alpha+1}}, \tag{3.6}$$

where for ease of notation we set

$$J_\alpha(p) := r - \frac{p}{r} - \frac{p^2}{r^3} - \cdots - C_{\alpha-1}\frac{p^\alpha}{r^{2\alpha-1}}, \tag{3.7}$$

with $C_n := \frac{1}{n+1}\binom{2n}{n}$ the nth Catalan number, which is always an integer. In analogy to the theorem of Jacobi (and a similar one due to Gauss which will be mentioned later), the following congruence was proved by Hudson and Williams [10]; see also [1, p. 270].

Theorem 4 (Hudson and Williams). *Let $p \equiv 1 \pmod 6$ be a prime and u as defined in* (3.1)–(3.3). *Then*

$$\binom{\frac{p-1}{3}}{\frac{p-1}{6}} \equiv (-1)^{\frac{p-1}{6}+1}u \pmod p. \tag{3.8}$$

In analogy to (3.6) we have the following result, the proof of which we will only sketch since it is quite similar to the proofs in [3]. This result will be the basis of much of what follows.

Theorem 5. *Let $p \equiv 1 \pmod 6$ be a prime and u as defined in* (3.1)–(3.3). *Then for any integer $\alpha \geqslant 1$ we have*

$$\frac{\left(\frac{p^{\alpha+1}-1}{3}\right)_p!}{\left(\left(\frac{p^{\alpha+1}-1}{6}\right)_p!\right)^2} \equiv (-1)^{\frac{p-1}{6}+1}K_\alpha(p) \pmod{p^{\alpha+1}}, \tag{3.9}$$

where

$$K_\alpha(p) := u - \frac{p}{u} - \frac{p^2}{u^3} - \cdots - C_{\alpha-1}\frac{p^\alpha}{u^{2\alpha-1}} \tag{3.10}$$

and C_n denotes the nth Catalan number.

The proof of this result is based on deep connections between the Jacobi sum $J(\chi,\psi)$ over the finite field $\mathbb{F}_p$, with χ and ψ characters on $\mathbb{F}_p$, and the p-adic gamma function $\Gamma_p(z)$ which can be defined as the limit

$$\Gamma_p(z) = \lim_{n\to z} F(n) \qquad (z \in \mathbb{Z}_p), \tag{3.11}$$

where n runs through any sequence of positive integers p-adically approaching z, and $F(n)$ is defined by $F(0) := 1$ and

$$F(n) := (-1)^n \prod_{\substack{0<j<n\\ p\nmid j}} j \qquad (n \geqslant 1). \tag{3.12}$$

For further details on $J(\chi,\psi)$ and $\Gamma_p(z)$ we refer the reader to a brief exposition in [3] which in turn is based on more detailed explanations in [1].

Proof of Theorem 5 (Sketch). We follow the outline of the related proofs of Theorems 7 and 8 in [3]. With the character χ_6 as defined before (3.1), we use the appropriate entries in Table 3.1.2 in [1, p. 107]:

$$J(\chi_6,\chi_6) = (-1)^{\frac{p-1}{6}}\frac{1}{2}(u+iv\sqrt{3}), \tag{3.13}$$

$$J(\chi_6^5,\chi_6^5) = (-1)^{\frac{p-1}{6}}\frac{1}{2}(u-iv\sqrt{3}), \tag{3.14}$$

where u and v are as in (3.1)–(3.3). Recall that $4p = u^2+3v^2$.

If $\mathfrak{p}$ is a nonzero prime ideal in the ring $\mathbb{Z}[\frac{1+i\sqrt{3}}{2}]$ of integers of $\mathbb{Q}(\sqrt{-3})$ dividing the prime p, then by Theorem 2.1.14 in [1, p. 66] we have $J(\chi_6,\chi_6) \equiv 0 \pmod{\mathfrak{p}}$. We combine this congruence with (3.13) and raise both sides to the power α, obtaining

$$(u+iv\sqrt{3})^\alpha \equiv 0 \pmod{\mathfrak{p}^\alpha}.$$

Since this holds for any nonzero prime ideal $\mathfrak{p}$ of $\mathbb{Z}[\frac{1+i\sqrt{3}}{2}]$ dividing p, we may conclude that this congruence also holds modulo p^α. Indeed, we know that p either remains prime, or splits, or ramifies in $\mathbb{Q}(\sqrt{-3})$. Therefore we have

$$(u+iv\sqrt{3})^\alpha \in p^\alpha\mathbb{Z}[\tfrac{1+i\sqrt{3}}{2}], \quad \text{resp.} \quad (u+iv\sqrt{3})^{2\alpha} \in p^\alpha\mathbb{Z}[\tfrac{1+i\sqrt{3}}{2}],$$

in the first case and the other two cases, respectively. This means that in any case, after replacing α by $\alpha+1$,

$$(u+iv\sqrt{3})^{\alpha+1} \equiv 0 \pmod{p^{\alpha+1}}. \tag{3.15}$$

Next, using identity (9.3.7) in [1, p. 278], together with (3.11) and (3.12), we obtain in analogy to the proof of Theorem 7 in [3],

$$J(\chi_6^5,\chi_6^5) = \frac{\Gamma_p(1-\frac{1}{3})}{\Gamma_p(1-\frac{1}{6})^2} \equiv -\frac{\left(\frac{p^{\alpha+1}-1}{3}\right)_p!}{\left(\left(\frac{p^{\alpha+1}-1}{6}\right)_p!\right)^2} \pmod{p^{\alpha+1}}. \tag{3.16}$$

The right-hand side of this is minus the left-hand side of (3.9). The remainder of the proof is now almost identical with the corresponding parts of the proofs of Theorems 7 and 8 in [3]: Expand the left-hand side of (3.15), collect real and imaginary parts, and use (3.14). Using appropriate combinatorial identities, we finally obtain the right-hand side of (3.9). ∎

We will now use Theorem 5 and elements in its proof to derive the following fundamental result which will also be very useful later on.

Theorem 6. *Let $p \equiv 1 \pmod 6$ be a prime and r, u as defined in* (3.1)–(3.3). *Then for all $\alpha \geqslant 1$ we have*

$$\left(r - \frac{p}{r} - \cdots - \frac{C_{\alpha-1}p^\alpha}{r^{2\alpha-1}}\right)^3 \equiv \left(u - \frac{p}{u} - \cdots - \frac{C_{\alpha-1}p^\alpha}{u^{2\alpha-1}}\right)^3 \pmod{p^{\alpha+1}}. \quad (3.17)$$

We obtain this congruence as a consequence of the following result.

Lemma 2. *Let g be a primitive root, and let χ_3 be a character modulo p of order 3 with $\chi_3(g) = e^{2\pi i/3} = (-1 + i\sqrt{3})/2$. Furthermore, let χ_6 be the character of order 6 defined before* (3.1). *Then*

$$\big(J(\chi_3^2, \chi_3^2)\big)^3 = \Big((-1)^{\frac{p-1}{6}} J(\chi_6^5, \chi_6^5)\Big)^3. \quad (3.18)$$

Proof of Theorem 6. A key congruence in the proof of Theorem 8 in [3, p. 114] shows that the left-hand side of (3.6) is congruent to $-J(\chi_3^2, \chi_3^2)$ modulo $p^{\alpha+1}$, so that

$$J(\chi_3^2, \chi_3^2) \equiv J_\alpha(p) \pmod{p^{\alpha+1}}. \quad (3.19)$$

Similarly, combining (3.9) and (3.16), we have

$$J(\chi_6^5, \chi_6^5) \equiv -(-1)^{\frac{p-1}{6}} K_\alpha(p) \pmod{p^{\alpha+1}}. \quad (3.20)$$

Substituting (3.19) and (3.20) into (3.18), we immediately obtain (3.17). ∎

Proof of Lemma 2. By Tables 3.1.1 and 3.1.2, respectively, in [1, p. 106–107], we have

$$J(\chi_3^2, \chi_3^2) = \frac{r - is\sqrt{3}}{2}, \qquad J(\chi_6^5, \chi_6^5) = (-1)^{\frac{p-1}{6}} \frac{u - iv\sqrt{3}}{2},$$

where r, s, u and v are as in (3.1)–(3.3). Hence (3.18) is equivalent to

$$(r - is\sqrt{3})^3 = (u - iv\sqrt{3})^3. \quad (3.21)$$

We distinguish between the following cases according to (3.1) and (3.2), (3.3):

(i) When $Z \equiv 0 \pmod 3$, then (3.21) is trivially true.

(ii) When $Z \equiv \pm 1 \pmod 3$, then (3.21) is equivalent to

$$(-a \mp 3b + i(\pm a - b)\sqrt{3})^3 = (-a \pm 3b + i(\mp a - b)\sqrt{3})^3,$$

where "upper" and "lower" signs correspond to each other. But this is easily verified, for instance by multiplying the expression in parentheses on the left by the 3rd root of unity $-\frac{1}{2} \pm \frac{i}{2}\sqrt{3}$, which gives the expression in parentheses on the right, thus completing the proof. ■

The above proofs show that the expressions in parentheses in (3.17), rather than their 3rd powers, are congruent to each other (in fact, equal) if and only if the case (3.1) holds. The following elementary congruence can be seen as a supplement to Theorem 6 for the case $\alpha = 0$.

Lemma 3. *For any* $p \equiv 1 \pmod 6$ *we have* $r^3 \equiv u^3 \pmod p$.

Proof. We consider the factorization $r^3 - u^3 = (r-u)(r^2+ru+u^2)$ and use the fact that by (3.1)-(3.3) we have either $r = u$, or else in both remaining cases,

$$r^2+ru+u^2 \equiv (a+3b)^2+(a+3b)(a-3b)+(a-3b)^2 = 3(a^2+3b^2) = 3p \equiv 0 \pmod p.$$

So in all three cases we have $r^3 - u^3 \equiv 0 \pmod p$. ■

Now that we have proved Theorem 6, we can use it to derive another very useful congruence.

Corollary 1. *For any prime* $p \equiv 1 \pmod 6$ *and integer* $\alpha \geqslant 1$ *we have*

$$\left(\left(\tfrac{p^\alpha-1}{3}\right)_p!\right)^{24} \equiv \left(\left(\tfrac{p^\alpha-1}{6}\right)_p!\right)^{12} \pmod{p^\alpha}. \tag{3.22}$$

Proof. For $\alpha = 1$ we cube (3.5) and (3.8) and combine the two by using Lemma 3. Similarly, for $\alpha \geqslant 2$ we cube both sides of (3.6) and (3.9), replace $\alpha+1$ by α, and combine the two by using (3.17). In all cases we then have, for $\alpha \geqslant 1$,

$$\left(\left(\tfrac{2(p^\alpha-1)}{3}\right)_p!\right)^3 \left(\left(\tfrac{p^\alpha-1}{6}\right)_p!\right)^6 \equiv \pm\left(\left(\tfrac{p^\alpha-1}{3}\right)_p!\right)^9 \pmod{p^\alpha}. \tag{3.23}$$

By a result of D. H. Lehmer [11, Theorem 4], the Gauss factorial $(\frac{2}{3}(p^\alpha-1))_p!$ has $\frac{2}{3}\varphi(p^\alpha)$ factors in its defining product. Similarly, $(\frac{1}{3}(p^\alpha-1))_p!$ has $\frac{1}{3}\varphi(p^\alpha)$ factors, which is an even number since $p \equiv 1 \pmod 6$. Hence by symmetry, the product of all integers strictly between $\frac{2}{3}(p^\alpha-1)$ and p^α, and not divisible by p, is congruent to $(\frac{1}{3}(p^\alpha-1))_p! \pmod{p^\alpha}$, and we obtain

$$\left(\tfrac{2(p^\alpha-1)}{3}\right)_p! \left(\tfrac{p^\alpha-1}{3}\right)_p! \equiv (p^\alpha-1)_p! \equiv -1 \pmod{p^\alpha}, \tag{3.24}$$

by the Gauss-Wilson theorem (1.2). Finally, we multiply both sides of (3.23) by $(\frac{p^\alpha-1}{3})_p!^3$ and apply (3.24) to the left-hand side. Then upon squaring both sides we obtain (3.22). ■

In [4, p. 159] we observed, without proof, that the ratios of the orders $\gamma_1^6(p)/\gamma_1^3(p)$ (see (1.4)) can take on only the 18 different values in the set

$$R_{18} := \left\{ \frac{1}{24}, \frac{1}{12}, \frac{1}{8}, \frac{1}{6}, \frac{1}{4}, \frac{1}{3}, \frac{3}{8}, \frac{1}{2}, \frac{2}{3}, \frac{3}{4}, 1, \frac{4}{3}, \frac{3}{2}, 2, 3, 4, 6, 12 \right\}. \tag{3.25}$$

We will now use Corollary 1 to show that this observation is actually true in a more general setting.

Corollary 2. *Let $\alpha \geqslant 1$ be fixed. Then for any $p \equiv 1 \pmod 6$ the ratio of orders $\gamma_\alpha^6(p)/\gamma_\alpha^3(p)$ can only take on values from the set R_{18} in* (3.25).

Proof. We use the congruence (3.22), and for greater ease of notation we set

$$X = \left(\tfrac{p^\alpha - 1}{3}\right)_p!, \qquad Y = \left(\tfrac{p^\alpha - 1}{6}\right)_p!.$$

Clearly none of the numbers X, Y, 12 or 24 is divisible by p. We set $R := \operatorname{ord}_{p^\alpha} X$, $S := \operatorname{ord}_{p^\alpha} Y$, so that $X^R \equiv 1 \pmod{p^\alpha}$, $Y^S \equiv 1 \pmod{p^\alpha}$. Then, by (3.22),

$$Y^{12R} \equiv \left(X^R\right)^{24} \equiv 1 \pmod{p^\alpha}, \qquad X^{24S} \equiv \left(Y^S\right)^{12} \equiv 1 \pmod{p^\alpha},$$

which means that $S \mid 12R$ and $R \mid 24S$. But we are interested in

$$\frac{\gamma_\alpha^6(p)}{\gamma_\alpha^3(p)} = \frac{S}{R} = \frac{s}{r},$$

where $r := R/d, s := S/d$, with $d := \gcd(R, S)$. So we have the conditions $s \mid 12r$, $r \mid 24s$, $\gcd(r, s) = 1$. This, in turn, means that s can only be a divisor of 12 and r a divisor of 24. It is now easy to check that the elements of the set R_{18} are the only possible ratios. ∎

Computations show that all 18 values in R_{18} are actually realized by ratios $\gamma_1^6(p)/\gamma_1^3(p)$.

Our next result brings us back to the concept of an α-exceptional prime for M, as defined at the beginning of Section 3. Also recall the numbers $T_\alpha^M(p)$ as defined in (1.10).

Theorem 7. *Let $p \equiv 1 \pmod 6$ be a prime, $\alpha \geqslant 1$ an integer, and let*

$$\frac{\gamma_\alpha^6(p)}{\gamma_\alpha^3(p)} = \frac{A_\alpha(p)}{B_\alpha(p)} \in R_{18}.$$

Then

$$2A_\alpha(p)T_\alpha^3(p) \equiv B_\alpha(p)T_\alpha^6(p) \pmod p. \tag{3.26}$$

Before we prove this result, we note that for $\alpha = 1$ this reduces to the congruence

$$2\gamma_1^6(p)T_1^3(p) \equiv \gamma_1^3(p)T_1^6(p) \pmod p$$

since neither one of $\gamma_1^6(p), \gamma_1^3(p)$ is divisible by p. This congruence was in fact obtained in [4] by different means.

As an immediate consequence of Theorem 7 we get the following result; it comes from the fact that by (3.26), $T_\alpha^3(p)$ and $T_\alpha^6(p)$ are either both zero or both nonzero modulo p.

Corollary 3. *Let $p \equiv 1 \pmod 6$ be a prime and $\alpha \geqslant 1$. Then p is α-exceptional for $M = 3$ if and only if it is α-exceptional for $M = 6$.*

Proof of Theorem 7. We raise the congruence (1.11) to the power 24, obtaining

$$\left(\left(\tfrac{p^{\alpha+1}-1}{3}\right)_p!\right)^{24\gamma_\alpha^3(p)} \equiv 1 + 24T_\alpha^3(p)p^\alpha \pmod{p^{\alpha+1}}. \tag{3.27}$$

The companion identity of (1.11) for $M = 6$, obtained in analogy to the proof of Proposition 2.2 in [4], is

$$\left(\left(\tfrac{p^{\alpha+1}-1}{6}\right)_p!\right)^{\gamma_\alpha^6(p)} \equiv \pm\left(1 + T_\alpha^6(p)p^\alpha\right) \pmod{p^{\alpha+1}}, \tag{3.28}$$

and raising this to the 12th power we get

$$\left(\left(\tfrac{p^{\alpha+1}-1}{6}\right)_p!\right)^{12\gamma_\alpha^6(p)} \equiv 1 + 12T_\alpha^6(p)p^\alpha \pmod{p^{\alpha+1}}. \tag{3.29}$$

Now, using the definition of $A_\alpha(p), B_\alpha(p)$ in the statement of the theorem, we let m be the common value of $A_\alpha(p)\gamma_\alpha^3(p) = B_\alpha(p)\gamma_\alpha^6(p)$. If we raise both sides of (3.27) to the power $A_\alpha(p)$ and (3.29) to the power $B_\alpha(p)$, then the left-hand sides are the mth powers of the two sides of (3.22), respectively (with α replaced by $\alpha + 1$) and are thus congruent to each other modulo $p^{\alpha+1}$. Then the right-hand sides of (3.27), (3.17) give, after the usual binomial expansion,

$$1 + 24A_\alpha(p)T_\alpha^3(p)p^\alpha \equiv 1 + 12B_\alpha(p)T_\alpha^6(p)p^\alpha \pmod{p^{\alpha+1}}.$$

Finally, we subtract 1 from both sides and divide by p^α, which gives (3.26). ∎

4. Tests for exceptionality for $M = 3$, 4 and 6

It can be seen from the definitions of the various functions of p in the criterion (1.10) that determining exceptionality in this way is computationally expensive. This is the case even when $M = 3$, 4 or 6, where the sums $S^M(p)$ can be written, modulo p, in terms of Fermat quotients which are easy to compute.

It is the main purpose of this section to give much simpler tests for exceptionality at all levels for $M = 3$, 4 and 6. These tests then allow us to carry the search for exceptional primes substantially further.

We begin with the cases $M = 3$ and 6; they are somewhat different from the case $M = 4$ which will be treated later in this section. As we will see, most of the key results of the previous section will be used in the proof of our first theorem.

Theorem 8. *Let $p \equiv 1 \pmod 6$ be a prime and u as defined in (3.1)–(3.3). Then for a fixed $\alpha \geqslant 1$, p is α-exceptional for $M = 3$ and also for $M = 6$ if and only if*

$$\left(u - \frac{p}{u} - \frac{p^2}{u^3} - 2\frac{p^3}{u^5} - \cdots - C_{\alpha-1}\frac{p^\alpha}{u^{2\alpha-1}}\right)^{p-1} \equiv 1 \pmod{p^{\alpha+1}}, \tag{4.1}$$

where C_n is the nth Catalan number.

Proof. We assume that p is α-exceptional for $M = 3$ and (by Corollary 3) equivalently for $M = 6$. Then by the definitions of $\gamma_\alpha^3(p)$ and $\gamma_\alpha^6(p)$, together with Theorem 3, we have $p - 1 = q\gamma_\alpha^3(p) = Q\gamma_\alpha^6(p)$ for some $q, Q \in \mathbb{N}$. Then with (3.9), (1.11) and (3.28) we get, after using binomial expansions in numerator and denominator,

$$K_\alpha(p)^{p-1} \equiv \frac{\left(\left(\frac{p^{\alpha+1}-1}{3}\right)_p!\right)^{q\gamma_\alpha^3(p)}}{\left(\left(\frac{p^{\alpha+1}-1}{6}\right)_p!\right)^{2Q\gamma_\alpha^6(p)}} \equiv \frac{1 + qT_\alpha^3(p)p^\alpha}{1 + 2QT_\alpha^6(p)p^\alpha} \pmod{p^{\alpha+1}}, \tag{4.2}$$

where $K_\alpha(p)$ is defined by (3.10), i.e., the left-hand sides of (4.2) and (4.1) are identical. Now, by Theorem 2, exceptionality means $T_\alpha^3(p) \equiv T_\alpha^6(p) \equiv 0 \pmod p$, which implies that the right-most term in (4.2) is congruent to $1 \pmod{p^{\alpha+1}}$, so (4.1) holds.

Conversely, suppose that (4.1) holds. Then (4.1) with (3.9) (or the left congruence of (4.2)) gives

$$\left(\left(\frac{p^{\alpha+1}-1}{3}\right)_p!\right)^{p-1} \equiv \left(\left(\frac{p^{\alpha+1}-1}{6}\right)_p!\right)^{2(p-1)} \pmod{p^{\alpha+1}}.$$

On the other hand, raising both sides of the congruence (3.22) to the (integer) power $(p-1)/6$, we obtain

$$\left(\left(\frac{p^{\alpha+1}-1}{3}\right)_p!\right)^{4(p-1)} \equiv \left(\left(\frac{p^{\alpha+1}-1}{6}\right)_p!\right)^{2(p-1)} \pmod{p^{\alpha+1}}.$$

Combining these last two congruences, we get

$$\left(\left(\frac{p^{\alpha+1}-1}{3}\right)_p!\right)^{3(p-1)} \equiv 1 \pmod{p^{\alpha+1}}.$$

Since $3(p-1) \not\equiv 0 \pmod p$ then $\gamma_{\alpha+1}^3(p) \not\equiv 0 \pmod p$; thus p is α-exceptional for $M = 3$ and by Corollary 3 also for $M = 6$. ∎

For computational purposes, and in view of Theorem 3, the case $\alpha = 1$ is of particular significance; we therefore state it as a separate result.

Corollary 4. *Let $p \equiv 1 \pmod 6$ be a prime and u as defined in* (3.1)–(3.3). *Then p is 1-exceptional for $M = 3$ and also for $M = 6$ if and only if*

$$\left(u - \tfrac{p}{u}\right)^{p-1} \equiv 1 \pmod{p^2}. \tag{4.3}$$

Although in the proof of Theorem 8 the use of the integer u was essential, Theorem 6 shows that it can be replaced by r, where both are defined in (3.1)–(3.3). We now give an elementary proof of this fact in the case $\alpha = 1$, and we also show that in this case we can replace r or u by $2a$, where a is uniquely determined by $p = a^2 + 3b^2$, $a \equiv -1 \pmod 3$.

Lemma 4. *Let $p \equiv 1 \pmod 6$, a as above, and u, r as defined in* (3.1)–(3.3). *Then*

$$\left(r - \tfrac{p}{r}\right)^3 \equiv \left(u - \tfrac{p}{u}\right)^3 \equiv \left(2a - \tfrac{p}{2a}\right)^3 \pmod{p^2}. \tag{4.4}$$

Proof. To prove the first congruence, we note that it is equivalent to

$$r^3 - 3rp \equiv u^3 - 3up \pmod{p^2},$$

or, upon rearranging and factoring, to

$$(r-u)(r^2 + ru + u^2) \equiv 3p(r-u) \pmod{p^2}. \tag{4.5}$$

If $r = u$, the congruences are trivially true; so we consider the case $r \neq u$. In this case r and u are given by (3.2) or (3.3), namely $r = -a \pm 3b$, $u = -a \mp 3b$. Upon expanding we obtain in both cases $r^2 + ru + u^2 = 3(a^2 + 3b^2) = 3p$, so that (4.5) holds again.

In analogy to (4.5) the second congruence in (4.4) is equivalent to

$$(u-2a)(u^2 + 2au + 4a^2) \equiv 3p(u-2a) \pmod{p^2}. \tag{4.6}$$

Here we have either $u = 2a$, in which the congruences hold trivially, or u is defined by (3.2) or (3.3), namely $u = -a \pm 3b$. We then obtain $u^2 + 2au + 4a^2 = 3(a^2 + 3b^2) = 3p$, and (4.6) holds again, and the proof is complete. ∎

By raising all three terms in (4.4) to the (integer) power $\frac{p-1}{3}$, we see that Corollary 4 remains true if in (4.3) we replace u by r or by $2a$. The latter case will be particularly useful for computations, and by expanding the left-hand side we immediately obtain the following criterion.

Corollary 5. *Let $p \equiv 1 \pmod 6$ be a prime and write $p = a^2 + 3b^2$ with $a \equiv -1 \pmod 3$. Then p is 1-exceptional for $M = 3$ and also for $M = 6$ if and only if*

$$(2a)^{p-3}\left((2a)^2 + p\right) \equiv 1 \pmod{p^2}. \tag{4.7}$$

In our final section we will make a few remarks on how to use this congruence in the search for 1-exceptional primes. To complete the current section, we prove the $M = 4$ analogue of Theorem 8. The proof, however, will be quite different.

Theorem 9. *Let $p \equiv 1 \pmod 4$ be a prime and write $p = a^2 + b^2$, where a and b are integers with $a \equiv 1 \pmod 4$. Then for a fixed $\alpha \geqslant 1$, p is α-exceptional for $M = 4$ if and only if*

$$\left(2a - \frac{p}{2a} - \frac{p^2}{(2a)^3} - \cdots - C_{\alpha-1}\frac{p^\alpha}{(2a)^{2\alpha-1}}\right)^{p-1} \equiv 1 \pmod{p^{\alpha+1}}, \tag{4.8}$$

where C_n is the nth Catalan number.

Proof. We use Theorem 7 of [3], namely

$$\frac{\left(\frac{p^{\alpha+1}-1}{2}\right)_p!}{\left(\left(\frac{p^{\alpha+1}-1}{4}\right)_p!\right)^2} \equiv G_\alpha(p) \pmod{p^{\alpha+1}}. \tag{4.9}$$

where

$$G_\alpha(p) := 2a - \frac{p}{2a} - \frac{p^2}{(2a)^3} - \cdots - C_{\alpha-1}\frac{p^\alpha}{(2a)^{2\alpha-1}}.$$

In analogy to the argument following (3.23), we note that by a result of D. H. Lehmer [11, Theorem 4], the Gauss factorial $(\frac{1}{2}(p^{\alpha+1}-1))_p!$ has $\frac{1}{2}\varphi(p^{\alpha+1})$ factors in its defining product. This number of factors is obviously an integer; in fact it is easily seen to be an even integer as $p \equiv 1 \pmod 4$. Therefore the above Gauss factorial is by symmetry congruent modulo $p^{\alpha+1}$ to the product of all integers from $\frac{1}{2}(p^{\alpha+1}-1)+1$ to $p^{\alpha+1}-1$, excluding the multiples of p. Thus we have

$$\left(\left(\frac{p^{\alpha+1}-1}{2}\right)_p!\right)^2 \equiv \left(p^{\alpha+1}-1\right)_p! \equiv -1 \pmod{p^{\alpha+1}},$$

again by the Gauss-Wilson theorem (1.2). We raise both sides of (4.9) to the 4th power and combine it with the square of this last congruence, obtaining

$$\left(\left(\frac{p^{\alpha+1}-1}{4}\right)_p!\right)^8 \equiv \frac{1}{G_\alpha(p)^4} \pmod{p^{\alpha+1}}.$$

Since p is relatively prime to 8 and to 4, we see that

$$\operatorname{ord}_{p^{\alpha+1}}\left(\left(\frac{p^{\alpha+1}-1}{4}\right)_p!\right) \not\equiv 0 \pmod p$$

(which, in light of Theorem 3, is equivalent to p being α-exceptional for $M = 4$) if and only if

$$\operatorname{ord}_{p^{\alpha+1}} G_\alpha(p) \not\equiv 0 \pmod p. \tag{4.10}$$

As before, we have by Euler's generalization of Fermat's little theorem,

$$G_\alpha(p)^{p^\alpha(p-1)} \equiv 1 \pmod{p^{\alpha+1}},$$

which immediately implies that (4.10) holds if and only if (4.8) holds, and we are done. ■

For $\alpha = 1$ we get an obvious analogue of Corollary 4. A 1-exceptionality test for $M = 4$ would then be identical with the congruence (4.7), but for the prime p and the integer a satisfying $p = a^2 + b^2$, $a \equiv 1 \pmod 4$.

5. Further consequences

We begin by briefly returning to the general case of $M \geqslant 2$. In Theorem 2 we defined the integer $T_\alpha^M(p)$ and recalled that a prime $p \equiv 1 \pmod M$ is α-exceptional for M if and only if $T_\alpha^M(p) \equiv 0 \pmod p$. However, in the case where $T_\alpha^M(p) \not\equiv 0 \pmod p$ (for some $\alpha \geqslant 1$) we did not say anything about the actual values (modulo p) of the $T_\beta^M(p)$, $\beta \geqslant \alpha$. Far from being arbitrary nonzero, these values behave in a very regular fashion, namely

$$\{T_\beta^M(p)\}_{\beta\geqslant\alpha} = \begin{cases} \{T, T, T, \ldots\}, \text{or} \\ \{T, \frac{1}{2}T, T, \frac{1}{2}T, \ldots\}, \text{or} \\ \{T, 2T, T, 2T, \ldots\}, \end{cases} \tag{5.1}$$

where $T = T_\alpha^M(p)$. We skip the proof of this fact, which is a fairly straightforward application of congruences such as (1.9) and a general version of (1.11).

In some special cases for $M = 3$ we can actually say more. We begin by quoting the following result from the forthcoming paper [7]; see also [5, p. 824]. We will refer to the integer r as defined in (3.1)–(3.3).

(i) Primes $p \equiv 1 \pmod 6$ for which the order of $\frac{p-1}{3}!$ is 1 or 3 are exactly those that are generated by $p = 3x^2 + 3x + 1$ and $x \equiv 1 \pmod 3$; equivalently, they are exactly those for which $r = 1$.

(ii) Primes $p \equiv 1 \pmod 6$ for which $\operatorname{ord}_p(\frac{p-1}{3}!) = 9$ are exactly those that are generated by the same quadratic $p = 3x^2 + 3x + 1$, but with $x \equiv 0$ or $2 \pmod 3$; equivalently, they are exactly those for which $\operatorname{ord}_p r = 3$.

Now, in connection with property (5.1), these primes also satisfy the following:

Theorem 10. *If the prime $p \equiv 1 \pmod 6$ satisfies $\operatorname{ord}_p(\frac{p-1}{3}!) = 3^\nu$ for $\nu = 0, 1$ or 2, then $T_1^3(p) \equiv 3^{\nu-1} \pmod p$. In particular, no prime of the form $p = 3x^2+3x+1$, $x \in \mathbb{N}$, is 1-exceptional for $M = 3$ and $M = 6$.*

Proof. By (1.11) with $\alpha = 1$ we have

$$\left(\left(\frac{p^2-1}{3}\right)_p!\right)^{\gamma_1^3(p)} \equiv 1 + T_1^3(p)p \pmod{p^2}, \tag{5.2}$$

and combining (3.24) for $\alpha = 2$ with (3.6) and (3.7) for $\alpha = 1$, we get

$$\left(\left(\tfrac{p^2-1}{3}\right)_p!\right)^3 \equiv \frac{1}{r - \frac{p}{r}} \pmod{p^2}. \tag{5.3}$$

We first assume that $\nu = 0$ or 1. Then by case (i) preceding the theorem we have $r = 1$, and thus (5.3) gives

$$\left(\left(\tfrac{p^2-1}{3}\right)_p!\right)^3 \equiv 1 + p \pmod{p^2}. \tag{5.4}$$

When $\nu = 0$, i.e., $\gamma_1^3(p) = 1$, we cube (5.2), and its right-hand side becomes $1+3T_1^3(p)p \pmod{p^2}$. Comparing this with (5.4), we immediately get $T_1^3(p) \equiv 1/3 \pmod{p}$, as desired. Similarly, when $\nu = 1$, i.e., $\gamma_1^3(p) = 3$, then (5.2) and (5.4) immediately give $T_1^3(p) \equiv 1 \pmod{p}$, again as desired.

Second, we assume that $\nu = 2$; then by case (ii) above $\operatorname{ord}_p r = 3$. Now an easy binomial expansion gives $(r - p/r)^3 \equiv r^3 - 3pr \pmod{p^2}$, so if we can show that

$$r^3 - 3pr \equiv 1 - 3p \pmod{p^2}, \tag{5.5}$$

then by cubing both sides of (5.3) we would have

$$\left(\left(\tfrac{p^2-1}{3}\right)_p!\right)^9 \equiv \frac{1}{1-3p} \equiv 1 + 3p \pmod{p^2}.$$

Comparing this with (5.2), where $\gamma_1^3(p) = 9$, we immediately get $T_1^3(p) \equiv 3 \pmod{p}$, as desired.

It remains to verify (5.5). From $r^3 \equiv 1 \pmod{p}$ we have $(r-1)(r^2+1+1) \equiv 0 \pmod{p}$. But $r \not\equiv 1 \pmod{p}$ since the order is 3, so we have $r^2 + r + 1 = mp$ for some $m \in \mathbb{N}$. First we note that m has to be odd since $r^2 + r + 1$ is. Next, since $r \equiv 1 \pmod{3}$ (see (3.4)) we have $3 \mid r^2 + r + 1$, so $m = 1$ is impossible. Finally, from $4p = r^2 + 3s^2$ (see (3.4) again) we have $r^2 < 4p$ and thus

$$r^2 + r + 1 < 4p + 2\sqrt{p} + 1 = \left(4 + \frac{2}{\sqrt{p}} + \frac{1}{p}\right) p,$$

so $m < 5$ for $p \geqslant 7$. This leaves $m = 3$ as the only possibility, i.e., we have $r^2 + r + 1 = 3p$. But this implies

$$r^3 - 3pr = r^3 - r(r^2 + r + 1) = -r^2 - r = 1 - 3p,$$

so (5.5) is actually an equality.

The final statement of the theorem follows from the remarks preceding it, and from Theorem 2 and Corollary 3. ■

We now turn to a class of primes, generated in a similar fashion to those in Theorem 10, that have the opposite property in that they are *all* 1-exceptional. In [4] we gave a rather involved proof of the following result which is now an easy consequence of Corollary 4.

Corollary 6. *Every prime p such that $p^2 = 3x^2 + 3x + 1$ for some integer x is 1-exceptional for $M = 3$ and $M = 6$.*

Proof. In [4, p. 169] we showed that the given primes satisfy

$$\left(r - \tfrac{p}{r}\right)^6 \equiv -1 \pmod{p^2}. \tag{5.6}$$

In particular, this congruence shows that -1 is a quadratic residue modulo p, and thus $p \equiv 1 \pmod 4$. This means that $\frac{1}{6}(p-1)$ is even, and from (5.6) we get

$$\left(r - \tfrac{p}{r}\right)^{p-1} \equiv (-1)^{\frac{p-1}{6}} = 1 \pmod{p^2}.$$

Corollary 4 now shows that p is 1-exceptional for $M = 3$ and $M = 6$. ■

Primes that satisfy $p^2 = 3x^2 + 3x + 1$ account for all of the entries in Table 1 for $M = 3$ and $M = 6$, with the sole exception of $p = 76\,543$. Following Theorem 3 we remarked that we checked all entries in Table 1 and found that they are not 2-exceptional. For $M = 3$ and $M = 6$, all entries except $p = 76\,543$ are of the type already considered in Corollary 6 above. For these primes we can actually *prove* that they are not 2-exceptional.

Theorem 11. *Suppose the prime p is such that $p^2 = 3x^2 + 3x + 1$ for some integer x. Then p is not 2-exceptional for $M = 3$ or $M = 6$.*

Before we can use Theorems 8 and 6 to prove this result, we need the following technical lemma.

Lemma 5. *Let p be a prime such that $p^2 = 3x^2 + 3x + 1$ for some integer x, and let r be defined by* (3.1)–(3.3)*. Then*

$$r^2(r^2 - 3p)^2 = (p+1)^2(2p-1). \tag{5.7}$$

Proof. The equation $p^2 = 3x^2 + 3x + 1$ can be rewritten in the form of the Pell equation $(2p)^2 - 3(2x+1)^2 = 1$, and from the theory of these equations (see, e.g., [14, Section 7.8]) we get

$$p = \frac{1}{2}A_{2k-1}, \tag{5.8}$$

where the sequence $\{A_j\}$ is defined by $A_0 = 1$, $A_1 = 2$, and

$$A_{n+1} = 4A_n - A_{n-1} \qquad (n \geqslant 1). \tag{5.9}$$

Properties of this well-known sequence can be found, e.g., in [15, A001075], and they include the identities

$$2A_{k-1}A_k = A_{2k-1} + 2, \qquad A_{k-1}A_{k+1} - A_k^2 = 3 \qquad (k \geqslant 1); \tag{5.10}$$

see also [4, p. 165] for further properties and a small table. Combining the second identity in (5.10) with (5.9), we obtain

$$A_k^2 - 4A_kA_{k-1} + A_{k-1}^2 + 3 = 0 \qquad (k \geqslant 1), \tag{5.11}$$

which will also be useful.

Now, in addition to p in (5.8), the integer r can also be expressed in terms of the sequence $\{A_j\}$; see [4, Lemma 9]: If $p = \frac{1}{2}A_{2k-1}$ is a prime, then

$$r = \begin{cases} (-1)^k A_k & \text{if} \quad 2k-1 \equiv 1 \pmod 3, \\ (-1)^{k-1} A_{k-1} & \text{if} \quad 2k-1 \equiv -1 \pmod 3. \end{cases} \tag{5.12}$$

We are now ready to prove (5.7). We first consider the case $2k-1 \equiv 1 \pmod 3$. Then $r^2 = A_k^2$, and with (5.8) the identity (5.7) is equivalent to

$$A_k^2 \left(A_k^2 - \tfrac{3}{2}A_{2k-1}\right)^2 = \left(\tfrac{1}{2}A_{2k-1} + 1\right)^2 (A_{2k-1} - 1)\,.$$

Using the first identity in (5.10) to replace all occurrences of A_{2k-1}, we obtain after dividing both sides by A_k^2,

$$\left(A_k^2 - 3A_kA_{k-1} + 3\right)^2 = A_{k-1}^2 \left(2A_kA_{k-1} - 3\right). \tag{5.13}$$

Applying (5.11), the left-hand side of (5.13) becomes

$$\left(A_{k-1}A_k - A_{k-1}^2\right)^2 = A_{k-1}^2 \left(A_k^2 - 2A_kA_{k-1} + A_{k-1}^2\right),$$

and upon using (5.11) a second time, we see that this gives the right-hand side of (5.13). This completes the proof of (5.7) when $2k-1 \equiv 1 \pmod 3$.

In the second case, (5.12) gives $r^2 = A_{k-1}^2$, and the proof will be very similar, with only a small shift in the subscripts. ∎

Proof of Theorem 11. We first expand the left-hand term of the following congruence, reducing modulo p^3; then we use (5.7) and expand and reduce again:

$$\begin{aligned} \left(r - \frac{p}{r} - \frac{p^2}{r^3}\right)^6 &\equiv r^6 - 6r^4p + 9r^2p^2 = r^2\left(r^2 - 3p\right)^2 \pmod{p^3} \\ &= (p+1)^2(2p-1) \equiv 3p^2 - 1 \pmod{p^3}. \end{aligned}$$

Now we raise the left- and right-most sides to the power $\frac{1}{6}(p-1)$, noting that this is an even integer, as we saw in the proof of Corollary 6. Then expanding and reducing again, we get

$$\begin{aligned} \left(r - \frac{p}{r} - \frac{p^2}{r^3}\right)^{p-1} &\equiv \left(1 - 3p^2\right)^{\frac{p-1}{6}} \equiv 1 - \frac{p-1}{6}3p^2 \pmod{p^3} \\ &\equiv 1 + \frac{1}{2}p^2 \not\equiv 1 \pmod{p^3}. \end{aligned} \tag{5.14}$$

This means that, by Theorem 6 and Theorem 8, p is not 2-exceptional for $M = 3$ and $M = 6$. ∎

We finish this section with a few further remarks concerning primes that satisfy $p^2 = 3x^2 + 3x + 1$ for an integer x. First, by reducing (5.14) modulo p^2, we immediately get another proof of Corollary 6.

Next we note that as part of the very different proof in [4] of this last corollary, we showed that $\gamma_1^3(p) = \gamma_2^3(p) = 36$ when $p \neq 13$, and the common value is 12 when $p = 13$. Using this, together with much of the work in the previous two proofs, one can also show that $T_2^3(p) \equiv 6 \pmod{p}$ when $p \neq 13$, and $T_2^3(13) \equiv 4 \pmod{13}$.

Our final remark concerns the identity (5.8) which provides an easy way of obtaining primes satisfying $p^2 = 3x^2 + 3x + 1$. In [4, Lemma 7] we showed that a necessary condition for the primality of p is the primality of $2k - 1$. It turns out that p is indeed prime for all odd primes $2k - 1 \leqslant 19$ (tabulated in [4, p. 166]), the first four of which appear in Table 1 of the present paper. But the next values $2k - 1$ for which p is prime are only 79, 151, 199, 233, 251, 317, 816 and 971; we also have probable primes for $2k - 1 = 3049$, 7451 and 7487. There are no more with $2k - 1 < 10\,000$, and the largest of these probable primes has 4282 decimal digits. It is reasonable to conjecture that there are infinitely many such primes.

6. Some final remarks

1. The quotient (1.3) is not always an integer unless $p \equiv 1 \pmod{M}$, but it is worth mentioning that by considering the floor function $\lfloor \frac{p^\alpha - 1}{M} \rfloor$, one can also define an appropriate analogue of the Gauss factorial in (1.3) for p in other residue classes modulo M. Such modified Gauss factorials and their orders were in fact studied in [4], Section 3. However, in the present paper we have, for the sake of simplicity and brevity, restricted our attention to primes $p \equiv 1 \pmod{M}$.

2. We conclude this paper with some notes on computations in the cases $M = 3, 6$ and $M = 4$. In both cases the congruence (4.7) is most convenient to use; when $M = 4$, however, we have $p = a^2 + b^2$ and $a \equiv 1 \pmod 4$, as opposed to the hypothesis of Corollary 5.

In practice we let a and b run through their respective residue classes of relevance, and then test (4.7) with p *defined* as $a^2 + 3b^2$ (respectively $a^2 + b^2$), whether or not p is prime. Only when a solution of (4.7) was found, we tested p for primality.

In this way we were able to check for 1-exceptionality in the case $M = 3$ (and thus also $M = 6$) for $p < 10^{12}$, and in the the case $M = 4$ for $p < 10^{11}$. The relevant entries in Table 1 are complete up to these limits.

The computations were all done with the computer algebra system Maple. Using our new exceptionality tests (as opposed to Theorem 2), we were able to reach the former search limits of $4 \cdot 10^8$ in under three minutes in each of the two cases. The new search limits in the two cases were reached in about 2 days of CPU time each, on a standard desktop computer. Obviously, one could reach higher search limits with a specially designed program, and also use opportunities for parallelization (as we did with Maple). However, the computational aspects were not the main focus of this paper.

Acknowledgments. We thank the anonymous referee for a very careful reading of this paper, and for helpful suggestions that led to its improvement.

References

[1] B.C. Berndt, R.J. Evans, and K.S. Williams, *Gauss and Jacobi Sums*, Wiley, New York, 1998.

[2] J.B. Cosgrave and K. Dilcher, *Extensions of the Gauss-Wilson theorem*, Integers **8** (2008) A39; available at http://www.integers-ejcnt.org/vol8.html.

[3] J.B. Cosgrave and K. Dilcher, *Mod p^3 analogues of theorems of Gauss and Jacobi on binomial coefficients*, Acta Arith. **142** (2010), no. 2, 103–118.

[4] J.B. Cosgrave and K. Dilcher, *The multiplicative orders of certain Gauss factorials*, Int. J. Number Theory **7** (2011), 145–171.

[5] J.B. Cosgrave and K. Dilcher, *An Introduction to Gauss Factorials*, Amer. Math. Monthly **118** (2011), 810–828.

[6] J.B. Cosgrave and K. Dilcher, *The Gauss–Wilson theorem for quarter-intervals*, Acta Math. Hungar. **142** (2014), no. 1, 199–230.

[7] J.B. Cosgrave and K. Dilcher, *A role for generalized Fermat numbers*, Math. Comp. (to appear).

[8] L.E. Dickson, *History of the Theory of Numbers. Volume I: Divisibility and Primality*, Chelsea, New York, 1966.

[9] Y. Gallot, Private communication, June, 2009.

[10] R.H. Hudson and K.S. Williams, *Binomial coefficients and Jacobi sums*, Trans. Amer. Math. Soc. **281** (1984), no. 2, 431–505.

[11] D.H. Lehmer, *The distribution of totatives*, Canad. J. Math. **7** (1955), 347–357.

[12] E. Lehmer, *On congruences involving Bernoulli numbers and the quotients of Fermat and Wilson*, Ann. of Math. Oxford Ser. **3**9 (1938), 350–360.

[13] L.J. Mordell, *The congruence* $(p-1/2)! \equiv \pm 1 \pmod{p}$, Amer. Math. Monthly **68** (1961), 145–146.

[14] I. Niven, H.S. Zuckerman, and H.L. Montgomery, *An Introduction to the Theory of Numbers*, 5th ed., Wiley, 1991.

[15] *The On-Line Encyclopedia of Integer Sequences*, http://oeis.org/.

Addresses: John B. Cosgrave: 79 Rowanbyrn, Blackrock, County Dublin, Ireland;
Karl Dilcher: Department of Mathematics and Statistics, Dalhousie University, Halifax, Nova Scotia, B3H 3J5, Canada.

E-mail: jbcosgrave@gmail.com, dilcher@mathstat.dal.ca

Received: 28 October 2014; **revised:** 7 May 2015

Functiones et Approximatio
54.1 (2016), 95–113
doi: 10.7169/facm/2016.54.1.8

APPROXIMATION AND GENERALIZED GROWTH OF SOLUTIONS TO A CLASS OF ELLIPTIC PARTIAL DIFFERENTIAL EQUATIONS

Susheel Kumar, Girja S. Srivastava

Abstract: In the present paper, we study the approximation and growth of solutions to a class of elliptic partial differential equations. The characterizations of generalized order and generalized type of solutions to a class of elliptic partial differential equations have been obtained in terms of approximation errors.

Keywords: Helmholtz type equation, regular solution, analytic function, approximation errors, generalized order, generalized type.

1. Introduction

Following McCoy [4] , we first give some definitions. A Helmholtz type equation is given by

$$\pounds[H] := [\partial_{rr} + r^{-1}\partial_r + r^{-2}\partial_{\theta\theta} + F(r^2)]H(r,\theta) = 0. \tag{1.1}$$

Here (r,θ) are polar coordinates and F is an entire function. Let $H(r,\theta) = H(r,e^{i\theta})$ be a regular solution of (1.1) in some sufficiently small star-shaped neighborhood Ω about origin. Let R be the radius of convergence of this regular solution. Following Bergman [1], we have

$$H(r,\theta) = \mathbb{B}[f(z)] \;=\; \int_{-1}^{+1} E(r^2,t)\, f(\sigma)\, d\mu(t)\ ,$$

where $z = re^{i\theta} \in \Omega$,$\sigma = z(1-t^2)/2$, $d\mu(t) = (1-t^2)^{-1/2}dt$, and the associated function f is analytic for $2z \in \Omega$. The Taylor series expansion of the kernel $E(r^2,t)$ is given as

$$E(r^2,t) = 1 + \sum_{n=1}^{\infty} t^{2n} Q^{(2n)}(r^2).$$

2010 Mathematics Subject Classification: primary: 30B10; secondary: 30D20, 32K05

For a fixed $r \geqslant 0$, the kernel $E(r^2, t)$ is analytic for $t \in [-1, +1]$ and for every fixed $t \in [-1, +1]$, it is entire for $r \geqslant 0$. The Taylor coefficients $Q^{(2n)}(r^2)$ are entire function solutions of the system

$$\frac{\partial \left(Q^{(2)}(r^2)\right)}{\partial r^2} + 2F(r^2) = 0, \qquad Q^{(0)}(r^2) = 1,$$

$$(2n+1)\frac{\partial \left(Q^{(2n+2)}(r^2)\right)}{\partial r^2} + 2\frac{\partial \left(r^2 Q^{(2n)}(r^2)\right)}{\partial r^2} + F(r^2)Q^{(2n)}(r^2) - n\frac{\partial \left(Q^{(2n)}(r^2)\right)}{\partial r^2} = 0,$$

$$Q^{(2n+2)}(r^2)|_{r=0} = 0, \qquad n = 1, 2, 3 \ldots$$

McCoy [4] defined the basic set of particular solutions

$$\Phi_n(r, e^{i\theta}) = [r^n G_n(r^2)/R^n G_n(R^2)]e^{in\theta}$$

normalized by the conditions

$$\Phi_n(r, e^{i\theta}) = e^{in\theta}, \qquad n = 0, 1, 2, 3 \ldots$$

Here

$$G_n(r^2) = \int_{-1}^{+1} E(r^2, t)\ \left(1 - t^2\right)^n d\mu(t).$$

This set is complete relative to compact convergence on a disk $D_R = \{z : |z| < R\}$. Let $\mathrm{Im}(D_R)$ be the space of regular solutions of (1.1) on D_R. Then $H \in \mathrm{Im}(D_R)$ has the expansion in a uniformly convergent series

$$H(r, e^{i\theta}) = \sum_{n=0}^{\infty} a_n \Phi_n(r, e^{i\theta}),$$

where $\{a_n\}$ is a sequence of real numbers. If $A(D_R)$ is the space of analytic functions on D_R, then $f \in A(D_R)$ has the Taylor series expansion

$$f(z) = \sum_{n=0}^{\infty} a_n\, z^n, \qquad z \in D_R.$$

McCoy [4] associated H with the analytic function f by defining an integral operator as given below:

$$H(r, e^{i\theta}) = T_\varepsilon[f(z)] = \frac{1}{2\pi i}\int_{|\zeta|=1-\varepsilon} K_R(\zeta) f(z/\zeta) d\zeta/\zeta, \qquad z = re^{i\theta}/R,$$

where $\varepsilon > 0$ is arbitrarily small. The kernel for this integral operator defined over the basis $\{\Phi_n\}$ is given by

$$K_R(\zeta) = \sum_{n=0}^{\infty} \zeta^n [G_n(r^2)/G_n(R^2)].$$

For $\varepsilon > 0$, there exists an integer $N(\varepsilon)$ such that for all $n \geqslant N(\varepsilon)$, we have

$$(1-\varepsilon) \leqslant |G_n(r^2)/G_n(R^2)| \leqslant (1+\varepsilon).$$

Thus we can say that the kernel of this operator has uniformly convergent expansion. The above integral operator maps the function $f \in A(D_{R(1-\varepsilon)})$ onto regular solution $H \in \mathrm{Im}(D_{R(1-\varepsilon)})$ and the disk of regularity of H coincides with the disk of analyticity of f. The maximum modulus of H on D_r is given by

$$M(r,H) = \max\{|H(s,e^{i\theta})| : s \leqslant r\}.$$

Let H be regular on the closure Δ^* of the unit disk $\Delta = \{z : |z| < 1\}$ and define the norm of H as

$$||H|| = \begin{cases} ||H||_p = \left[\iint_{\Delta^*} |H|^p r dr d\theta\right]^{1/p}, & 1 \leqslant p < \infty, \\ ||H||_\infty = \lim\limits_{r\to 1^-} M(r,H). \end{cases}$$

The spaces of polynomial solutions of fixed degree $n = 0, 1, 2, ...$ are given by

$$\Pi_n = \left\{ P : P(r,e^{i\theta}) = \sum_{k=0}^{n} c_k \Phi_k(r,e^{i\theta}),\ c_k \in \mathbb{R} \right\}.$$

We define the approximation errors $E_n(H)$ (see [4]) by

$$E_n(H) = \inf_P \{||H-P|| : P \in \Pi_n\}, \qquad n = 0, 1, 2....$$

The definition of order and type for regular solution H are the same as those for the associated analytic function f (see [4], pp. 209). Hence the order ρ of regular solution H on D_R is given by

$$\rho = \lim_{r\to R^-} \sup \frac{\ln^+ \ln^+ M(r,H)}{\ln[R/(R-r)]},$$

where

$$\ln^+ x = \begin{cases} \ln x, & x > 1; \\ 0, & 0 < x \leqslant 1. \end{cases}$$

Further, for $0 < \rho < \infty$ the type σ of regular solution H on D_R is given by

$$\sigma = \lim_{r\to R^-} \sup \frac{\ln^+ M(r,H)}{[R/(R-r)]^\rho}.$$

McCoy [4] obtained the characterizations of order and type of function H in terms of approximation errors. Later, in [5], using the concept of index, McCoy studied the growth of entire solutions of the Helmoltz equation. Using the concept of (p,q) growth, Kumar [3] studied the relation between the growth and Chebyshev approximation of entire function solutions of Helmoltz equation. Srivastava and Kumar [7] obtained the characterizations of generalized growth of function H in terms of approximation errors and Taylor series coefficients It is clear from the above that the definition of σ is not valid if the order $\rho = \infty$. For such cases, following Janik [2] and Seremeta [6] we define the generalized order and generalized type of function H. Hence, let L^0 denote the class of functions h satisfying the following conditions:

(i) h is defined on $[a,\infty)$ and is positive, strictly increasing, differentiable and $h(x)$ tends to ∞ as $x \to \infty$,

(ii) $\lim\limits_{x\to\infty} \frac{h\{(1+1/\psi(x))x\}}{h(x)} = 1$, for every function ψ such that $\psi(x) \to \infty$ as x tends to ∞.

(iii) let Λ denote the class of functions h satisfying condition (i) and

$$\lim_{x\to\infty} \frac{h(cx)}{h(x)} = 1, \qquad c > 0,$$

i.e., h is slowly increasing.

For $\alpha \in \Lambda$ and $\beta \in L^0$ we define the generalized order of H as

$$\rho(\alpha,\beta,H) = \lim_{r\to R^-} \sup \frac{\alpha[\ln^+ M(r,H)]}{\beta[R/(R-r)]}. \tag{1.2}$$

Further, for $\alpha,\beta,\gamma \in \Lambda$ and $0 < \rho < \infty$, we define the generalized type of H as

$$\sigma(\alpha,\beta,\gamma,H) = \lim_{r\to R^-} \sup \frac{\alpha[\ln^+ M(r,H)]}{\beta\{[\gamma\{R/(R-r)\}]^\rho\}}. \tag{1.3}$$

If $\rho(\alpha,\beta,H)$ defined as above is zero then the analytic function is of generalized order zero and $\sigma(\alpha,\beta,\gamma,H)$ is no longer defined. For such functions we give the modified definition of generalized order. Hence for $\alpha(x) \in \Lambda$, we define the generalized order $\rho(\alpha,H), (0 \leqslant \rho(\alpha,H) < \infty)$ of H on D_R as

$$\rho(\alpha,H) = \lim_{r\to R^-} \sup \frac{\alpha\left[\ln^+ M(r,H)\right]}{\alpha\left[\ln\{R/(R-r)\}\right]}. \tag{1.4}$$

Also for $\beta(x) \in L^0$ and $1 < \rho(\alpha,H) < \infty$, we define the generalized type $\sigma(\beta,\rho,H)$ of H on D_R as

$$\sigma(\beta,\rho,H) = \lim_{r\to R^-} \sup \frac{\beta\left[\ln^+ M(r,H)\right]}{(\beta\left[\ln\{R/(R-r)\}\right])^\rho}. \tag{1.5}$$

In the present paper we have obtained the characterizations of generalized order and type defined by (1.2) and (1.3). We have also obtained the characterizations of generalized slow growth of function H in terms of approximation errors.

2. Generalized (α, β)-growth

We now prove

Theorem 1. *Let H be a regular solution of (1.1) having the series expansion $H(r, e^{i\theta}) = \sum_{n=0}^{\infty} a_n \Phi_n(r, e^{i\theta})$. For $\alpha \in \Lambda, \beta \in L^0$ and positive numbers x and μ_1, set $U(x, \mu_1) = \beta^{-1}\{\mu_1 \alpha(x)\}$. Assume that $\alpha\,(x/U(x, \mu_1)) \cong [1 + o(x)]\alpha(x)$ as $x \to \infty$. Then H is the restriction of a solution H_1 whose disk of regularity is $D_R(R > 1)$ and having generalized order $\rho(0 < \rho < \infty)$ if and only if*

$$\rho = \rho(\alpha, \beta, H) = \lim_{n\to\infty} \sup \frac{\alpha(n)}{\beta\left\{n/\ln^+ (E_n(H)R^n)\right\}}. \tag{2.1}$$

Proof. Write

$$\eta_1 = \lim_{n\to\infty} \sup \frac{\alpha(n)}{\beta\left\{n/\ln^+ (E_n(H)R^n)\right\}}. \tag{2.2}$$

Now first we prove that $\eta_1 \leqslant \rho$. From (1.2), for $\mu_1 > \rho$ and r sufficiently close to R, we have

$$\log^+ M(r, H_1) \leqslant \alpha^{-1}[\mu_1 \beta\{R/(R - r)\}].$$

Let $\varepsilon > 0$ be arbitrary such that $\upsilon = (R^{-1} + \varepsilon) < 1$. Following McCoy ([4], pp.208), we have

$$E_k(H) \leqslant \frac{\pi K(\varepsilon)\upsilon^k}{1 - \upsilon}; \qquad k = n, n + 1, ...,$$

where $K(\varepsilon)$ is a finite positive number. Let us put $r = \upsilon^{-1}$. Then $1 < r < R$. For sufficiently small ε, r is close to R and $\pi K(\varepsilon) \leqslant M(r, H)$. Hence we have

$$E_k(H) \leqslant \frac{M(r, H)}{(r - 1)r^{k-1}} \leqslant \frac{M(r, H_1)}{(r - 1)r^{k-1}}, \qquad 1 < r < R,\ k \geqslant n. \tag{2.3}$$

Hence for every r sufficiently close to R and large n, we get

$$\ln^+ (E_n(H)R^n) \leqslant O(1) - n \ln(r/R) + \alpha^{-1}[\mu_1 \beta\{R/(R - r)\}].$$

Putting

$$r = r_n = R\left[1 - 1/U\left(n/U(n, \mu_1^{-1}), \mu_1^{-1}\right)\right],$$

we get

$$\ln^+ (E_n(H)R^n) \leqslant O(1) - n \ln\left[1 - 1/U\left(n/U(n, \mu_1^{-1}), \mu_1^{-1}\right)\right] + n/U(n, \mu_1^{-1}).$$

Now using the properties of logarithm and assumptions of the theorem for $\alpha(x)$ and $\beta(x)$, we get for sufficiently large values of n,

$$\ln^+ (E_n(H)R^n) \leqslant C_1 \frac{n}{\beta^{-1}\left\{\mu_1^{-1}\alpha(n)\right\}},$$

where C_1 is a positive constant. Hence by using the properties of β, we get

$$\frac{\alpha(n)}{\beta\left\{n/\ln^+ (E_n(H)R^n)\right\}} \leqslant \mu_1.$$

Now proceeding to limits as $n \to \infty$, we get $\eta_1 \leqslant \mu_1$. Since $\mu_1 > \rho$ is arbitrary, therefore we get $\eta_1 \leqslant \rho$.

Now we will prove that $\rho \leqslant \eta_1$. Let us assume that $0 \leqslant \eta_1 < \infty$ otherwise for $\eta_1 = \infty$, the inequality obviously holds. Therefore for a given $\varepsilon > 0$ there exists a positive integer n_0 such that for all $n > n_0$, we have

$$0 \leqslant \frac{\alpha(n)}{\beta\left\{n/\ln^+ (E_n(H)R^n)\right\}} \leqslant \eta_1 + \varepsilon = \eta_1^*$$

or

$$E_n(H)r^n \leqslant r^n R^{-n} \exp\left[n/\beta^{-1}\left\{(\eta_1^*)^{-1}\alpha(n)\right\}\right]. \tag{2.4}$$

Now from the property of maximum modulus, we have

$$M(r,H) \leqslant \sum_{n=0}^{\infty} E_n(H)r^n$$

or

$$M(r,H) \leqslant \sum_{n=0}^{n_0} E_n(H)r^n + \sum_{n=n_0+1}^{\infty} r^n R^{-n} \exp\left[n/\beta^{-1}\left\{(\eta_1^*)^{-1}\alpha(n)\right\}\right]$$

or

$$M(r,H) \leqslant A_1 r^{n_0} + \sum_{n=n_0+1}^{\infty} r^n R^{-n} \exp\left[n/\beta^{-1}\left\{(\eta_1^*)^{-1}\alpha(n)\right\}\right], \tag{2.5}$$

where A_1 is a positive real constant. We take

$$N(r) = \left[\alpha^{-1}\left(\eta_1^*\beta\left\{[\ln\{R/(N+1)r\}]^{-1}\right\}\right)\right],$$

where $[x]$ denotes the integer part of $x \geqslant 0$. Since $\alpha \in \Lambda$ and $\beta \in L^0$, the integer $N(r)$ is well defined. Now if r is sufficiently large, then from (2.4) we have

$$M(r,H) \leqslant A_1 r^{n_0} + r^{N(r)} \sum_{n_0+1 \leqslant n \leqslant N(r)} R^{-n} \exp\left[n/\beta^{-1}\left\{(\eta_1^*)^{-1}\alpha(n)\right\}\right]$$
$$+ \sum_{n > N(r)} r^n R^{-n} \exp\left[n/\beta^{-1}\left\{(\eta_1^*)^{-1}\alpha(n)\right\}\right]$$

or

$$M(r,H) \leqslant A_1 r^{n_0} + r^{N(r)} \sum_{n=1}^{\infty} R^{-n} \exp\left[n/\beta^{-1}\left\{(\eta_1^*)^{-1}\alpha(n)\right\}\right] + \sum_{n>N(r)} r^n R^{-n} \exp\left[n/\beta^{-1}\left\{(\eta_1^*)^{-1}\alpha(n)\right\}\right]. \tag{2.6}$$

Now we have

$$\lim_{n\to\infty} \sup\left(R^{-n}\exp\left[n/\beta^{-1}\left\{(\eta_1^*)^{-1}\alpha(n)\right\}\right]\right)^{1/n} = \frac{1}{R} < 1.$$

Hence the first series on right hand side of (2.6) converges to a positive real constant A_2. So from (2.6) we get

$$M(r,H) \leqslant A_1 r^{n_0} + A_2 r^{N(r)} + \sum_{n>N(r)} r^n R^{-n} \exp\left[n/\beta^{-1}\left\{(\eta_1^*)^{-1}\alpha(n)\right\}\right]$$

or

$$M(r,H) \leqslant A_1 r^{n_0} + A_2 r^{N(r)} + \sum_{n>N(r)} r^n R^{-n} \exp[n\ln\{R/(N+1)r\}]$$

or

$$M(r,H) \leqslant A_1 r^{n_0} + A_2 r^{N(r)} + \sum_{n>N(r)} \left(\frac{1}{N+1}\right)^n$$

or

$$M(r,H) \leqslant A_1 r^{n_0} + A_2 r^{N(r)} + \sum_{n=1}^{\infty} \left(\frac{1}{N+1}\right)^n. \tag{2.7}$$

It can be easily seen that the series in (2.7) converges to a positive real constant A_3. Therefore from (2.7), we get

$$M(r,H) \leqslant A_2 r^{N(r)}[1+o(1)]$$

or

$$\ln^+ M(r,H) \leqslant [1+o(1)]\left[\alpha^{-1}\left(\overline{\eta_1}\beta\left\{[\ln\{R/(N+1)r\}]^{-1}\right\}\right)\right]\ln r$$

or

$$\ln^+ M(r,H) \leqslant [1+o(1)]\alpha^{-1}\left[\{\eta_1^*+\delta_1\}\beta\left\{[\ln\{R/(N+1)r\}]^{-1}\right\}\right],$$

where $\delta_1 > 0$ is suitably small. Hence

$$\alpha[\ln^+ M(r,H)] \leqslant \{\eta_1^*+\delta_1\}\beta\left\{[1+o(1)]^{-1}[\ln(R/r)]^{-1}\right\}.$$

Thus for r sufficiently close to R, we get

$$\frac{\alpha[\ln^+ M(r,H)]}{\beta\{[1+o(1)]^{-1}[R/(R-r)]\}} \leqslant \eta_1^* + \delta_1.$$

Proceeding to limits as $r \to R$ and using the property of β, we get

$$\lim_{r \to R^-} \sup \frac{\alpha[\ln^+ M(r,H)]}{\beta\{R/(R-r)\}} \leqslant \eta_1^* + \delta_1.$$

Since ε and δ_1 are arbitrarily small, therefore finally we get $\rho \leqslant \eta_1$. Combining this with the earlier inequality obtained, we get $\rho = \eta_1$.

Now from (2.2), for every $\lambda_1 > \eta_1$ and for sufficiently large n, we have

$$\frac{\alpha(n)}{\beta\left\{n/\ln^+(E_n(H)R^n)\right\}} \leqslant \lambda_1$$

or

$$E_n(H)R^n \leqslant \exp\left[n/\beta^{-1}\left\{\lambda_1^{-1}\alpha(n)\right\}\right].$$

Hence proceeding to limits as $n \to \infty$, we get

$$\lim_{n\to\infty} \sup (E_n(H)R^n)^{1/n} \leqslant 1.$$

Since $\eta_1 > 0$, the sequence $(E_n(H)R^n)_{n\in\mathbb{N}}$ is unbounded, whence

$$\lim_{n\to\infty} \sup (E_n(H)R^n)^{1/n} \geqslant 1.$$

Hence finally we get

$$\lim_{n\to\infty} \sup (E_n(H)R^n)^{1/n} = 1.$$

Thus following McCoy ([4], Theorem 1) we claim that the regular solution H can be continuously extended to a regular solution whose disk of regularity is $D_R(R > 1)$.

Let us put

$$H_1(r, e^{i\theta}) = \sum_{n=0}^{\infty} E_n(H)\Phi_n(r, e^{i\theta}).$$

Now we show that H_1 is the required continuation of H and $\rho(\alpha, \beta, H_1) = \eta_1$. For every $\lambda_1 > \eta_1$ and for sufficiently large n, we have

$$E_n(H)R^n \leqslant \exp\left[n/\beta^{-1}\left\{\lambda_1^{-1}\alpha(n)\right\}\right].$$

Now as in the proof of this theorem (see (2.4) to (2.7) above), we claim that

$$\rho(\alpha, \beta, H_1) \leqslant \lambda_1.$$

Since $\lambda_1 > \eta_1$ is arbitrary, so we get

$$\rho(\alpha, \beta, H_1) \leqslant \eta_1.$$

Also following the proof of first part given above, we get

$$\eta_1 \leqslant \rho(\alpha, \beta, H_1).$$

Hence finally we get $\rho(\alpha, \beta, H_1) = \eta_1$. This completes the proof of Theorem 1. ■

Next we prove

Theorem 2. *Let H be a regular solution of (1.1) and have the series expansion $H(r,e^{i\theta})=\sum_{n=0}^{\infty}a_n\Phi_n(r,e^{i\theta})$. For positive x,μ_2 and ρ, we set*

$$V(x,\mu_2,\rho)=\gamma^{-1}\{[\beta^{-1}(\mu_2\alpha(x))]^{1/\rho}\}.$$

Assume that for $\alpha(x),\beta(x),\gamma(x)\in\Lambda$,

$$V\left(\frac{n(\rho+1)}{\rho V(n/\rho,1/\mu_2,\rho+1)},\frac{1}{\mu_2},\rho\right)\cong[1+o(n)]V(n/\rho,1/\mu_2,\rho+1)\qquad\text{as } x\to\infty.$$

Then H is the restriction of a solution H_1 whose disk of regularity is $D_R(R>1)$ and having generalized type $\sigma(0<\sigma<\infty)$ if and only if

$$\sigma=\sigma(\alpha,\beta,\gamma,H_1)=\limsup_{n\to\infty}\frac{\alpha(n/\rho)}{\beta\left\{\left[\gamma\left\{(\rho+1)\left[\rho\ln^{+}(E_n(H)R^n)^{1/n}\right]^{-1}\right\}\right]^{(\rho+1)}\right\}}.$$

Proof. Write

$$\eta_2=\limsup_{n\to\infty}\frac{\alpha(n/\rho)}{\beta\left\{\left[\gamma\left\{(\rho+1)\left[\rho\ln^{+}(E_n(H)R^n)^{1/n}\right]^{-1}\right\}\right]^{(\rho+1)}\right\}}.\tag{2.8}$$

Now first we prove that $\eta_2\leqslant\sigma$. From (1.3), for $\mu_2>\sigma$ and r sufficiently close to R, we have

$$\ln^{+}M(r,H_1)\leqslant\alpha^{-1}[\mu_2\beta\{[\gamma\{R/(R-r)\}]^{\rho}\}].$$

Thus as in the proof of Theorem 1, here we have

$$\ln^{+}(E_n(H)R^n)\leqslant O(1)-n\ln(r/R)+\alpha^{-1}[\mu_2\beta\{[\gamma\{R/(R-r)\}]^{\rho}\}].$$

Putting

$$r=r_n=R\left[1-\left\{V\left(\frac{n(\rho+1)}{\rho V(n/\rho,1/\mu_2,\rho+1)},\frac{1}{\mu_2},\rho\right)\right\}^{-1}\right],$$

we get

$$\ln^{+}(E_n(H)R^n)\leqslant O(1)-n\ln\left[1-\left\{V\left(\frac{n(\rho+1)}{\rho V(n/\rho,1/\mu_2,\rho+1)},\frac{1}{\mu_2},\rho\right)\right\}^{-1}\right]$$
$$+n\frac{\rho+1}{\rho}\left[\gamma^{-1}\left\{\left[\beta^{-1}\left\{\mu_2^{-1}\alpha(n/\rho)\right\}\right]^{1/(\rho+1)}\right\}\right]^{-1}.$$

Now using the properties of logarithm and assumptions of theorem, we get for sufficiently large values of n

$$\ln^+ (E_n(H)R^n) \leqslant C_2 n \frac{\rho+1}{\rho} \left[\gamma^{-1}\left\{\left[\beta^{-1}\left\{\mu_2^{-1}\alpha(n/\rho)\right\}\right]^{1/(\rho+1)}\right\}\right]^{-1},$$

where C_2 is a positive constant. Hence by using the properties of α, β and γ, we get

$$\frac{\alpha(n/\rho)}{\beta\left\{\left[\gamma\left\{(\rho+1)\left[\rho \ln^+ (E_n(H)R^n)^{1/n}\right]^{-1}\right\}\right]^{(\rho+1)}\right\}} \leqslant \mu_2.$$

Now proceeding to limits as $n \to \infty$ we get $\eta_2 \leqslant \mu_2$. Since $\mu_2 > \sigma$ is arbitrary, therefore finally we get $\eta_2 \leqslant \sigma$. Now we will prove that $\sigma \leqslant \eta_2$. If $\eta_2 = \infty$, then there is nothing to prove. So let us assume that $0 \leqslant \eta_2 < \infty$. Therefore for a given $\varepsilon > 0$ there exists $n_0 \in N$ such that for all $n > n_0$, we have

$$0 \leqslant \frac{\alpha(n/\rho)}{\beta\left\{\left[\gamma\left\{(\rho+1)\left[\rho \log^+ (E_n(H)R^n)^{1/n}\right]^{-1}\right\}\right]^{(\rho+1)}\right\}} \leqslant \eta_2 + \varepsilon = \eta_2^*$$

or

$$E_n(H)R^n \leqslant \exp\left\{n^{\frac{\rho+1}{\rho}}\left[\gamma^{-1}\left\{\left[\beta^{-1}\left\{(\eta_2^*)^{-1}\alpha(n/\rho)\right\}\right]^{1/(\rho+1)}\right\}\right]^{-1}\right\} \tag{2.9}$$

or

$$E_n(H)r^n \leqslant r^n R^{-n} \exp\left\{n^{\frac{\rho+1}{\rho}}\left[\gamma^{-1}\left\{\left[\beta^{-1}\left\{(\eta_2^*)^{-1}\alpha(n/\rho)\right\}\right]^{1/(\rho+1)}\right\}\right]^{-1}\right\}.$$

Now from the property of maximum modulus, we have

$$\begin{aligned} M(r,H) &\leqslant \sum_{n=0}^{\infty} E_n(H)r^n \\ &\leqslant \sum_{n=0}^{n_0} E_n(H)r^n \\ &\quad + \sum_{n=n_0+1}^{\infty} r^n R^{-n} \exp\left\{n\frac{\rho+1}{\rho}\left[\gamma^{-1}\left\{\left[\beta^{-1}\left\{(\eta_2^*)^{-1}\alpha(n/\rho)\right\}\right]^{1/(\rho+1)}\right\}\right]^{-1}\right\} \end{aligned}$$

or

$$\begin{aligned} M(r,H) \leqslant B_1 r^{n_0} + \sum_{n=n_0+1}^{\infty} r^n R^{-n} \\ \times \exp\left\{n\frac{\rho+1}{\rho}\left[\gamma^{-1}\left\{\left[\beta^{-1}\left\{(\eta_2^*)^{-1}\alpha(n/\rho)\right\}\right]^{1/(\rho+1)}\right\}\right]^{-1}\right\}, \end{aligned} \tag{2.10}$$

where B_1 is a positive real constant. We take

$$N(r) = \left[\rho\alpha^{-1}\left\{\eta_2^*\beta\left([\gamma\{(\rho+1)[\rho\ln\{R/(N+1)r\}]^{-1}\}]^{(\rho+1)}\right)\right\}\right],$$

where $[x]$ denotes the integer part of $x \geqslant 0$. Since $\alpha(x), \beta(x), \gamma(x) \in \Lambda$, the integer $N(r)$ is well defined. Now if r is sufficiently close to R, then from (2.10) we have

$$\begin{aligned}
M(r,H) &\leqslant B_1 r^{n_0} \\
&+ r^{N(r)} \sum_{n_0+1\leqslant n\leqslant N(r)} R^{-n} \exp\left\{n\frac{\rho+1}{\rho}\left[\gamma^{-1}\left\{\left[\beta^{-1}\left\{(\eta_2^*)^{-1}\alpha(n/\rho)\right\}\right]^{1/(\rho+1)}\right\}\right]^{-1}\right\} \\
&+ \sum_{n>N(r)} r^n R^{-n} \exp\left\{n\frac{\rho+1}{\rho}\left[\gamma^{-1}\left\{\left[\beta^{-1}\left\{(\eta_2^*)^{-1}\alpha(n/\rho)\right\}\right]^{1/(\rho+1)}\right\}\right]^{-1}\right\}
\end{aligned}$$

or

$$\begin{aligned}
M(r,H) &\leqslant B_1 r^{n_0} \\
&+ r^{N(r)} \sum_{n=1}^{\infty} R^{-n} \exp\left\{n\frac{\rho+1}{\rho}\left[\gamma^{-1}\left\{\left[\beta^{-1}\left\{(\eta_2^*)^{-1}\alpha(n/\rho)\right\}\right]^{1/(\rho+1)}\right\}\right]^{-1}\right\} \\
&+ \sum_{n>N(r)} r^n R^{-n} \exp\left\{n\frac{\rho+1}{\rho}\left[\gamma^{-1}\left\{\left[\beta^{-1}\left\{(\eta_2^*)^{-1}\alpha(n/\rho)\right\}\right]^{1/(\rho+1)}\right\}\right]^{-1}\right\}.
\end{aligned} \tag{2.11}$$

Now we have

$$\begin{aligned}
\limsup_{n\to\infty}\left(R^{-n}\exp\left\{n\frac{\rho+1}{\rho}\left[\gamma^{-1}\left\{\left[\beta^{-1}\left\{(\eta_2^*)^{-1}\alpha(n/\rho)\right\}\right]^{1/(\rho+1)}\right\}\right]^{-1}\right\}\right)^{1/n} \\
= \frac{1}{R} < 1.
\end{aligned}$$

Hence the first series in (2.11) converges to a positive real constant B_2. Hence from (2.11), we get

$$\begin{aligned}
M(r,H) &\leqslant B_1 r^{n_0} + B_2 r^{N(r)} \\
&+ \sum_{n>N(r)} r^n R^{-n} \exp\left\{n\frac{\rho+1}{\rho}\left[\gamma^{-1}\left\{\left[\beta^{-1}\left\{(\eta_2^*)^{-1}\alpha(n/\rho)\right\}\right]^{1/(\rho+1)}\right\}\right]^{-1}\right\}
\end{aligned}$$

or

$$M(r,H) \leqslant B_1 r^{n_0} + B_2 r^{N(r)} + \sum_{n>N(r)} r^n R^{-n} \exp[n\ln\{R/(N+1)r\}]$$

or

$$M(r,H) \leqslant B_1 r^{n_0} + B_2 r^{N(r)} + \sum_{n>N(r)} \left(\frac{1}{N+1}\right)^n$$

or

$$M(r,H) \leqslant B_1 r^{n_0} + B_2 r^{N(r)} + \sum_{n=1}^{\infty} \left(\frac{1}{N+1}\right)^n. \tag{2.12}$$

It can be easily seen that the series in (2.12) converges to a positive real constant B_3. Therefore from (2.12), we get

$$M(r,H) \leqslant B_1 r^{n_0} + B_2 r^{N(r)} + B_3 \leqslant B_2 r^{N(r)}[1+o(1)]$$

or

$$\ln^+ M(r,H) \leqslant [1+o(1)] \times \left[\rho\alpha^{-1}\left\{\eta_2^*\beta\left([\gamma\{(\rho+1)[\rho\ln\{R/(N+1)r\}]^{-1}\}]^{(\rho+1)}\right)\right\}\right]\ln r,$$

or

$$\ln^+ M(r,H) \leqslant [1+o(1)] \times \left[\alpha^{-1}\left\{(\eta_2^*+\delta_2)\,\beta\left([\gamma\{(\rho+1)[\rho\ln\{R/(N+1)r\}]^{-1}\}]^{(\rho+1)}\right)\right\}\right],$$

where $\delta_2 > 0$ is suitably small. Hence

$$\alpha[\ln^+ M(r,H)] \leqslant (\eta_2^*+\delta_2)\,\beta\left([\gamma\{(\rho+1)[\rho\ln\{R/(N+1)r\}]^{-1}\}]^{(\rho+1)}\right).$$

When r is sufficiently close to R, then by using properties of β and γ, we get

$$\frac{\alpha[\ln^+ M(r,H)]}{\beta\{[\gamma\{R/(R-r)\}]^{\rho}\}} \leqslant \eta_2^* + \delta_2.$$

Since ε and δ_2 are arbitrarily small, proceeding to limits as $r \to R^-$, we get

$$\sigma \leqslant \eta_2. \tag{2.13}$$

Now as in Theorem 1 we can similarly prove that the regular solution H can be continuously extended to a regular solution whose disk of regularity is $D_R(R>1)$. Let us put

$$H_1(r,e^{i\theta}) = \sum_{n=0}^{\infty} E_n(H)\Phi_n(r,e^{i\theta}).$$

Now we claim that H_1 is the required continuation of H and $\sigma(\alpha,\beta,\gamma,H_1) = \eta_2$. From (2.8), for every $\lambda_2 > \eta_2$ and for sufficiently large n, we have

$$E_n(H)R^n \leqslant \exp\left\{n\frac{\rho+1}{\rho}\left[\gamma^{-1}\left\{\left[\beta^{-1}\left\{(\lambda_2)^{-1}\alpha(n/\rho)\right\}\right]^{1/(\rho+1)}\right\}\right]^{-1}\right\}.$$

Now as in the proof of this theorem (see (2.9) to (2.13)), we claim that

$$\sigma(\alpha,\beta,\gamma,H_1) \leqslant \lambda_2.$$

Since $\lambda_2 > \eta_2$ is arbitrary, so finally we get

$$\sigma(\alpha, \beta, \gamma, H_1) \leqslant \eta_2.$$

Also following the proof of first part given above, we get

$$\eta_2 \leqslant \sigma(\alpha, \beta, \gamma, H_1).$$

Hence finally we get $\sigma(\alpha, \beta, \gamma, H_1) = \eta_2$. This completes the proof of Theorem 2. ■

3. Functions of generalized slow growth

In this section we give the characterizations of generalized order and type for functions of slow growth. We have

Theorem 3. *Let H be a regular solution of (1.1) and have the series expansion $H(r, e^{i\theta}) = \sum_{n=0}^{\infty} a_n \Phi_n(r, e^{i\theta})$. Then for $\alpha(x) \in \Lambda$, H is a restriction of a solution H_1 whose disk of regularity is $D_R(R > 1)$ and having generalized order $\rho(\alpha, H_1)$ if and only if*

$$\rho(\alpha, H_1) = \limsup_{n \to \infty} \frac{\alpha(n)}{\alpha\left[\log^+\left\{n / \ln^+\left(E_n(H) R^n\right)\right\}\right]}.$$

Proof. First we assume that H has an extension H_1 whose disk of regularity is $D_R(R > 1)$ and is of generalized order $\rho(\alpha, H_1)$. We write $\rho(\alpha, H_1) = \rho$ and

$$\zeta_1 = \limsup_{n \to \infty} \frac{\alpha(n)}{\alpha\left[\log^+\left\{n / \ln^+\left(E_n(H) R^n\right)\right\}\right]}. \tag{3.1}$$

First we prove that $\zeta_1 \leqslant \rho$. As shown above, from (2.3) we have

$$E_k(H) \leqslant \frac{M(r, H)}{(r-1) r^{k-1}}, \qquad 1 < r < R,\ k \geqslant n \tag{3.2}$$

Also using (1.4), for arbitrarily small $\varepsilon > 0$ and $r > r_0(\varepsilon)$, we have

$$M(r, H) \leqslant \exp\left(\alpha^{-1}\left\{\rho^* \alpha\left[\ln\left\{R / (R-r)\right\}\right]\right\}\right), \tag{3.3}$$

where $\rho^* = \rho + \varepsilon$. From (3.2) and (3.3), we get

$$\ln^+\left(E_n(H) R^n\right) \leqslant -\ln^+(r-1) - n \ln^+(r/R) + \alpha^{-1}\left\{\rho^* \alpha\left[\ln\left\{R / (R-r)\right\}\right]\right\}.$$

Write $F(x, c_1) = \alpha^{-1}\left\{c_1 \alpha(x)\right\}$, where x and c_1 are positive real numbers. Now putting $r = r_n$, where

$$r_n = R\left(1 - \left[\exp\left\{F\left(n / \exp\left\{F\left(n, (\rho^*)^{-1}\right)\right\}, (\rho^*)^{-1}\right)\right\}\right]^{-1}\right),$$

we get

$$\ln^+ (E_n(H)R^n) \leqslant -\ln^+(r_n - 1) - n \ln^+ \left(1 - \left[\exp\left\{F\left(n/\exp\left\{F\left(n,(\rho^*)^{-1}\right)\right\},(\rho^*)^{-1}\right)\right\}\right]^{-1}\right) + n/\exp\left\{F\left(n,(\rho^*)^{-1}\right)\right\}.$$

Now using the properties of logarithm, we get for sufficiently large value of n

$$\ln^+ (E_n(H)R^n) \leqslant \{1 + o(1)\}\left[n/\exp\left\{F\left(n,(\rho^*)^{-1}\right)\right\}\right].$$

From the above inequality, we get

$$\alpha^{-1}\left\{(\rho^*)^{-1}\alpha(n)\right\} \leqslant \{1 + o(1)\}\ln^+\left\{n/\ln^+ (E_n(H)R^n)\right\}$$

or

$$\alpha(n) \leqslant \rho^* \alpha\left[\{1 + o(1)\}\ln^+\left\{n/\ln^+ (E_n(H)R^n)\right\}\right]$$

or

$$\frac{\alpha(n)}{\alpha\left[\ln^+\left\{n/\ln^+ (E_n(H)R^n)\right\}\right]} \leqslant \rho^* \frac{\alpha\left[\{1 + o(1)\}\ln^+\left\{n/\ln^+ (E_n(H)R^n)\right\}\right]}{\alpha\left[\ln^+\left\{n/\ln^+ (E_n(H)R^n)\right\}\right]}.$$

Proceeding to limits as $n \to \infty$ and using the properties of $\alpha(x)$, we get $\zeta_1 \leqslant \rho^*$. Since $\varepsilon > 0$ is arbitrarily small, we finally get $\zeta_1 \leqslant \rho$.

Now we will prove that $\rho \leqslant \zeta_1$. If $\zeta_1 = \infty$, then there is nothing to prove. So let us assume that $0 \leqslant \zeta_1 < \infty$. Therefore for a given $\varepsilon > 0$ there exists $n_0 \in N$ such that for all $n > n_0$, we have

$$0 \leqslant \frac{\alpha(n)}{\alpha\left[\log^+\left\{n/\log^+ (E_n(H)R^n)\right\}\right]} \leqslant \zeta_1 + \varepsilon = \zeta_1^*$$

or

$$E_n(H)R^n \leqslant \exp\left\{n/\exp\left[\alpha^{-1}\left\{(\zeta_1^*)^{-1}\alpha(n)\right\}\right]\right\} \tag{3.4}$$

or

$$E_n(H)r^n \leqslant r^n R^{-n} \exp\left\{n/\exp\left[\alpha^{-1}\left\{(\zeta_1^*)^{-1}\alpha(n)\right\}\right]\right\}.$$

Now from the property of maximum modulus, we have

$$M(r, H_1) \leqslant \sum_{n=0}^{\infty} E_n(H)r^n \leqslant \sum_{n=0}^{n_0} E_n(H)r^n + \sum_{n=n_0+1}^{\infty} r^n R^{-n} \exp\left\{n/\exp\left[\alpha^{-1}\left\{(\zeta_1^*)^{-1}\alpha(n)\right\}\right]\right\}$$

or

$$M(r,H_1)\leqslant A_1r^{n_0}+\sum_{n=n_0+1}^{\infty}r^nR^{-n}\exp\left\{n/\exp\left[\alpha^{-1}\left\{\left(\zeta_1^*\right)^{-1}\alpha(n)\right\}\right]\right\},\quad(3.5)$$

where A_1 is a positive real constant. We take

$$W_1(r)=\left[\alpha^{-1}\left\{\zeta_1^*\alpha\left[\ln\left\{\ln\left[R/\left(\delta_1+1\right)r\right]\right\}^{-1}\right]\right\}\right],$$

where $\delta_1>0$ is arbitrarily small and $[x]$ denotes the integer part of $x\geqslant 0$. Since $\alpha(x)\in\Lambda$, the integer $W_1(r)$ is well defined. Now if r is sufficiently large, then from (3.5), we have

$$\begin{aligned}M(r,H_1)&\leqslant A_1r^{n_0}+r^{W_1(r)}\\&\quad\times\sum_{n_0+1\leqslant n\leqslant W_1(r)}R^{-n}\exp\left\{n/\exp\left[\alpha^{-1}\left\{\left(\zeta_1^*\right)^{-1}\alpha(n)\right\}\right]\right\}\\&\quad+\sum_{n>W_1(r)}r^nR^{-n}\exp\left\{n/\exp\left[\alpha^{-1}\left\{\left(\zeta_1^*\right)^{-1}\alpha(n)\right\}\right]\right\}\end{aligned}$$

or

$$\begin{aligned}M(r,H_1)&\leqslant A_1r^{n_0}+r^{W_1(r)}\sum_{n=1}^{\infty}R^{-n}\exp\left\{n/\exp\left[\alpha^{-1}\left\{\left(\zeta_1^*\right)^{-1}\alpha(n)\right\}\right]\right\}\\&\quad+\sum_{n>W_1(r)}r^nR^{-n}\exp\left\{n/\exp\left[\alpha^{-1}\left\{\left(\zeta_1^*\right)^{-1}\alpha(n)\right\}\right]\right\}.\end{aligned}\quad(3.6)$$

Now we have

$$\limsup_{n\to\infty}\left(R^{-n}\exp\left\{n/\exp\left[\alpha^{-1}\left\{\left(\zeta_1^*\right)^{-1}\alpha(n)\right\}\right]\right\}\right)^{1/n}=\frac{1}{R}<1.$$

Hence the first series in (3.6) converges to a positive real constant A_2. So from (3.6), we get

$$\begin{aligned}M(r,H_1)&\leqslant A_1r^{n_0}+A_2r^{W_1(r)}\\&\quad+\sum_{n>W_1(r)}r^nR^{-n}\exp\left\{n/\exp\left[\alpha^{-1}\left\{\left(\zeta_1^*\right)^{-1}\alpha(n)\right\}\right]\right\}\\&\leqslant A_1r^{n_0}+A_2r^{W_1(r)}+\sum_{n>W_1(r)}r^nR^{-n}\exp[n\ln\{R/(\delta_1+1)r\}]\\&\leqslant A_1r^{n_0}+A_2r^{W_1(r)}+\sum_{n>W_1(r)}[1/(\delta_1+1)]^n\end{aligned}$$

or

$$M(r,H_1)\leqslant A_1r^{n_0}+A_2r^{W_1(r)}+\sum_{n=1}^{\infty}[1/(\delta_1+1)]^n.\quad(3.7)$$

It can be easily seen that the series in (3.7) converges to a positive real constant A_3. Therefore from (3.7), we get

$$M(r, H_1) \leqslant A_1 r^{n_0} + A_2 r^{W_1(r)} + A_3 \leqslant A_2 r^{W_1(r)}[1 + o(1)]$$

or

$$\begin{aligned}\ln^+ M(r, H_1) &\leqslant [1 + o(1)]W_1(r) \ln r \\ &\leqslant [1 + o(1)] \left[\alpha^{-1} \left\{\zeta_1^* \alpha \left[\ln \{\ln [R/ (\delta_1 + 1) r]\}^{-1}\right]\right\}\right] \ln r \\ &\leqslant O(1) \left[\alpha^{-1} \left\{\zeta_1^* \alpha \left[\ln \{\ln [R/ (\delta_1 + 1) r]\}^{-1}\right]\right\}\right].\end{aligned}$$

Since $\delta_1 > 0$ is arbitrarily small, for r sufficiently close to R, we get

$$\ln^+ M(r, H_1) \leqslant O(1) \left[\alpha^{-1} \{\zeta_1^* \alpha [\ln \{R/(R - r)\}]\}\right]$$

or

$$\alpha \left[\ln^+ M(r, H_1)\right] \leqslant \zeta_1^* \alpha [\ln \{R/(R - r)\}] + O(1)$$

Thus for r sufficiently close to R, we get

$$\frac{\alpha \left[\ln^+ M(r, H_1)\right]}{\alpha [\ln \{R/(R - r)\}]} \leqslant \zeta_1^* + o(1).$$

Proceeding to limits as $r \to R^-$, we get

$$\rho \leqslant \zeta_1^*.$$

Since $\varepsilon > 0$ is arbitrarily small, therefore finally we get

$$\rho \leqslant \zeta_1. \tag{3.8}$$

Now from (3.1), for every $\lambda_1 > \zeta_1$ and for sufficiently large value of n, we have

$$\frac{\alpha(n)}{\alpha \left[\log^+ \left\{n/ \log^+ (E_n(H) R^n)\right\}\right]} \leqslant \lambda_1$$

or

$$E_n(H) R^n \leqslant \exp \left\{n/ \exp \left[\alpha^{-1} \left\{(\lambda_1)^{-1} \alpha(n)\right\}\right]\right\}.$$

Now for sufficiently large value of n, we get

$$[E_n(H) R^n]^{1/n} \leqslant 1.$$

Proceeding to limits as $n \to \infty$, we get

$$\limsup_{n \to \infty} [E_n(H) R^n]^{1/n} \leqslant 1.$$

Since $\eta_1 > 0$, the sequence $(E_n(H)R^n)_{n\in\mathbb{N}}$ is unbounded, whence

$$\lim_{n\to\infty} \sup \left[E_n(H)R^n\right]^{1/n} \geqslant 1.$$

Hence finally we get

$$\lim_{n\to\infty} \sup \left[E_n(H)R^n\right]^{1/n} = 1.$$

Thus following McCoy ([4], Theorem 1) we claim that the regular solution H can be continuously extended to a regular solution whose disk of regularity is $D_R(R > 1)$. Let us put

$$H_1(r, e^{i\theta}) = \sum_{n=0}^{\infty} E_n(H)\Phi_n(r, e^{i\theta}).$$

Now we claim that H_1 is the required continuation of H and $\rho(\alpha, H_1) = \zeta_1$. For every $\lambda_1 > \zeta_1$ and for sufficiently large value of n, we have

$$E_n(H)R^n \leqslant \exp\left\{n/\exp\left[\alpha^{-1}\left\{(\lambda_1)^{-1}\,\alpha(n)\right\}\right]\right\}.$$

Now as in the proof of this theorem [(3.4) to (3.8)], we claim that

$$\rho(\alpha, H_1) \leqslant \lambda_1.$$

Since $\lambda_1 > \zeta_1$ is arbitrary, so we get

$$\rho(\alpha, H_1) \leqslant \zeta_1.$$

Also following the proof of first part given above, we get

$$\zeta_1 \leqslant \rho(\alpha, H_1).$$

So finally we get

$$\rho(\alpha, H_1) = \zeta_1.$$

This completes the proof of Theorem 3. ■

Next we have

Theorem 4. *Let H be a regular solution of (1.1) and have the series expansion $H(r, e^{i\theta}) = \sum_{n=0}^{\infty} a_n\Phi_n(r, e^{i\theta})$. Then for $1 < \rho < \infty$ and $\beta(x) \in L^0$, H is a restriction of a solution H_1 whose disk of regularity is $D_R(R > 1)$ and having generalized type $\sigma(\beta, \rho, H_1)$ if and only if*

$$\sigma(\beta, \rho, H_1) = \lim_{n\to\infty} \sup \frac{\beta(n)}{\left(\beta\left[\log^+\left\{n/\ln^+\left(E_n(H)R^n\right)\right\}\right]\right)^{\rho}}.$$

Proof. The proof of the above theorem follows on the lines of proof of Theorem 2 and Theorem 3. Hence we omit the proof. ■

Next we have

Theorem 5. *Let H be a regular solution of* (1.1) *and have the series expansion $H(r,e^{i\theta}) = \sum_{n=0}^{\infty} a_n \Phi_n(r,e^{i\theta})$. Then for $\alpha(x) \in \Lambda$ the generalized order $\rho(\alpha,H)$ $(0 \leqslant \rho(\alpha,H) < \infty)$ of H is given by*

$$\rho(\alpha,H) = \limsup_{n\to\infty} \frac{\alpha(n)}{\alpha\left[\ln^+\left\{n/\ln^+\left(|a_n|R^n\right)\right\}\right]}.$$

Proof. The proof is similar to Theorem 3 above and ([7], Theorem 2.1). Hence the proof is omitted. ■

Lastly we have

Theorem 6. *Let H be a regular solution of* (1.1) *and have the series expansion $H(r,e^{i\theta}) = \sum_{n=0}^{\infty} a_n \Phi_n(r,e^{i\theta})$. Then for $1 < \rho < \infty$ and $\beta(x) \in L^0$ the generalized type $\sigma(\beta,\rho,H)$ of H is given by*

$$\sigma(\beta,\rho,H) = \limsup_{n\to\infty} \frac{\beta(n)}{\left(\beta\left[\ln^+\left\{n/\ln^+\left(|a_n|R^n\right)\right\}\right]\right)^{\rho}}.$$

Proof. The proof is similar to Theorem 2 above and ([7], Theorem 2.2). Hence the proof is omitted. ■

Acknowledgement. The authors are very much indebted to the referee for his valuable comments which helped in improving the paper.

References

[1] S. Bergman, *Integral operators in the theory of linear partial differential equations*, Ergebnisse der Mathematik und ihrer Grenzgebiete, Band 23, Springer-Verlag, New York, 1969.

[2] A. Janik, *On approximation of analytic functions and generalized order*, Ann. Polon. Math. **55** (1991), 163–167.

[3] D. Kumar, *Growth and Chebyshev approximation of entire function solutions of Helmoltz equation in* $\mathbb{R}^2$, Eur. J. Pure Appl. Math. **3** (2010), no. 6, 1062–1069.

[4] P.A. McCoy, *Optimal approximation and growth of solutions to a class of elliptic partial differential equations*, J. Math. Anal. Appl. **154** (1991), 203–211.

[5] P.A. McCoy, *Solutions of the Helmoltz equation having rapid growth,* Complex Var. Elliptic Equ. **18** (1992), no. 1, 91–101.

[6] M.N. Seremeta, *On the connection between the growth of a function analytic in a disc and moduli of the coefficients of its Taylor series,* Visnik L'viv. Derzh. Univ. Ser. Mekh. Mat. **2** (1965), 101–110.

[7] G.S. Srivastava and S. Kumar, *Generalized growth of solutions to a class of elliptic partial differential equations*, Acta Math. Vietnam. **37** (2012), no. 1, 11–21.

Addresses: Susheel Kumar: Department of Mathematics, Jaypee University of Engineering and Technology, Guna - 473226 (M. P.), India;
Girja S. Srivastava: Department of Mathematics, Jaypee Institute of Information Technology, Noida-201309 (U. P.), India.

E-mail: sus83dma@gmail.com, gs91490@gmail.com

Received: 25 June 2015; **revised:** 16 November 2015

Functiones et Approximatio
54.1 (2016), 115–140
doi: 10.7169/facm/2016.54.1.9

ÉTUDE PROBABILISTE DES QUOTIENTS DE FERMAT

Georges Gras

Abstract: For fixed $a \geqslant 2$, we suggest that the probability of nullity mod p of the Fermat quotient $q_p(a)$ is $\ll \frac{1}{p}$ for $p \to \infty$. For this we propose various heuristics (as the existence of a suitable binomial law of probability), justified by means of numerical computations and analytical results, which may imply, via the Borel–Cantelli heuristic, that $q_p(a) \neq 0$ for all p except a finite number (Th. 4.9). These heuristics are based on the possible existence (with an analogous probability) of $O(\log(p))$ "abundant" solutions $z_i \in [2, p-1[$ which are not necessarily of the "exceptional" form a^k, $1 \leqslant k < \log(p)/\log(a)$, when $q_p(a) = 0$, showing the exceptional solutions as a particular case of abundant solutions, for which a law of probability is natural.

We also compute the density of integers A such that $q_p(A) \neq 0$, $\forall p \leqslant x$ (Th. 4.12).

Keywords: Fermat quotients, cyclotomic polynomials, prime numbers, probabilistic number theory, Borel–Cantelli heuristic.

1. Introduction

Nous étudions la probabilité de nullité modulo p du quotient de Fermat $q_p(a) := \frac{a^{p-1}-1}{p}$, de $a \geqslant 2$ fixé dans $\mathbb{N}$, p premier étant la variable (par abus, l'écriture $q_p(a) = u \in [0, p[$ signifie $q_p(a) \equiv u \pmod p$).

Nous démontrons le résultat probabiliste suivant (Théorème 4.9):

Si l'Heuristique 4.4 est vraie (existence d'une loi de probabilité binomiale sur le nombre d'entiers $z \in [2, p-1[$ tels que $q_p(z) = 0$) alors, pour $p \to \infty$, $\mathrm{Prob}\big(q_p(a) = 0\big) < C_\infty(a) \times p^{-\left(\frac{\log_2(p)}{\log(a)} - \frac{\log_2(a)+1}{\log(a)} + O\left(\frac{\log_2(p)}{\log(p)}\right)\right)}$, *où* $\log_2 = \log \circ \log$ *et où la constante* $C_\infty(a)$ *vérifie* $e^{-1} < C_\infty(a) < 1$. *En admettant le principe de Borel–Cantelli, le nombre de p tels que $q_p(a) = 0$ est fini.*

Nous convenons de désigner par a un entier fixé, par A un entier positif quelconque (utilisé pour définir des densités sur $\mathbb{N}$ ou $\mathbb{N} \setminus p\,\mathbb{N}$), et enfin par z (resp. Z) un entier de $[1, p[$ (resp. de $[1, p^2[$).

(i) Dans un premier temps, on remarque que $q_p(a) = 0$ si et seulement si p^2 divise la valeur en a du $o_p(a)$-ième polynôme cyclotomique $\Phi_{o_p(a)}$, où

2010 Mathematics Subject Classification: primary: 11K65, 11R18; secondary: 11N37

$o_p(a)\,|\,p-1$ est l'ordre de a modulo p. On utilise la densité des $A \in \mathbb{N}\setminus p\mathbb{N}$ relative à la condition locale $p^2\,|\,\Phi_m(A)$, $m \geqslant 1$ fixé: si ϕ est l'indicateur d'Euler, cette densité est égale à $\frac{\phi(m)}{p(p-1)}$ pour $p \equiv 1 \pmod m$ ou pour $m = p = 2$, à 0 sinon. La densité des $A \in \mathbb{N}\setminus p\mathbb{N}$ tels que $q_p(A) = 0$ est donc $\sum_{d\,|\,p-1} \frac{\phi(d)}{p(p-1)} = \frac{1}{p}$.

On justifie alors au § 3.5 l'heuristique suivante, reposant sur l'idée qu'une *probabilité* portant sur a fixé (resp. sur $z \in [1, p[$), est inférieure à la densité correspondante:

$$\mathrm{Prob}\big(q_p(a) = 0\big) \leqslant \mathrm{Prob}\big(q_p(z) = 0, z \in [1, p[\big) \leqslant \sum_{d\,|\,p-1} \frac{\phi(d)}{p-1}\,\frac{\phi(d)}{p\,(p-1)} < \frac{1}{p}$$

ce qui ne renseigne que partiellement sur la finitude ou non des $q_p(a) = 0$ (Heuristique 3.7, Remarque 3.8, et § 3.7).

(ii) Dans un second temps, nous montrons comment tenir compte du fait que $a \geqslant 2$ est fixé et que si $q_p(a) = 0$ alors $q_p(a^j) = 0$ pour les exposants $j \in \big[1, \frac{\log(p)}{\log(a)}\big[$, pour lesquels $a^j \in [2, p-1[$ (solutions dites *exceptionnelles*). Cette répartition de $O(\log(p))$ solutions $z_j = a^j$, par rapport aux $p-1$ solutions "canoniques" $Z \in [1, p^2[$, est un cas particulier de *répétitions* (entiers $z \in [2, p-1[$ ayant même quotient de Fermat $q_p(z) = u$, $u \in [0, p[$). Si l'on pose $m_p(u) := |\{z \in [2, p-1[,\ q_p(z) = u\}|$, une étude numérique approfondie montre que ce nombre de répétitions est au plus $O(\log(p))$ car $M_p := \sup_{u\in[0,p[}\big(m_p(u)\big)$ est statistiquement très stable en $O(\log(p))$ *pour tout nombre premier* p (point essentiel).

Plus généralement, on peut avoir $m_p(0) = O(\log(p))$, auquel cas on parle de *solutions abondantes* $z_i \in [2, p-1[$, sans qu'il existe nécessairement $a \ll p$ tel que $q_p(a) = 0$ (cf. exemples du § 4.3). Les solutions étant aléatoires (les quotients de Fermat sont uniformément répartis d'après Heath-Brown [H-B]), l'existence d'une loi de probabilité standard est tout à fait crédible et donne, par un calcul analytique simple, une probabilité de cas abondant tendant vers 0 plus vite que $\frac{1}{p}$; or si "par hasard" l'une des solution z_i est égale à $a \ll p$, par ce simple fait d'ordre de grandeur Archimédien, les solutions abondantes sont (presque toutes) exceptionnelles de la forme:

$$z_1 = a, \ldots, z_h = a^h, z_{h+1}, \ldots, z_{m_p(0)},$$

où $h := h_p(a) := \big\lfloor \frac{\log(p)}{\log(a)} \big\rfloor$ (partie entière), $h \leqslant m_p(0)$, ce qui ferait que les célèbres "Wieferich primes" $p = 1093, 3511$, ne seraient pas de nature particulière, mais encore plus rares que pour le cas abondant (voir les commentaires à la suite de l'Heuristique 4.2, § 4.2).

On étudie alors une heuristique stipulant l'existence d'une loi binomiale, pour le nombre $m_p(u)$ de $z \in [2, p-1[$ tels que $q_p(z) = u$, à savoir: [1]

$$\mathrm{Prob}\big(m_p(u) \geqslant n\big) = 1 - \sum_{j=0}^{n-1} \binom{p-1}{j} \frac{1}{p^j} \left(1 - \frac{1}{p}\right)^{p-1-j}, \qquad 0 \leqslant n \ll p,$$

pour tout $u \in [0, p[$ fixé. Appliquée à $u = 0$ et au cas $n = h = O(\log(p))$, on obtient, *via le principe de Borel–Cantelli et sous cette heuristique*, la finitude des p tels que $q_p(a) = 0$ (Théorème 4.9).

(iii) Enfin, en utilisant le fait que $q_p(A) = 0$ si et seulement si p^2 divise $\dfrac{\Phi_{o_p(A)}(A)}{\text{p.g.c.d.}\,(\Phi_{o_p(A)}(A), o_p(A))}$, on démontre que la densité des $A \in \mathbb{N}$ tels que $q_p(A) \neq 0,\ \forall p \leqslant x$, est $O\big(\frac{1}{\log(x)}\big)$ (Théorème 4.12).

2. Cyclotomie et quotients de Fermat

2.1. Rappels sur le quotient de Fermat

Soit $a \geqslant 1$. Soit p un nombre premier, $p \nmid a$. Soit $m = o_p(a)$ l'ordre de a modulo p et soit ξ une racine primitive m-ième de l'unité dans $\mathbb{C}$; alors on peut écrire $a^m - 1 = \prod_{j=1}^{m}(a - \xi^j) \equiv 0 \pmod p$. Comme m est l'ordre de a modulo p, c'est le facteur de $a^m - 1$ défini par $\Phi_m(a) = \prod_{t \in (\mathbb{Z}/m\mathbb{Z})^\times} (a - \xi^t)$ qui est dans $p\,\mathbb{Z}$, où Φ_m est le m-ième polynôme cyclotomique. De façon précise on a la relation $q_p(a) = \frac{a^{p-1}-1}{p} = \frac{\Phi_m(a)}{p} \times F,\ F \not\equiv 0 \pmod p$. On a donc l'implication $m = o_p(a) \Longrightarrow p \,|\, \Phi_m(a)$. La réciproque est inexacte; par exemple, si $p = 3$, $m = 6$, $a = 5$, on a $\Phi_m(a) = 7 \times p$ avec pour ordre de a modulo p, $o_p(a) = 2$ et $\Phi_2(a) = 2 \times p$ comme attendu, avec ici $m = p \cdot o_p(a)$.

Ce phénomène sera précisé par le Théorème 2.3, mais on a toujours $q_p(a) \equiv 0 \pmod p$ si et seulement si $\Phi_{o_p(a)}(a) \equiv 0 \pmod{p^2}$.

Pour diverses propriétés des quotients de Fermat on peut se reporter à [CDP], [EM], [Hat], [KR], [Sh], [OS], ainsi qu'à [Si], [GM], [W] pour les liens avec la conjecture ABC.

2.2. Utilisation des corps cyclotomiques

Nous utilisons des propriétés classiques que l'on peut trouver dans [Wa].

Lemme 2.1. *Soient $a \geqslant 1$, $p \nmid a$, et $m \geqslant 1$. Alors la congruence $\Phi_m(a) \equiv 0 \pmod{p^H}$, $H \geqslant 1$, est équivalente à l'existence d'un couple $(\xi, \mathfrak{P})$, défini à conju-*

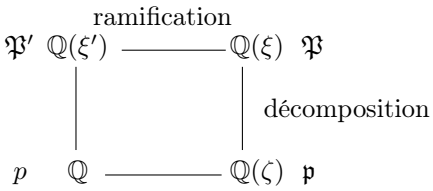
[1] Bien que $z = 1$ et $z = p - 1$ introduisent un biais ($q_p(1) = 0$, $q_p(p-1) = 1$), les paramètres $(p-1, 1/p)$ se justifient car on pourrait utiliser un intervalle décalé de $p-1$ résidus de la forme $[-t\,p + 1, (-t+1)\,p[$, $t \in [0, p[$, n'ayant pas ce biais; or ces intervalles ont les mêmes propriétés statistiques (cf. Remarque 4.3). De plus, la loi en $(p-1, 1/p)$ est légèrement majorante pour $\mathrm{Prob}\big(m_p(u) \geqslant n\big)$, ce qui est favorable.

gaison près, tel que $a \equiv \xi \pmod{\mathfrak{P}^H}$*, où* ξ *est une racine primitive* m*-ième de l'unité et* $\mathfrak{P}$ *un idéal premier de* $\mathbb{Q}(\xi)$ *au-dessus de* p*, de degré résiduel* 1*. Lorsque ceci a lieu,* m *est de la forme* $p^e \cdot o_p(a)$*,* $e \geqslant 0$*.*

Démonstration. La relation $a \equiv \xi \pmod{\mathfrak{P}^H}$, $H \geqslant 1$, prouve déjà que $\mathfrak{P}$ est de degré résiduel 1 car ξ est congrue à un rationnel modulo $\mathfrak{P}$. Un sens est donc évident puisque $\Phi_m(a) = \mathrm{N}_{\mathbb{Q}(\xi)/\mathbb{Q}}(a-\xi)$. Supposons $\Phi_m(a) \equiv 0 \pmod{p^H}$, $H \geqslant 1$. Comme $\Phi_m(a) = \prod_{t \in (\mathbb{Z}/m\mathbb{Z})^\times} (a - \xi^t) \equiv 0 \pmod{p^H}$, il existe $\mathfrak{P}_1 \,|\, p$ dans $\mathbb{Q}(\xi)$ tel que $a - \xi \equiv 0 \pmod{\mathfrak{P}_1}$. Supposons que l'on ait aussi $a - \xi \equiv 0 \pmod{\mathfrak{P}_2}$, $\mathfrak{P}_2 \,|\, p$, avec $\mathfrak{P}_2 \neq \mathfrak{P}_1$; il existe donc une conjuguaison non triviale $\xi \mapsto \xi^t \neq \xi$ telle que $\mathfrak{P}_2 = \mathfrak{P}_1^{t^{-1}} \neq \mathfrak{P}_1$ et on obtient $a - \xi^t \equiv 0 \pmod{\mathfrak{P}_1}$, d'où $\xi^t - \xi \equiv 0 \pmod{\mathfrak{P}_1}$. D'où deux cas:

(i) $p \nmid m$ & $\xi^t \neq \xi$; alors $\xi^t - \xi$ est une unité en p (absurde).
(ii) $p \,|\, m$ & $\xi^t \neq \xi$.

Donc si $p \nmid m$, un seul $\mathfrak{P} \,|\, p$ intervient et on a $a - \xi \equiv 0 \pmod{\mathfrak{P}^H}$.
Examinons le cas $p \,|\, m$ & $\xi^t \neq \xi$ en considérant le schéma suivant:



Si l'on pose $m = p^e m'$, $e \geqslant 1$, $p \nmid m'$, et $\xi = \zeta\,\xi'$ (ζ d'ordre p^e, ξ' d'ordre m'), il vient $\zeta^t \xi'^t - \zeta\,\xi' \equiv 0 \pmod{\mathfrak{P}_1}$. Or on a toujours $\zeta \equiv 1 \pmod{\mathfrak{P}_1}$ car dans $\mathbb{Q}(\zeta)$ il y a un unique idéal premier $\mathfrak{p} = (1-\zeta)$ totalement ramifié dans $\mathbb{Q}(\zeta)/\mathbb{Q}$, donc tel que $\mathfrak{P}_1 \,|\, \mathfrak{p}$ et $\mathfrak{P}_2 \,|\, \mathfrak{p}$ (si $p^e = 2$, $\mathbb{Q}(\zeta) = \mathbb{Q}$ et $\mathfrak{p} = (2)$).

D'où $\xi'^t - \xi' \equiv 0 \pmod{\mathfrak{P}'_1 = \mathfrak{P}_1 \cap \mathbb{Z}[\xi']}$ dans $\mathbb{Q}(\xi')$, et par conséquent $\xi'^t = \xi'$ (i.e., $t \equiv 1 \pmod{m'}$) puisque $p \nmid m'$. Mais ceci implique $\mathfrak{P}_2 = \mathfrak{P}_1$ car $\mathbb{Q}(\xi)/\mathbb{Q}(\xi')$ est totalement ramifiée en p et t fixe $\mathbb{Q}(\xi')$ (absurde).

On a obtenu dans tous les cas $a - \xi \equiv 0 \pmod{\mathfrak{P}^H}$ pour un unique $\mathfrak{P} \,|\, p$.

Montrons enfin que $m' = o_p(a)$ dans tous les cas. On a à, ce stade, $m = p^e \,.\, m'$, $e \geqslant 0$, et $a \equiv \xi' \pmod{\mathfrak{P}' = \mathfrak{P} \cap \mathbb{Z}[\xi']}$ puisque $\zeta \equiv 1 \pmod{\mathfrak{P}}$, ce qui implique $a^d \equiv 1 \pmod{p}$ (i.e., $\xi'^d \equiv 1 \pmod{\mathfrak{P}'}$) si et seulement si $\xi'^d = 1$, d'où $d \equiv 0 \pmod{m'}$; d'où le lemme. ∎

Revenons à l'aspect réciproque de l'implication $m = o_p(a) \Longrightarrow p \,|\, \Phi_m(a)$ en tenant compte des questions de divisibilités par p^H. D'après le lemme précédent, si $p \,|\, \Phi_m(a)$, on a $m = p^e \,.\, o_p(a)$, $e \geqslant 0$, et par conséquent $p \,|\, \Phi_{o_p(a)}(a)$. Le cas $p \nmid m$ est donc résolu et conduit à l'équivalence partielle $p \,|\, \Phi_m(a)$ & $p \nmid m \iff m = o_p(a)$. Dans ce cas toute puissance p^H, $H \geqslant 1$, peut diviser $\Phi_m(a) = \Phi_{o_p(a)}(a)$ (c'est le problème du quotient de Fermat pour $H \geqslant 2$). Examinons maintenant le cas où $p \,|\, m$.

Lemme 2.2. *Supposons que pour $H \geqslant 1$, $p^H \,||\, \Phi_m(a)$ avec $m = p^e m'$, $e \geqslant 1$, $p \nmid m'$ (i.e., $m = p^e \,.\, o_p(a)$). Alors nécessairement $H = 1$ (i.e., $\Phi_m(a) \not\equiv 0 \pmod{p^2}$) sauf si $p^e = m = 2$, auquel cas si $a = -1 + 2^H \psi$, $H \geqslant 1$ quelconque, on a $\Phi_2(a) = 2^H \ \psi$, $\Phi_1(a) = -2 + 2^H \psi$.*

Démonstration. On a donc par hypothèse, d'après le Lemme 2.1, $a \equiv \xi \pmod{\mathfrak{P}^H}$, pour $\xi = \zeta\xi'$ d'ordre $p^e \,.\, o_p(a)$ (ζ d'ordre p^e, ξ' d'ordre $o_p(a)$), et $a \equiv \xi' \pmod{\mathfrak{P}'^{H'}}$, $\mathfrak{P}' = \mathfrak{P} \cap \mathbb{Z}[\xi']$, avec $H' \geqslant 1$ puisque $\zeta \equiv 1 \pmod{\mathfrak{P}}$; on a l'identité $a - \xi = a - \xi' + \xi'\,(1 - \zeta)$, où les $\mathfrak{P}$-valuations des termes sont respectivement H, $H'p^{e-1}(p-1), 1$.

Si $H'p^{e-1}(p-1) > 1$, nécessairement $H = 1$. Le cas $H'p^{e-1}(p-1) = 1$ correspond au cas $p = 2$, $H' = e = 1$, donc $o_2(a) = 1$, $\xi' = 1$, $\xi = -1$, $\Phi_2(a) = a+1$ et p.g.c.d. $(2, \Phi_2(a)) = 2$ (e.g. $p = 2$, $a = 23$, $m = 2$, $\Phi_2(a) = 8 \times 3$, $\Phi_1(a) = 2 \times 11$, $H' = 1$, $H = 3$). En dehors du cas $m = p = 2$, on a $H = 1$. ■

Théorème 2.3. *Pour tout $m \geqslant 1$, le p.g.c.d. de $\Phi_m(a)$ et de m est égal à 1 ou à un nombre premier p. Dans ce dernier cas, $m = p^e \cdot o_p(a)$, $e \geqslant 1$. Réciproquement, pour tout premier p et tout $e \geqslant 1$, $m = p^e \cdot o_p(a)$ conduit à* p.g.c.d. $(\Phi_m(a), m) = p$. *On a donc l'équivalence (pour tout p et tout m) $p \,|\, \Phi_m(a) \iff m = p^e \cdot o_p(a)$, $e \geqslant 0$.*

Démonstration. Si p et q, $p \neq q$, sont des nombres premiers divisant m et $\Phi_m(a)$, on a nécessairement $m = p^e q^f m''$, $e, f \geqslant 1$, avec $o_p(a) = q^f m'' \,|\, p - 1$ et $o_q(a) = p^e m'' \,|\, q - 1$, qui suppose $q < p$ et $p < q$ (absurde).

Enfin montrons que tout p premier et tout $e \geqslant 1$ conviennent pour $m = p^e \cdot o_p(a)$. Comme $p \,|\, \Phi_{o_p(a)}(a)$, on a $a \equiv \xi' \pmod{\mathfrak{P}'}$ dans $\mathbb{Q}(\xi')$ (ξ' d'ordre $o_p(a)$); donc pour toute racine ζ d'ordre p^e, et pour $\mathfrak{P} \,|\, \mathfrak{P}'$ dans $\mathbb{Q}(\zeta\xi')$, on a $a \equiv \zeta\xi' \pmod{\mathfrak{P}}$ (d'où le résultat par le Lemme 2.1). Il est clair que p.g.c.d. $(m, \Phi_m(a)) = p$. ■

Nous réserverons la notation r au cas où $m = r^e \cdot o_r(a)$, $e \geqslant 1$, car r n'intervient pas pour le calcul des $q_p(a)$ pour les $p \,|\, \Phi_m(a)$. En effet, dans le cas où p.g.c.d. $(\Phi_m(a), m) = r$, la nullité du r-quotient de Fermat de a est donnée via $\dfrac{\Phi_{o_r(a)}(a)}{r}$ en général distinct (mod r) des $\dfrac{\Phi_{r^e \cdot o_r(a)}(a)}{r}$ pour $e \geqslant 1$ puisque dans ce cas, et pour $m = r^e \cdot o_r(a) \neq 2$, $\Phi_{r^e \cdot o_r(a)}(a) \not\equiv 0 \pmod{r^2}$ (Lemme 2.2). Par exemple, pour $r = 29$ et $a = 14$ on a $o_{29}(a) = 28$, $\dfrac{\Phi_{29 \cdot 28}(a)}{29} = F \not\equiv 0 \pmod{29}$ mais $\dfrac{\Phi_{28}(a)}{29} = 29 \times F'$ (i.e., $q_{29}(14) = 0$).

2.3. Définition et propriétés des nombres $\widetilde{\Phi}_m(a)$

On peut donc considérer dans tous les cas $\widetilde{\Phi}_m(a) := \dfrac{\Phi_m(a)}{\text{p.g.c.d.}\,(\Phi_m(a), m)}$, qui est égal à $\Phi_m(a)$ ou à $\dfrac{\Phi_{r^e \cdot o_r(a)}(a)}{r}$, $e \geqslant 1$, pour éliminer le facteur premier r éventuel (ramifié dans $\mathbb{Q}(\xi)/\mathbb{Q}$). Dans le second cas $m = r^e \cdot o_r(a)$, $e \geqslant 1$, si $p \neq r$ divise $\Phi_m(a)$, alors $m = o_p(a)$ et on a $p \equiv 1 \pmod{r^e \cdot o_r(a)}$.

Soit $m \neq 2$; d'après les résultats précédents, tout premier ℓ divisant $\widetilde{\Phi}_m(a)$ est congru à 1 modulo m (car de degré 1 et non ramifiés dans $\mathbb{Q}(\mu_m)/\mathbb{Q}$). Il en résulte aussi que ℓ (en posant $\ell - 1 = t\,m$) est totalement décomposé dans l'extension Galoisienne $\mathbb{Q}(\mu_{\ell-1})(\sqrt[t]{a})/\mathbb{Q}$ puisque a est localement de la forme b^t modulo ℓ. Ces questions d'ordres modulo ℓ sont liées à des techniques issues de la conjecture d'Artin sur les racines primitives et de la démonstration de Hooley; elles sont susceptibles de s'appliquer aux quotients de Fermat (nous renvoyons à [Mo] pour un exposé exhaustif).

Lemme 2.4. *Supposons $(m,p) \neq (2,2)$. On a $p^2 \mid \widetilde{\Phi}_m(a)$ si et seulement si $m = o_p(a)$ & $p^2 \mid \Phi_m(a)$, donc si et seulement si $m = o_p(a)$ & $q_p(a) = 0$.*

Démonstration. En effet, si $p^2 \mid \Phi_{o_p(a)}(a)$, comme $p \mid \Phi_{o_p(a)}(a)$ et $p \nmid o_p(a)$, on a $\widetilde{\Phi}_{o_p(a)}(a) = \Phi_{o_p(a)}(a)$ et donc $p^2 \mid \widetilde{\Phi}_m(a) = \widetilde{\Phi}_{o_p(a)}(a)$.

Réciproquement, si $p^2 \mid \widetilde{\Phi}_m(a)$, on peut supposer p.g.c.d. $(\Phi_m(a), m) = r$ avec $m = r^e\, o_r(a)$, $e \geqslant 1$, sinon p.g.c.d. $(\Phi_m(a), m) = 1$, $\widetilde{\Phi}_m(a) = \Phi_m(a)$ et nécessairement $m = o_p(a)$. Ainsi $\widetilde{\Phi}_m(a) = \dfrac{\Phi_m(a)}{r}$, donc $p \nmid m$ (i.e., $p \neq r$ car $r^2 \nmid \Phi_m(a)$ par le Lemme 2.2 qui exclue le cas $p^e = m = 2$), d'où $p^2 \mid \Phi_m(a) = \Phi_{o_p(a)}(a)$. ■

Lemme 2.5. *Pour a fixé, les $\widetilde{\Phi}_m(a)$, $m \geqslant 1$, sont premiers entre eux deux à deux sauf pour $\widetilde{\Phi}_1(a)$ et $\widetilde{\Phi}_2(a)$ dont le p.g.c.d. est 2 pour $a \equiv 3 \pmod 4$. Pour tout $p > 2$ il existe un et un seul $m \geqslant 1$ (égal à $o_p(a)$), tel que $p \mid \widetilde{\Phi}_m(a)$.*

Démonstration. Si $p \neq 2$ divise $\widetilde{\Phi}_m(a)$ et $\widetilde{\Phi}_{m'}(a)$, d'après le Théorème 2.3 on a $m = p^e o_p(a)$ et $m' = p^{e'} o_p(a)$, $e, e' \geqslant 0$. Si par exemple $e \geqslant 1$, on a $p = r$ (absurde car r^2 ne divise pas $\Phi_m(a)$); donc $e = e' = 0$ et $m = m'$.

Si $p = 2$, on obtient encore $m = 2^e$, $m' = 2^{e'}$, $e, e' \geqslant 0$; le cas e ou $e' \geqslant 2$ étant impossible car alors $\widetilde{\Phi}_m(a)$ ou $\widetilde{\Phi}_{m'}(a)$ est impair, il reste par exemple le cas $e = 1$, $e' = 0$, mais alors $\widetilde{\Phi}_2(a) = \frac{a+1}{2}$ et $\widetilde{\Phi}_1(a) = a - 1$ sont divisibles par 2 pour $a \equiv 3 \pmod 4$. Enfin tout p divise $\Phi_{o_p(a)}(a) = \widetilde{\Phi}_{o_p(a)}(a)$. ■

En résumé on a obtenu l'équivalence suivante, plus forte que "$q_p(a) = 0$ *si et seulement si* $p^2 \mid \Phi_{o_p(a)}(a)$":

Théorème 2.6. *Soit $a \geqslant 1$ et soit p premier, $p \geqslant 2$. Alors $q_p(a) = 0$ si et seulement si p^2 divise $\widetilde{\Phi}_{o_p(a)}(a)$.*

Ce résultat ainsi que le Lemme 2.5 seront utilisés, entre autres, au § 4.6.

3. Première heuristique pour Prob $(q_p(a) = 0)$

3.1. Remarques préliminaires sur les probabilités

Soit $a \geqslant 2$ fixé et soit u donné dans $\mathbb{N}$. Pour $p \to \infty$, l'événement $q_p(a) \equiv u \pmod p$ est a priori de probabilité $\frac{1}{p}$ puisque $q_p(a)$ et u sont vus modulo p. Des probabilités inférieures à $\frac{1}{p}$ en moyenne ne sont pas contradictoires car une étude

numérique montre qu'environ un tiers des $u \in [0, p[$ ne sont pas de la forme $q_p(z)$, $z \in [1, p[$. Pour les grands nombres premiers, la proportion moyenne se stabilise autour de $e^{-1} \approx 0.3678...$ (déjà observé dans [EM], § 4), ce qui constituera un bon argument pour l'existence d'une loi de probabilité binomiale car c'est précisément la probabilité (calculée via cette loi) d'avoir 0 solutions $z \in [2, p-1[$ à $q_p(z) = 0$ (Remarque 4.6 (ii)).

Le cadre probabiliste des solutions $z \in [2, p-1[$ à $q_p(z) = 0$ (p fixé) est très différent du cas a fixé (p variable) et est plutôt de type densité; or on verra au § 3.4 que ces deux cas de figure sont à distinguer soigneusement, tout se régularisant sur l'intervalle $[1, p^2[$ où "probabilité = densité" (surjectivité de l'application $Z \in [1, p^2[\mapsto q_p(Z) \in [0, p[$ par l'existence de $p-1$ solutions $Z \in [1, p^2[$ à $q_p(Z) = u$, cf. Lemme 3.4).

3.2. Résultats généraux de densités locales et globales

Citons, à titre d'information, le résultat suivant de Granville [G] (sous la conjecture ABC), dans la mesure où il peut éclairer notre démarche.

Proposition 3.1. *Soit $f \in \mathbb{Z}[X]$ un polynôme tel que l'ensemble des $f(n)$, $n \in \mathbb{Z}$, ait un plus grand commun diviseur égal à 1. La densité naturelle des entiers $A \in \mathbb{N}$ tels que $f(A)$ est sans facteur carré non trivial est $\prod_{p \text{ premier} \geqslant 2} \left(1 - \frac{c_p}{p^2}\right)$, où $c_p = \left| \left\{ b \in [0, p^2[,\ \ f(b) \equiv 0 \pmod{p^2} \right\} \right|$, chaque facteur $1 - \frac{c_p}{p^2}$ étant la densité (dite densité locale associée à p) des $A \in \mathbb{N}$ tels que $p^2 \nmid f(A)$.*

D'une certaine manière on peut dire que les événements $p^2 \nmid f(A)$ sont indépendants par rapport à p, ce qui constitue une information "probabiliste" intéressante. Par la suite, nous utiliserons essentiellement l'aspect local que l'on retrouve élémentairement dans le cadre cyclotomique.

3.3. Calcul des coefficients c_p pour les polynômes Φ_m

Le p.g.c.d. des $\Phi_m(n)$, $n \in \mathbb{Z}$, est égal à 1 car $\Phi_m(0) = \pm 1$ puisque toute racine de l'unité est de norme ± 1. Comme $\Phi_m(0) = \pm 1$, on a, pour tout p premier, $c_p = \left| \left\{ A \in [1, p^2[,\ \ \Phi_m(A) \equiv 0 \pmod{p^2} \right\} \right|$.

Proposition 3.2. *Considérons Φ_m pour $m \geqslant 1$. Si $p \geqslant 2$ ne divise pas m, on a $c_p = 0$ pour les $p \not\equiv 1 \pmod{m}$ et $c_p = \phi(m)$ sinon, où ϕ est l'indicateur d'Euler. Si $m = p^e m'$, $e \geqslant 1$, $p \nmid m'$, on a $c_p = 0$ sauf si $m = p = 2$, auquel cas $c_2 = 1$.*

Démonstration. (i) Cas $p \nmid m$. Dans ce cas, la congruence $\Phi_m(A) \equiv 0 \pmod{p}$ est équivalente à $m = o_p(A)$ et on a $p \equiv 1 \pmod{m}$; donc pour $p \nmid m$, il y a $\phi(m)$ nombres distincts $A_i \in [1, p[$ pour lesquels $\Phi_m(A_i) \equiv 0 \pmod{p}$. On vérifie, en dérivant $X^m - 1 = \Phi_m(X) \cdot Q(X)$, qu'il existe un unique $\psi_i \in [0, p[$ tel que $\Phi_m(A_i + \psi_i\, p) \equiv 0 \pmod{p^2}$, pour chaque i.

(ii) Cas $p \mid m$. D'après le Lemme 2.2, $m = p^e \cdot o_p(A)$, $e \geqslant 1$, et $\Phi_m(A) \equiv 0 \pmod{p^2}$ n'a pas de solutions sauf si $m = p = 2$ où $c_2 = 1$. ∎

3.4. Densités et probabilités – généralités

Si F_p est la propriété locale $p^2 \mid f(A)$ (p fixé), la densité des $A \in \mathbb{N} \setminus p\mathbb{N}$, donnée à partir des Propositions 3.1, 3.2, est égale à $\frac{c_p}{p\,(p-1)}$.

Il faut distinguer la notion de densité relative à la propriété:

$$\textit{pour } p \textit{ fixé, } p^2 \mid f(A),\ A \in \mathbb{N} \setminus p\mathbb{N} \textit{ variant arbitrairement,}$$

de celle de probabilités définissant l'un des événements suivants:

$$\textit{pour } z \in [2, p-1[,\ p^2 \mid f(z),\ p \textit{ variant arbitrairement,}$$
$$\textit{pour } a \textit{ fixé, } p^2 \mid f(a),\ p \textit{ variant arbitrairement.}$$

La densité locale ne dépend que de p et est de nature *algébrique*, tandis que ce que nous définissons comme probabilités est, pour un unique "tirage" $z \in [2, p-1[$, une fonction de p et, pour a fixé, une fonction de p de paramètre a; c'est le cas de $\mathrm{Prob}\big(q_p(a) = 0\big)$.

Le cas $q_p(a) = u$, u donné dans $\mathbb{N}$, est analogue; par exemple, on a $q_7(2) = 2$, mais les seuls $p < 10^{10}$, tels que $q_p(2) = 2$ sont $7, 71, 379, 2659$.

Chacun des p intervalles $[\lambda p + 1, (\lambda+1)p[$, $\lambda \in [0, p[$, contient a priori $\frac{p-1}{p}$ solutions en moyenne si l'on se réfère à la densité donnée par les $p-1$ solutions canoniques modulo p^2 (de fait $\frac{p-3}{p}$ solutions en raison de l'exclusion des "racines de l'unité" $\pm 1 \pmod{p^2}$ qui ne doivent pas intervenir en termes de probabilités: cas particulier de [Gr1], § 6.1.3, qui reviendrait à utiliser ici le système de représentants plus canonique $[-\frac{p-1}{2}, \frac{p-1}{2}] \setminus \{\pm 1\}$, $p \neq 2$).

On peut donc déjà envisager la première heuristique générale suivante:

Heuristique 3.3. *Supposons donnée une propriété locale $F_p(A)$, $p \to \infty$. Alors, la densité des $A \in \mathbb{N} \setminus p\mathbb{N}$ vérifiant $F_p(A)$ est un majorant de la "densité sur $[1, p[$" (notée par abus $\mathrm{Prob}\big(F_p(z)\big)$) des $z \in [1, p[$ tels que $F_p(z)$, celle-ci étant un majorant de $\mathrm{Prob}\big(F_p(a)\big)$ pour a fixé.*

Par exemple (cf. Théorème 2.6, Lemme 2.4 et Proposition 3.2), les densités locales $\frac{\phi(d)}{p\,(p-1)}$, caractérisant la propriété $p^2 \mid \widetilde{\Phi}_d(A)$ (i.e., $q_p(A) = 0$ pour les A d'ordre d modulo p), sont des *majorants* de $\mathrm{Prob}\big(q_p(z) = 0\big)$ (resp. $\mathrm{Prob}\big(q_p(a) = 0\big)$) pour $z \in [1, p[$ (resp. a fixé), z et a d'ordre d modulo p. Ceci sera utilisé pour justifier l'Heuristique 3.7.

Au plan numérique, pour $10^6 < p < 10^6 + 10^4$, il y a 754 nombres premiers et pour 284 d'entre eux, on a 0 solutions dans $[2, p-1[$. Enfin, si $m_p(0)$ est le nombre de solutions, les sommes $s = \sum_p \frac{m_p(0)}{p-1}$ et $s' = \sum_p \frac{1}{p-1}$ (sur cet intervalle) sont respectivement égales à 0.00012178... et 0.00012417....

3.5. Densités et probabilités des $q_p(\,\bullet\,) = u \in [0, p[$

Le résultat suivant généralise le cas précédent par un calcul direct de densité dans l'intervalle $[0, p^2[$:

Lemme 3.4. *Soit $z \in [1,p[$. Alors il existe un unique entier $\lambda_{p,u}(z) \in [0,p[$ tel que $Z := z + \lambda_{p,u}(z)\,p \in [1,p^2[$ vérifie $q_p(Z) = u$. On a $\lambda_{p,u}(z) \equiv z\,(q_p(z) - u) \pmod p$, d'où $Z \equiv z^p - zu\,p \pmod{p^2}$.*

La densité des $A \in \mathbb{N} \setminus p\mathbb{N}$, d'ordre $d \mid p-1$ modulo p, tels que $q_p(A) = u$ est égale à $\frac{\phi(d)}{p(p-1)}$.

Démonstration. Pour tout $\lambda \in \mathbb{N}$, $(z+\lambda\,p)^p - (z+\lambda\,p) \equiv z^p - z - \lambda\,p \pmod{p^2}$, d'où $\lambda \equiv z\,q_p(z) - Z\,q_p(Z) \equiv z\,q_p(z) - z\,q_p(Z) \pmod p$. Donc $q_p(Z) = u$ si et seulement si $\lambda = \lambda_{p,u}(z) \equiv z\,q_p(z) - z\,u \pmod p$. On a donc pour chaque $z \in [1,p[$ un unique $Z = z + \lambda_{p,u}(z)\,p \in [1,p^2[$ tel que $q_p(Z) = u$ (Z est aussi le résidu modulo p^2 de $z^p - zu\,p$), d'où la densité car $o_p(Z) = d$ équivaut à $o_p(z) = d$. ■

Remarques 3.5. Posons $\lambda_{p,0}(z) =: \lambda_p(z)$. On a alors les faits suivants:

(i) La relation $\lambda_p(z) \equiv z\,q_p(z) \pmod p$ pour tout $z \in [1,p[$ montre que pour a fixé, $q_p(a)$ et $\lambda_p(a)$ ont des comportements heuristiques analogues. En particulier, $z \in [1,p[\mapsto \lambda_p(z) \in [0,p[$ est non surjective.

(ii) Pour tout $z \in [1,p[$, on a les identités $q_p(p-z) \equiv q_p(z) + z^{-1} \pmod p$ et $\lambda_p(p-z) + \lambda_p(z) = p-1$, ce qui établit des relations de dépendance puisque, par exemple, $q_p(z)$ et $q_p(p-z)$ ne peuvent être nuls simultanément.

Revenons au cas $a \geqslant 2$ fixé. Pour $p \to \infty$ considérons l'intervalle $[1,p[$. D'après l'Heuristique 3.3, $\mathrm{Prob}\big(q_p(a) = 0\big)$ est majorée par la densité des $z \in [1,p[$ tels que $q_p(z) = 0$. Soit alors $d \mid p-1$; comme $o_p(z)$ ne dépend que de la classe de z modulo p, $\mathrm{Prob}\big(o_p(z) = d\big)$ est exactement la densité correspondante, égale à $\frac{\phi(d)}{p-1}$. Ensuite, $\mathrm{Prob}\big(p^2 \mid \widetilde{\Phi}_d(z)\big) \leqslant \frac{\phi(d)}{p\,(p-1)}$ (exemple illustrant l'Heuristique 3.3). Par conséquent, la probabilité de nullité de $q_p(a)$, pour a fixé et $p \to \infty$, est majorée par $\mathrm{Prob}\big(q_p(z) = 0, z \in [1,p[\big)$ qui est la somme pondérée:

$$\sum_{d \mid p-1} \mathrm{Prob}\big(o_p(z) = d\big) \times \mathrm{Prob}\big(p^2 \mid \widetilde{\Phi}_d(z),\, o_p(z) = d\big) \leqslant \sum_{d \mid p-1} \frac{\phi(d)}{p-1} \times \frac{\phi(d)}{p\,(p-1)}.$$

Remarques 3.6.

(i) Soient $z_1, \ldots, z_{\phi(d)}$ les $\phi(d)$ éléments d'ordre d de $[1,p[$. Pour chaque z_i, il existe (Lemme 3.4) $\lambda_i \in [0,p[$ tel que $q_p(z_i + \lambda_i p) = 0$ et λ_i est unique; autrement dit, pour i fixé, les p éléments $Z_\mu := z_i + \mu p$, $\mu \in [0,p[$, ne sont pas indépendants pour la probabilité $\mathrm{Prob}\big(q_p(Z_\mu) = 0\big)$ car la loi de probabilité pour la variable μ (i fixé) est telle que $\mathrm{Prob}\big(q_p(Z_\mu) = 0\big) = \frac{1}{p}$ et $\mathrm{Prob}\big(q_p(Z_{\mu_1}) = q_p(Z_{\mu_2}) = 0\big) = 0$ si $\mu_1 \neq \mu_2$. Mais sur $[1,p[$, une heuristique d'indépendance est possible au vu des résultats numériques (cf. § 4.3) et de l'uniforme distribution des $q_p(z)$.
Ceci explique que si l'on veut retrouver la densité des A tels que $q_p(A) = 0$ par ce raisonnement, à savoir écrire:

$$\sum_{d \mid p-1} \mathrm{Prob}\big(o_p(A) = d\big) \times \mathrm{Prob}\big(p^2 \mid \widetilde{\Phi}_d(A),\, o_p(A) = d\big),$$

le premier facteur est $\frac{p\,\phi(d)}{p\,(p-1)} = \frac{\phi(d)}{p-1}$, mais le second n'est pas la densité $\frac{\phi(d)}{p\,(p-1)}$ car la probabilité conditionnelle porte sur les $o_p(A) = d$ qui se répartissent en $\phi(d)$ classes à p éléments non indépendants comme expliqué ci-dessus.

(ii) La relation $a^{o_p(a)} = 1 + \lambda p > p$, implique $o_p(a) > h_p(a) =: h$, ce qui conduit à $\mathrm{Prob}\big(o_p(a) = d\big) = 0$ pour les petits diviseurs, ce qui favorise les plus grands (somme des probabillités égale à 1). On doit donc considérer une somme de la forme $\Sigma := \sum_{d>h} \Big(\frac{\phi(d)}{p-1} + \pi_d\Big) \frac{\phi(d)}{p(p-1)}$, où $\sum_{d>h} \pi_d = \sum_{d<h} \frac{\phi(d)}{p-1}$; on admet que l'on peut prendre pour π_d la valeur moyenne $\pi = \frac{1}{N_h} \sum_{d<h} \frac{\phi(d)}{p-1}$, où $N_h := |\{d \,|\, p-1,\ d > h\}|$. On vérifie que π est majoré par $\frac{1}{p^{1-\beta(p)}}$ où $\beta(p) > 0$ est de la forme $O\big(\frac{1}{\log_2(p)}\big)$ et $\sum_{d>h} \pi_d \frac{\phi(d)}{p(p-1)} < O(\frac{1}{p^{2-\beta(p)}})$.
On compare Σ et $\frac{1}{p}$ en posant $\Sigma = \alpha_p \frac{1}{p}$. Les extrema locaux de α_p sont obtenus pour les nombres de Sophie Germain $p = 1 + 2\ell$, ℓ premier, où $o_p(a) = 1$ ou 2 est impossible et où l'on peut supposer que $\mathrm{Prob}\big(o_p(a) = \ell\big) = \mathrm{Prob}\big(o_p(a) = 2\ell\big) = \frac{1}{2}$; on a $\pi = \frac{1}{p-1}$, auquel cas $\Sigma = \frac{\ell-1}{2\ell\,p} \sim \frac{1}{2p}$, $p = 1 + 2\ell \to \infty$. Donc $\mathrm{Sup}_p(\alpha_p) = \frac{1}{2}$. Lorsque $p-1$ est très composé, on a toujours $\alpha_p < \frac{1}{2}$, et $\mathrm{Inf}_p(\alpha_p)$ est proche de 0; par exemple, pour $p \in I := [10^6, 11 \times 10^8]$ et pour $a = 3$, on trouve $\mathrm{Inf}_{p\in I}(\alpha_p) = 0.050061...$ (atteint pour $p = 232792561 = 1 + 2^4 \,.\, 3^2 \,.\, 5 \,.\, 7 \,.\, 11 \,.\, 13 \,.\, 17 \,.\, 19$) et $\mathrm{Sup}_{p\in I}(\alpha_p) = 0.499999999090...$ (atteint pour $p = 1099998587 = 1 + 2 \,.\, \ell$, $\ell = 549999293$).

(iii) Si l'on calcule naïvement cette probabilité au moyen du polynôme $X^{p-1} - 1$ pour lequel la densité locale est $\frac{c_p}{p\,(p-1)} = \frac{p-1}{p\,(p-1)} = \frac{1}{p}$, l'expression analogue $\sum_{d\,|\,p-1} \mathrm{Prob}\big(o_p(z) = d\big) \times \mathrm{Prob}\big(p^2 \,|\, z^{p-1} - 1,\ o_p(z) = d\big)$ serait majorée par $\sum_{d\,|\,p-1} \frac{\phi(d)}{p-1} \times \frac{1}{p} = \frac{1}{p}$ indépendamment de toute "corection probabiliste", ce qui montre la pertinence de l'utilisation de $\Phi_d(X)$ au lieu de $X^{p-1} - 1$ qui remplace terme à terme $\frac{1}{p}$ par $\frac{\phi(d)}{p\,(p-1)} < \frac{1}{p}$.

On convient de négliger le phénomène des $d < h$ dans la mesure où seule l'information $\mathrm{Prob}\big(q_p(a) = 0\big) < \frac{1}{p}$ est l'objectif de cette section. On a donc la première heuristique probabiliste suivante pour $q_p(a) = 0$:

Heuristique 3.7. *Pour $a \geqslant 2$ fixé dans $\mathbb{N}$ et tout p assez grand, posons $\mathrm{Prob}\big(q_p(a) = 0\big) = \frac{1}{p^{1+\epsilon(p,a)}}$. Alors $\mathrm{Prob}\big(q_p(a) = 0\big) \leqslant \frac{1}{p\,(p-1)^2} \sum_{d\,|\,p-1} \phi(d)^2$, ou, de façon équivalente, $\epsilon(p,a) \geqslant \frac{1}{\log(p)} \big(2\log(p-1) - \log\big(\sum_{d\,|\,p-1} \phi(d)^2\big)\big)$.*

Remarque 3.8. Sous l'heuristique précédente, on obtient $\epsilon(p,a) > 0$ car

$$\frac{1}{p^{1+\epsilon(p,a)}} \leqslant \frac{\sum_{d\,|\,p-1} \phi(d)^2}{p\,(p-1)^2} < \frac{\big(\sum_{d\,|\,p-1} \phi(d)\big)^2}{p\,(p-1)^2} = \frac{1}{p}.$$

Autrement dit, si $\upsilon(p) = \frac{1}{\log(p)} \big(2\log(p-1) - \log\big(\sum_{d\,|\,p-1} \phi(d)^2\big)\big)$, on a $\epsilon(p,a) > \upsilon(p) > 0$, $p \to \infty$.

3.6. Une série de référence convergente

Afin de proposer de telles fonctions $\epsilon(p,a)$, rappelons une condition suffisante très classique de convergence des séries du type $\sum_p \frac{1}{p^{1+\epsilon(p,a)}}$, la série $\sum_p \frac{1}{p^{1+\upsilon(p)}}$ ne l'étant pas comme l'a montré G. Tenenbaum (cf. § 3.7).

Lemme 3.9. *Soit $C>1$ une constante et soit $\eta(p) := C\cdot\frac{\log_3(p)}{\log(p)}$, où $\log_k$ désigne le k-ième itéré de la fonction* log. *Alors on a $S := \sum\limits_{p\geqslant 2}\frac{1}{p^{1+\eta(p)}} < \infty$.*

Démonstration. Pour tout $n\geqslant 1$, désignons par p_n le n-ième nombre premier. On a $\sum_{p\geqslant 2}\frac{1}{p^{1+C\cdot\log_3(p)/\log(p)}} = \sum_{p\geqslant 2}\frac{1}{p\cdot\log_2^C(p)} = \sum_{n\geqslant 1}\frac{1}{p_n\cdot\log_2^C(p_n)}$.

On a $p_n > n\log(n)$ (théorème de Rosser); donc on peut majorer S par $\sum_{n\geqslant n_0}\frac{1}{n\log(n)\cdot\log_2^C(n\log(n))} < \sum_{n\geqslant n_0}\frac{1}{n\log(n)\cdot\log_2^C(n)}$, à une constante près, ce qui a même comportement que $\int_{x_0}^{\infty}\frac{dx}{x\log(x)\cdot\log_2^C(x)} = \int_{y_0}^{\infty}\frac{dy}{y\cdot\log^C(y)} < \infty$. ∎

On a $\epsilon(p,a) > \upsilon(p)$ (Remarque 3.8); donc $\epsilon(p,a) > \eta(p)$ reste largement possible. La différence entre $\upsilon(p)$ (situation divergente pour $\sum_p \frac{1}{p^{1+\upsilon(p)}}$) et $\eta(p)$ (situation convergente pour $\sum_p \frac{1}{p^{1+\eta(p)}}$) est très faible comme le montrent les résultats numériques suivants (p très grand, $C=1.1$):

$$\begin{aligned} p &= 2\times 10^{40}+477 && eta-upsilon = 0.007099..., \\ p &= 2\times 10^{40}+513 && eta-upsilon = 0.004805..., \\ p &= 2\times 10^{40}+593 && eta-upsilon = -0.004780..., \\ p &= 2\times 10^{40}+723 && eta-upsilon = 0.008382.... \end{aligned}$$

Les "croisements de courbes" (fréquents au début) correspondent aux $p-1$ divisibles par un très grand nombre premier donnant de grands $\phi(d)$ (cas favorables mais non significatifs pour $\sum_p \frac{1}{p^{1+\upsilon(p)}}$). Ci-dessus, on a celui de:

$$p-1 = 2^4\times 3^2\times 11\times 13\times 971250971250971250971250971250971251.$$

3.7. Première majoration du nombre de solutions

Une estimation majorante du nombre de $p\leqslant x$ tels que $q_p(a)=0$ est $\sum_{p\leqslant x}\frac{1}{p^{1+\upsilon(p)}}$. Or la série $\widetilde{S} := \sum_p \frac{1}{p^{1+\upsilon(p)}} = \sum_p \frac{1}{p\,(p-1)^2}\sum_{d\,|\,p-1}\phi(d)^2$, comme on pouvait s'y attendre, est divergente, et G. Tenenbaum a démontré que

$$\widetilde{S}(x) := \sum_{p\leqslant x}\frac{1}{p\,(p-1)^2}\sum_{d\,|\,p-1}\phi(d)^2 = O(\log_2(x))$$

lorsque $x\to\infty$ ([T2]). Sa démonstration repose entre autres sur le théorème de Bombieri–Vinogradov ([T1], Théorème II.8.34).

On en déduit, en admettant le principe de Borel–Cantelli, que pour a fixé le nombre moyen de solutions p à $q_p(a)=0$ vérifie:

$$\big|\{p\leqslant x,\ q_p(a)=0\}\big| < \widetilde{S}(x) = O(\log_2(x)) < 0.452...\times\log_2(x), \qquad \text{pour } x\to\infty,$$

après une estimation majorante de la constante (obtenue pour $x=10^9$), ce qui reste une croissance très faible mais ne permet pas de conclure dans le cas de a fixé.

Remarque 3.10. Soient $p_1,\cdots,p_n$ des nombres premiers distincts donnés. Pour chaque $p\in\{p_1,\dots,p_n\}$ soit $(Z_p^j)_{j=1,\dots,p-1}$ la famille des $p-1$ solutions $Z_p^j\in[1,p^2[$ à $q_p(Z_p^j)=0$ (Lemme 3.4); alors tout A satisfaisant à l'un des systèmes de congruences:

$$\begin{cases} A\equiv Z_{p_1}^{j_1} \pmod{p_1^2}, & j_1\in\{1,\dots,p_1-1\}\\ \quad\vdots\\ A\equiv Z_{p_n}^{j_n} \pmod{p_n^2}, & j_n\in\{1,\dots,p_n-1\}\end{cases}$$

conduit à $q_{p_1}(A)=\cdots=q_{p_n}(A)=0$, et c'est en outre une équivalence. Naturellement la solution minimale A devient en général très grande.

Dans une autre direction, il n'est pas rare de trouver des valeurs de a pour lesquelles $q_p(a)\neq 0$ sur un intervalle $p\in[2,x[$ où x est de l'ordre de 10^{10}, ce qui accrédite la finitude et on peut se demander s'il existe des a tels que $q_p(a)\neq 0$ pour tout p. On abordera cette existence au Théorème 4.12 par le calcul effectif, de type "théorème chinois" (cf. Remarque 3.10), de la densité des $A\in\mathbb{N}$ tels que $q_p(A)\neq 0$ pour tout $p\leqslant x$.

Pour $2\leqslant a\leqslant 100$ on trouve les exemples suivants (le cas $p=2$ éliminant tous les $a\equiv 1 \pmod 4$, $p=3$ éliminant tous les $a\equiv 1,8 \pmod 9$, etc.):

Pour $a=34$, la première solution est $p=46145917691$.

Pour $a=66$, la première solution est $p=89351671$.

Pour $a=88$, la première solution est $p=2535619637$.

Pour $a=90$, la première solution est $p=6590291053$.

Pour $a=47$ et $a=72$, on ne trouve aucune solution pour $p\leqslant 10^{11}$.

Dans [KR] on trouve les grandes solutions $p\leqslant 10^{11}$ suivantes, pour $a\in[2,101]$:

$$(a,p)=(5,6692367337),(23,15546404183),(37,76407520781),(97,76704103313),$$

et la solution remarquable $(5,188748146801)$ (se reporter à la Remarque 4.10 (ii) pour une analyse possible de ce phénomène).

4. Seconde analyse probabiliste pour $q_p(a)=0$

L'approche précédente, reposant en partie sur des calculs de densités, ne tient pas assez compte du fait que l'on étudie $q_p(a)$ pour a fixé et $p\to\infty$. Or $q_p(a)=0$ pour $p\gg a$ conduit à de nombreuses solutions dans $[2,p-1[$ puisque

$$q_p(a^j)=0 \qquad \& \qquad a^j\in[2,p-1[\qquad \text{pour } \ 1\leqslant j\leqslant h_p(a):=\Big\lfloor\frac{\log(p)}{\log(a)}\Big\rfloor.$$

Il se pose également la question de savoir si d'autres solutions sont possibles et quel est leur nombre au vu des propriétés de l'application $z \mapsto q_p(z)$.

Mais on peut supposer, sous peine de répartition inhomogène, que ces phénomènes sont limités par le fait que le nombre total de solutions Z dans $[1, p^2[$ est $p-1$, et comme on l'a vu, on peut s'attendre *en moyenne* à un peu moins d'une solution $z \in [2, p-1[$.

D'où la nécessité d'une première étude sur l'intervalle $[2, p-1[$, étude qui est intermédiaire entre les cas $a \in [2, p-1[$ fixé et $Z \in [2, p^2-1[$ et qui, sur un plan heuristique, caractérise les propriétés du quotient de Fermat.

4.1. Etude des solutions $z \in [2, p-1[$ à $q_p(z) = 0$

Répartition des $q_p(z)$ sur $[1, p[$, pour p fixé

Le résultat de Heath-Brown ([H-B], Theorem 1, Corollary, p. 2) affirme que les $q_p(z)$, $z \in [1, p[$, sont uniformément répartis (mod p) ainsi que les résidus (mod p^2) des z^p, $z \in [1, p[$ (or ce sont les solutions $Z \in [1, p^2[$ à $q_p(Z) = 0$, cf. Lemme 3.4 pour $u = 0$), ce qui renforce notre démarche.

On obtient aussi le curieux phénomène de répartition suivant. On calcule la somme des puissances de $q_p(z)$ vus dans $[0, p[$:

$$\sigma_n(p) := \frac{n+1}{(p-1)^{n+1}} \sum_{z=1}^{p-1} q_p(z)^n,$$

pour tout $n \geqslant 1$. On obtient alors, quel que soit n, une remarquable convergence alternée vers 1 lorsque $p \to \infty$ (couples $(p, \sigma_n(p))$ avec $n = 11$):

$$\begin{array}{lll} (50001037,\ 1.0000456), & (50002037,\ 0.9997580), & (50003039,\ 0.9998901), \\ (50004049,\ 0.9995318), & (50005079,\ 1.0003779), & (50006093,\ 1.0002476), \\ (50007101,\ 1.0005291), & (50008129,\ 0.9999471), & (50009143,\ 1.0000493), \\ (50010157,\ 0.9998406), & (50011019,\ 0.9997204), & (50012029,\ 1.0002561). \end{array}$$

La valeur moyenne des exemples ci-dessus étant 1.000016182....

Pour $n = 100$ les résultats numériques (avec les mêmes nombres premiers) sont quasi-identiques et conduisent à une moyenne de 0.999796908....

Répartition des p par nombre de solutions

Le Programme 1 de [Gr3] (d'exécution assez longue), calcule les proportions de nombres premiers p pour lesquels on a *exactement* 0, 1, ou 2 solutions, puis lorsque l'on a *au moins* 3 solutions $z \in [2, p-1[$ telles que $q_p(z) = 0$.

Dans ce cas, les résultats numériques sont remarquablement cohérents avec la répartition probabiliste que nous allons préciser:

cas de 0 solutions:	proportion: 0.3694945...;	probabilité: 0.367879...,
au moins 1 solution:	proportion: 0.6305054...;	probabilité: 0.632120...,
au moins 2 solutions:	proportion: 0.2646531...;	probabilité: 0.264241...,
au moins 3 solutions:	proportion: 0.0805782...;	probabilité: 0.080301....

Pour les nombres premiers de l'intervalle $]2.10^3, 2\,(10^3 + 10^5)[$, il y a 17866 solutions cumulées pour 17845 nombres premiers (une solution en moyenne comme prévu).

Cas des solutions "exceptionnelles"

Lorsque $q_p(a) = 0$ pour $p \gg a$, on parlera de *solutions exceptionnelles* pour les puissances $a^j \in [2, p-1[$, $j = 1, \ldots, h_p(a)$; on verra plus loin que l'on peut considérer qu'il ne s'agit que d'une question de répartition et non d'une dépendance probabiliste.

Ce type de "répétitions" se produit aussi en dehors de l'existence de $a \ll p$ tel que $q_p(a) = 0$ (ce qui sera un point fondamental de justification d'une heuristique probabiliste, cf. § 4.2).

Remarque 4.1. On peut aussi faire le même genre d'analyse sur $\lambda_p(z) = z\, q_p(z)$, $z \in [2, p-1[$, en étudiant le nombre de solutions à $\lambda_p(z) = v$, v donné dans $[0, p[$, sachant que le résultat de [H-B] donne aussi leur répartition uniforme; pour $10^3 \leqslant p \leqslant 10^3 + 10^4$ il y a 1168 nombres premiers, et on a retenu le nombre N de cas pour lesquels il y a au moins 4 solutions:

En prenant d'abord $v = 0, \ldots, 9$, on obtient $(v, N) = (0, 24)$, $(1, 21)$, $(2, 26)$, $(3, 17)$, $(4, 20)$, $(5, 33)$, $(6, 25)$, $(7, 21)$, $(8, 22)$, $(9, 21)$.

Pour une autre tranche de v, on a $(v, N) = (123, 21)$, $(124, 11)$, $(125, 27)$, $(126, 23)$, $(127, 32)$, $(128, 19)$, $(129, 17)$, $(130, 21)$, $(131, 18)$, $(132, 21)$.

La moyenne cumulée observée pour le nombre N est de 22; or $\frac{22}{1168} \approx 0.0188...$, et la probabilité pour "au moins 4 solutions à $\lambda_p(z) = v$" (analogue à celle relative à $q_p(z) = u$) est égale à 0.0189... (Remarque 4.6 (iv)).

4.2. Définitions des invariants $m_p(u)$ et M_p

On considère le nombre $m_p(u)$ de répétitions de $z \in [2, p-1[$ ayant le même quotient de Fermat $u \in [0, p[$ fixé, puis $M_p = \sup_{u \in [0,p[} \big(m_p(u)\big)$. On obtient alors une stabilité remarquable pour M_p, fonction très régulière de p pouvant faire l'objet de l'heuristique suivante:

Heuristique 4.2. *Le nombre maximum* $M_p = \sup_{u \in [0,p[} \big(m_p(u)\big)$ *de valeurs de* $z \in [2, p-1[$ *ayant même quotient de Fermat est* $O(\log(p))$ *pour tout nombre premier* $p \geqslant 2$.

Solutions exceptionnelles vs solutions abondantes

Le cas des solutions exceptionnelles pouvant poser question par le fait que les solutions données par les $h := h_p(a)$ premières puissances de a ne sont pas aléatoires et de ce fait semblent dépendantes au plan probabiliste, analysons l'heuristique précédente afin de justifier qu'il n'en est rien.

Soit $g \in \mathbb{Z}$ une racine primitive modulo p. Supposons qu'il existe $m_p(0) = O(\log(p))$ solutions $z_i \in [2, p-1[$ à $q_p(z) = 0$ (on parle alors de *solutions abondantes* dans $[2, p-1[$ car on a $m_p(0) \approx M_p$); on a $z_i \equiv g^{t_i} \pmod p$, $t_i \in \mathbb{Z}/(p-1)\mathbb{Z}$. C'est exclusivement une propriété de p et de l'intervalle $[1, p[$ et on peut admettre que les t_i sont aléatoires. De plus ils ne sont définis qu'à un automorphisme près de $\mathbb{Z}/(p-1)\mathbb{Z}$.

Ensuite, toujours dans le cas de solutions abondantes z_i, on peut se demander si $a \ll p$ (e.g. $a = 2, 3, \ldots$) est tel que $q_p(a) = 0$; ceci implique par exemple $z_i = a^i \in [2, p-1[$, pour tout $i = 1, \ldots, h \leqslant m_p(0)$, et constitue un sous-cas moins probable, l'ensemble $\{t_i,\ 1 \leqslant i \leqslant h\}$ d'exposants correspondant étant *nécessairement* égal à $\{k, 2\,k, \ldots, h\,k\}$ si $a \equiv g^k \pmod p$ (pour a donné, on peut choisir g telle que $k = \frac{p-1}{d}$, $d = o_p(a)$, car $d > h$, auquel cas $i\,k < p\ \forall i$). La situation la plus générale étant que l'ensemble des $m_p(0)$ solutions abondantes est mixte de la forme:

$$\{b, b^2, \ldots, b^{h'}, z_{h'+1}, \ldots, z_{m_p(0)}\}, \qquad \text{avec } 0 \leqslant h' \leqslant m_p(0),$$

où $b \in [2, p-1[$ est la solution minimale, toute valeur $h' \in [0, O(\log(p))]$ étant rencontrée. Noter que la probabilité d'une solution minimale $b < \sqrt{p}$ est inférieure à $\frac{1}{\sqrt{p}}$. Le cas $b = a \ll p$ (cas exceptionnel) n'étant alors qu'un hasard pour lequel on a *mécaniquement* $t_i \equiv i\,k \mod (p-1)\mathbb{Z}$ pour presque tout i en raison de la proximité de h et $m_p(0)$. Autrement dit, on a un contexte "p-adique" sur lequel se greffe une considération Archimédienne. Voir le § 4.3 pour l'aspect numérique des solutions abondantes et la Remarque 4.3 pour un éclairage complémentaire.

Expérimentation numérique sur M_p.

Donnons quelques aspects numériques (Programme 3 de [Gr3]):

(α) *Cas des petits nombres premiers.* La régularité a lieu dès le début car on obtient les valeurs (p, M_p) suivantes pour $2 \leqslant p \leqslant 100$:

$(2,0),\ (3,1),\ (5,2),\ (7,2),\ (11,2),\ (13,2),\ (17,3),\ (19,2),\ (23,3),\ (29,3),\ (31,2),$
$(37,3),\ (41,3),\ (43,2),\ (47,3),\ (53,3),\ (59,4),\ (61,4),\ (67,5),\ (71,3),\ (73,4),$
$(79,3),\ (83,4),\ (89,4),\ (97,3).$

(β) *Cas des grands nombres premiers.* On a ensuite les valeurs (p, M_p) suivantes pour $100003 \leqslant p \leqslant 100313$:

$(100003,7),\ (100019,7),\ (100043,8),\ (100049,9),\ (100057,8),\ (100069,7),$
$(100103,8),\ (100109,8),\ (100129,7),\ (100151,8),\ (100153,7),\ (100169,8),$
$(100183,8),\ (100189,7),\ (100193,9),\ (100207,9),\ (100213,8),\ (100237,8),$
$(100267,8),\ (100271,7),\ (100279,7),\ (100291,8),\ (100297,8),\ (100313,8).$

Moyenne des M_p sur les $p \in [100003, 100313]$, égale à $M \approx 7.79...$, moyenne des $\log(p)$ égale à $S \approx 13.96...$, avec $M/S \approx 0.558...$.

Dans la limite des possibilités (listes L à p éléments) on obtient pour $p = 48543217$, $M_p = 10$, $\log(p) \approx 17.698...$, et $M_p/\log(p) \approx 0.5650...$.

(γ) *Données numériques pour $p = 100003$.* Il est utile de voir quels sont les $u \in [0, p[$ et les $z \in [2, p-1[$ qui réalisent M_p-fois le même quotient de Fermat u. Pour $p = 100003$, où $M_p = 7$, on obtient les résultats suivants:

$$\begin{aligned}
u_1 &= 7504 \qquad z_1 \in \{10670,\ 11850,\ \ 1700,\ 53108,\ 59887,\ 80486,\ 82613\}\\
u_2 &= 9011 \qquad z_2 \in \{4199,\ 26730,\ \ 3895,\ 69156,\ 71121,\ 87157,\ 88803\}\\
u_3 &= 13940 \qquad z_3 \in \{646,\ 13662,\ 26364,\ 41841,\ 46741,\ 64523,\ 79877\}\\
u_4 &= 79026 \qquad z_4 \in \{26892,\ 38196,\ 54518,\ 58955,\ 62398,\ 78928,\ 80081\}\\
u_5 &= 91190 \qquad z_5 \in \{3551,\ \ 9604,\ 15491,\ 20035,\ 63185,\ 80223,\ 82748\}.
\end{aligned}$$

On constate que les valeurs de z ne sont pas du type $a \ll p$, mais que $M_p = 7$ est réalisé par cinq valeurs de u.

(δ) *Cas des solutions exceptionnelles.* Le cas $a = 2$, avec $q_{1093}(a) = 0$, conduit à la série de valeurs suivantes pour (p, M_p) $(1039 \leqslant p \leqslant 1163)$:

$$\begin{aligned}
&(1039, 7),\ (1049, 5),\ (1051, 5),\ (1061, 5),\ (1063, 5),\ (1069, 5),\\
&(1087, 5),\ (1091, 5),\ (1093, 11),\ (1097, 7),\ (1103, 7),\ (1109, 6),\\
&(1117, 5),\ (1123, 5),\ (1129, 5),\ (1151, 5),\ (1153, 6),\ (1163, 6).
\end{aligned}$$

Pour $p = 1093$, on obtient $M_p = 11$, or on a seulement $h_p(2) = 10$ et $m_p(0) = 10$. Le plus remarquable est que la valeur $q_p(z) = 624$ se produit 11 fois, à savoir pour $z = 9, 2.9, 2^2.9, 71, 2^3.9, 2.71, 2^4.9, 2^2.71, 2^5.9, 2^3.71, 2^6.9$, et que la valeur $q_p(z) = 960$ se produit aussi 11 fois, pour $z = 13, 2.13$, $2^2.13$, 93, $2^3.13$, 2.93, $2^4.13$, $2^2.93$, $2^5.13$, $2^3.93$, $2^6.13$. On a donc $M_p = m_p(624) = m_p(960) = 11$.

Pour $a = 3$, $p = 1006003$, $q_p(a) = 0$ et $h_p(3) = 12$; on a cependant $m_p(u) = 16$ pour $u = 56450, 1004048$, et $M_p = m_p(u) = 17$ pour $u = 297548$; dans ce dernier cas, les valeurs de z qui réalisent $q_p(z) = 297548$ sont: 3389, 8102, 3.3389, 3.8102, $3^2.3389$, 51550, $3^2.8102$, $3^3.3389$, 3.51550, $3^3.8102$, 236000, $3^4.3389$, 340292, $3^2.51550$, $3^4.8102$, 3.236000, $3^5.3389$.

Il est clair que s'il existe $a \ll p$ tel que $q_p(a) = 0$ (solutions exceptionnelles), ceci peut conduire à une plus grande valeur de $M_p = m_p(u_0)$ puisque si $q_p(z_0) = u_0$, alors on a les solutions $a^j z_0$ pour tout $j \leqslant \left\lfloor \frac{\log(p)}{\log(a)} - \frac{\log(z_0)}{\log(a)} \right\rfloor$. Dans le cas $q_p(2) = u_0 \neq 0$, on obtient systématiquement $O(\log(p))$ solutions à $q_p(z) = u_0$ en plus peut-être des $O(\log(p))$ solutions attendues. Mais ceci ne modifie pas l'heuristique en $O(\log(p))$ pour M_p.

4.3. Etude numérique de $m_p(0)$

Ici, nous imposons la valeur $u = 0$ pour l'étude des répétitions; si l'on se restreint aux nombres premiers p tels que $m_p(0) = O(\log(p))$ (solutions abondantes), il y a une très importante raréfaction des nombres premiers p.

Recherche des solutions abondantes ($m_p(0) = O(\log(p))$)

Nous allons constater qu'il existe des valeurs de p où $m_p(0) = O(\log(p))$ sans que cela ne provienne d'un $a \ll p$ tel que $q_p(a) = 0$.

Les couples $(p, m_p(0))$ correspondants, pour $p < 10^5$, aux répétitions issues d'un $a \ll p$, sont omis et sont pour mémoire $(1093, 10)$, $(3511, 11)$, $(20771, 6)$, $(40487, 8)$, $(66161, 6)$. Le tableau ci-dessous indique les couples $(p, m_p(0))$ pour $m_p(0) \geqslant 6$ et $2 \leqslant p \leqslant 1.5 \times 10^5$, ainsi que les solutions $z \in [2, p-1[$ à $q_p(z) = 0$ (Programme 2 de [Gr3]):

(5107, 6)	{560, 1209, 1779, 2621, 4295, 4361}
(51427, 6)	{10364, 14795, 26183, 28411, 34111, 39159}
(52517, 6)	{13425, 18243, 34196, 38462, 39362, 51787}
(61417, 6)	{12947, 15631, 17144, 20287, 41739, 51605}
(103291, 7)	{14866, 27419, 39660, 80408, 92041, 96106, 98404}
(116731, 6)	{5999, 21399, 32127, 61099, 69145, 115067}
(119359, 6)	{25627, 26486, 43165, 57879, 78988, 98633}
(128657, 6)	{28237, 62334, 85135, 120099, 123891, 125137}
(140741, 6)	{44757, 53828, 63099, 107890, 133072, 137002}
(147647, 6)	{198, 39204, 75352, 90252, 98878, 141188}

En continuant jusqu'à $p \approx 10^6$, on obtient les nombres premiers suivants:

150559, 199783, 203773, 213949, 229939, 237283, 261761, 286751, 288929, 303089, 339139, 342373, 381853, 384611, 385657, 475897, 491531, 528679, 534851, 553699, 559831, 560317, 565937, 571933, 577069, 584791, 587123, 602227, 602627, 616513, 622159, 631549, 634609, 634979, 663587, 728471, 733277, 747871, 757403, 767071, 778187, 781283, 785779, 787079, 797897, 800677, 804367, 824753, 879239, 893609, 907589, 921001, 997961,

pour lesquels on a $m_p(0) = 6$ sauf pour $p = 491531$ où $m_p(0) = 7$ et où les solutions z sont données par six puissances de $b = 7$ et $397783 = 17 \times 23399$; de même pour $p = 534851$, où $m_p(0) = 7$, les solutions z sont données par sept puissances de $b = 6$ (cas avec solutions en partie exceptionnelles).

Par contre, on a $m_p(0) = 7$ pour $p = 804367$ et la liste des solutions {100933, 434207, 586707, 654355, 677456, 750045, 751958}, puis $m_p(0) = 8$ pour $p = 728471$ et la liste {36709, 159316, 241830, 288664, 418571, 443653, 653451, 679977} et enfin $m_p(0) = 7$ pour $p = 997961$ et la liste {196462, 324572, 505976, 517837, 612235, 636080, 990873}.

Comparaison de $\mathbf{Prob}(m_p(0) \geqslant n)$ et $\mathbf{Prob}(q_p(a') = 0)$

En utilisant la probabilité donnée plus loin (Remarque 4.6 (i)), on trouve que pour $p \approx 5 \times 10^5$ la probabilité d'un cas de solutions abondantes avec $m_p(0) = 6$ est

égale à 0.000594... $\approx \frac{1}{p^{1+\epsilon}}$ avec $\epsilon \approx -0.433916...$, ce qui en termes de solutions exceptionnelles qui proviendraient d'un $a' \ll p$ (a' fictif fixé) donnerait, pour $h_p(a') = 6$, $a' = 8$ ou 9 en moyenne, qui doit être considérée comme déjà "trop grand" si l'on avait prévu d'étudier le cas de a donné petit ($a = 2$ par exemple); en effet, on a pour $p \approx 5 \times 10^5$:

$$h_p(2) = 18, \quad h_p(3) = 11, \quad h_p(4) = 9, \quad h_p(5) = 8, \quad h_p(6) = 7,$$
$$h_p(7) = \lfloor 6.743... \rfloor, \quad h_p(8) = \lfloor 6.310... \rfloor, \quad h_p(9) = \lfloor 5.972... \rfloor, \qquad \text{etc.}$$

Autrement dit, $m_p(0) \geqslant 6$ (dans le cadre abondant) est plus probable que l'existence de a' fixé tel que $q_p(a') = 0$, dans la mesure où il correspondrait à un a' moyen (fictif), non "très petit par rapport à p" (probablement $a' = O(\log(p))$).

Si l'on écrit les probabilités sous la forme $\text{Prob}\big(q_p(a') = 0\big) = \frac{1}{p^{1+\epsilon}}$, on obtient (pour $p \approx 5 \times 10^5$), le tableau suivant:

$$(a' = 2, \epsilon \approx +1.845); \qquad (a' = 3, \epsilon \approx +0.403); \qquad (a' = 4, \epsilon \approx +0.044);$$
$$(a' = 5, \epsilon \approx -0.124); \qquad (a' = 6, \epsilon \approx -0.284); \qquad (a' = 7, \epsilon \approx -0.434);$$
$$(a' = 8, \epsilon \approx -0.434); \qquad (a' = 9, \epsilon \approx -0.572).$$

Pour a' assez grand, le ϵ est négatif, donnant une probabilité supérieure à $\frac{1}{p}$. En décroissant vers $a' = 4$, on commence à obtenir une probabilité inférieure à $\frac{1}{p}$. Quant à $a' = 2$, on obtient une probabilité de la forme $\frac{1}{p^{1+\epsilon}}$ avec $\epsilon \approx 1.845...$. La probabilité $\text{Prob}\big(m_p(0) \geqslant n\big)$ est supérieure à celle qui proviendrait d'une solution exceptionnelle $a' \ll p$ fictive fixée assez petite.

Remarque 4.3. On pourrait se placer dans n'importe quel intervalle de $\mathbb{Z}$, translaté modulo p, $I_p^{(t)} := [-t\,p + 1, (-t+1)\,p[$, $t \in [0, p[$, en renormalisant de la façon suivante: on remplace $q_p(x)$ par $x\,q_p(x) = \lambda_p(x)$ (cf. Lemme 3.4 et Remarque 4.1) et on considère l'application T définie par $T(z) = z - t\,p$ pour tout $z \in [1, p[$. Si $a \in [1, p[$ est fixé et est tel que $aq_p(a) = 0$, il vient facilement:

$$T(a^j)\,q_p(T(a^j)) \equiv a^j\,q_p(a^j) + t \equiv t \pmod{p},$$

pour tout j tel que $a^j \in [1, p[$; comme $T(a^j) \in I_p^{(t)}$, on a bien translaté les solutions exceptionnelles (relatives à $u = 0$ dans $I_p^{(0)}$) en des solutions exceptionnelles relatives à $u = t$ dans $I_p^{(t)}$. Un calcul identique montre que les éventuelles solutions abondantes $z_i \in [1, p[$ (pour $u = 0$) sont translatées dans $I_p^{(t)}$ par l'opération T en solutions abondantes (pour $u = t$) et inversement, ce qui relativise les deux notions abondantes/exceptionnelles, ainsi que le phénomène Archimédien à l'origine des solutions exceptionnelles.

Une étude numérique (non reproduite ici) montre que les valeurs statistiques ($m_p(\bullet)$, M_p) sur $I_p^{(t)}$, sont analogue à celle sur $I_p^{(0)}$, ce qui fait que nous pouvons supposer $t = 0$ avec les données et définitions habituelles.

4.4. Sur l'existence d'une loi binomiale pour $m_p(0)$

L'étude précédente conduit à une heuristique utilisant une loi binomiale (majorante) de paramètres $\big(p-1, \frac{1}{p}\big)$, car on peut considérer que l'on réalise n "tirages" $z \in [1, p[$ (ensemble à $p-1$ éléments) pour lesquels on regarde combien de fois on obtient l'événement $q_p(z) = 0$ (ou plus généralement $q_p(z) = u$, $u \in [0, p[$ fixé, si l'on prend en compte les résultats du § 4.2). On néglige le biais provenant de $z = 1$ et $z = p-1$. La relation de dépendance rappelée Remarque 3.5 (ii) conduit à supposer n assez petit ($n \ll p$). Le second paramètre $\frac{1}{p}$ est une approximation de $\mathrm{Prob}\big(q_p(z) = u\big)$. Par conséquent, on devrait remplacer $\frac{1}{p}$ par $\frac{1}{p^{\kappa(z)}}$, $\kappa(z) > 1$.

On vérifie que cela ne modifie pas la nature des résultats ultérieurs (Lemmes 4.5, 4.7, 4.8, Théorème 4.9) et conduit à des probabilités majorantes. Aussi on conservera $(p-1, \frac{1}{p})$ par commodité.

La probabilité d'avoir exactement $n \ll p$ cas favorables $z \in [2, p-1[$ est alors:

$$\binom{p-1}{n} \frac{1}{p^n} \left(1 - \frac{1}{p}\right)^{p-1-n} = \binom{p-1}{n} \frac{1}{p^{p-1}} (p-1)^{p-1-n}.$$

Heuristique 4.4. *Soit $u \in [0, p[$ fixé. Soit $n \geqslant 0$, $n \ll p$; alors la probabilité d'avoir au moins n valeurs $z_1, \ldots, z_n \in [2, p-1[$ telles que $q_p(z_j) = u$ pour $j = 1, \ldots, n$ (i.e., $m_p(u) \geqslant n$), est donnée par l'expression:*

$$\mathrm{Prob}\big(\big|\big\{z \in [2, p-1[,\ q_p(z) = u\big\}\big| \geqslant n\big) \leqslant \frac{1}{p^{p-1}} \sum_{j=n}^{p-1} \tbinom{p-1}{j} (p-1)^{p-1-j}.$$

Lemme 4.5. *On a*

$$\frac{1}{p^{p-1}} \sum_{j=n}^{p-1} \binom{p-1}{j} (p-1)^{p-1-j} < \frac{1}{p^n} \binom{p-1}{n}$$

pour tout $n \leqslant p-1$.

Démonstration. Vérifions que $\sum_{j=n}^{p-1} \binom{p-1}{j} (p-1)^{p-1-j} < \binom{p-1}{n} p^{p-1-n}$ pour tout $n \leqslant p-1$. On considère, pour $0 \leqslant n \leqslant N$, $t \in]1, \infty[$, la dérivée de la fonction $f_{N,n}(t) = \sum_{j=n}^{N} \binom{N}{j} (t-1)^{N-j} - \binom{N}{n} t^{N-n}$; elle est égale à $N f_{N-1,n}(t)$. On raisonne ensuite par récurrence, à partir de $f_{n,n}(t) = 0$ et de $f_{N,n}(1) < 0$, pour montrer que la dérivée est négative ou nulle sur tout l'intervalle $]1, \infty[$. On aura ensuite à poser $t = p$, $N = p-1$. ∎

Remarques 4.6.

(i) On a, pour $n \ll p$, la formule plus commode ($p \to \infty$) $\mathrm{Prob}\big(m_p(u) \geqslant n\big) = 1 - \big(1 - \frac{1}{p}\big)^p \frac{p}{p-1} \sum_{j=0}^{n-1} \frac{1}{(p-1)^j} \binom{p-1}{j}$.

(ii) La probabilité d'avoir 0 solutions est $\big(1 - \frac{1}{p}\big)^p \frac{p}{p-1} \approx e^{-1} \approx 0.36788....$

(iii) Celle d'au moins une solution est proche de $1 - e^{-1} \approx 0.63212....$

(iv) Celle d'au moins 2 solutions est proche de $1 - 2\,e^{-1} \approx 0.264...$; pour au moins 3 (resp. 4) solutions, on obtient 0.0803... (resp. 0.0189...).

Application à la probabilité de nullité de $q_p(a)$

Maintenant, nous supposons que $u = 0$, que a est fixé et que $p \to \infty$. On a $\mathrm{Prob}\big(q_p(a) = 0\big) < \mathrm{Prob}\big(m_p(0) \geqslant h\big)$, où $h = \big\lfloor \frac{\log(p)}{\log(a)} \big\rfloor$, puisque alors $a, \dots, a^h \in [2, p-1[$ sont h solutions distinctes. Or, lorsque $p \to \infty$, le rapport $\dfrac{\mathrm{Prob}\big(m_p(0) \geqslant h\big)}{p^{-h}\binom{p-1}{h}}$ (majoré par 1 d'après le Lemme 4.5) tend rapidement vers une constante $C_\infty(a)$, en décroissant, selon le résultat suivant:

Lemme 4.7.

(i) *On a pour p assez grand l'encadrement:*

$$\exp\big(-1 + \frac{1}{p}(h + \frac{1}{2})\big) < \frac{p^{-(p-1)} \sum_{j=h}^{p-1} \binom{p-1}{j} (p-1)^{p-1-j}}{p^{-h}\binom{p-1}{h}} < 1.$$

(ii) *Il en résulte* $\mathrm{Prob}\big(q_p(a) = 0\big) < \mathrm{Prob}\big(m_p(0) \geqslant h\big) \approx C_\infty(a) \times \frac{1}{p^h}\binom{p-1}{h}$ *pour tout p assez grand, où la constante $C_\infty(a)$ vérifie $e^{-1} \leqslant C_\infty(a) < 1$.*

Démonstration. On a la minoration

$$\begin{aligned}
&\frac{p^h}{\binom{p-1}{h}} \times \frac{1}{p^{p-1}} \sum_{j=h}^{p-1} \binom{p-1}{j} (p-1)^{p-1-j} \\
&\quad = \Big(\frac{p-1}{p}\Big)^{p-1} \frac{p^h\, h!}{(p-h)\cdots(p-1)} \sum_{j=h}^{p-1} \frac{1}{j!} \frac{p-j}{p-1} \cdots \frac{p-1}{p-1} \\
&\quad = \Big(\frac{p-1}{p}\Big)^{p-1} \frac{p^h}{(p-1)^h} \sum_{j=h}^{p-1} \frac{h!}{j!} \frac{p-j}{p-h} \cdots \frac{p-1}{p-1} \times \frac{1}{(p-1)^{j-h}} \\
&\quad = \Big(\frac{p-1}{p}\Big)^{p-1-h} \Big[1 + \frac{p-(h+1)}{(p-1)(h+1)} + \cdots + \frac{p-(h+1)}{(p-1)(h+1)} \cdots \frac{p-j}{(p-1)\,j} + \cdots \\
&\qquad \cdots + \frac{p-(h+1)}{(p-1)(h+1)} \cdots \frac{p-(p-1)}{(p-1)(p-1)}\Big] > \Big(\frac{p-1}{p}\Big)^{p-1-h} = \Big(1 - \frac{1}{p}\Big)^{p-1-h}.
\end{aligned}$$

D'où facilement le résultat en considérant la minoration:

$$(p-1-h)\log\Big(1 - \frac{1}{p}\Big) = -(p-1-h)\left(\frac{1}{p} + \frac{1}{2p^2} + \cdots\right) > -1 + \frac{1}{p}\Big(h + \frac{1}{2}\Big),$$

tous les termes négligés étant positifs et tendant vers 0 comme $O(\frac{\log(p)}{p^2})$. ∎

On écrira par abus $\mathrm{Prob}\big(q_p(a) = 0\big) < C_\infty(a) \times \frac{1}{p^h}\binom{p-1}{h}$, qui est le majorant obtenu lorsque $m_p(0) = h$. On obtiendra, au niveau de la preuve du Lemme 4.8, que ce majorant est $p^{-\left(\frac{\log_2(p)}{\log(a)} - \frac{\log_2(a)+1}{\log(a)} + O\left(\frac{\log_2(p)}{\log(p)}\right)\right)}$.

Donnons, sous les heuristiques précédentes, des majorants des probabilités d'avoir au moins $h_p(a) = \big\lfloor \frac{\log(p)}{\log(a)} \big\rfloor$ solutions exceptionnelles avec $a = 2$, pour p

croissant; ceci correspondrait au cas où le quotient de Fermat de a serait nul pour des p arbitrairement grands et il convient de voir que c'est numériquement peu compatible.

On écrit alors ces majorants sous la forme $\frac{1}{p^{1+\epsilon}}$ qui correspond à la probabilité exacte de au moins $h_p(a)$ solutions abondantes:

$p = 101$	probabilité $< 5.075... \times 10^{-4}$	$\epsilon = 0.6437...$
$p = 127$	probabilité $< 5.245... \times 10^{-4}$	$\epsilon = 0.5591...$
$p = 10007$	probabilité $< 6.310... \times 10^{-11}$	$\epsilon = 1.5498...$
$p = 200003$	probabilité $< 1.094... \times 10^{-15}$	$\epsilon = 1.8222...$
$p = 1000003$	probabilité $< 3.182... \times 10^{-18}$	$\epsilon = 1.9162...$
$p = 5000011$	probabilité $< 3.421... \times 10^{-22}$	$\epsilon = 2.2043....$

On confirmera dans la section suivante que ϵ tend vers l'infini très lentement. La dernière valeur de p pour laquelle $\epsilon < 1$ est $p = 1021$.

4.5. Conséquence principale – finitude des solutions

Soit $a \geqslant 2$ fixé. Sous l'Heuristique 4.4 on a, pour $p \to \infty$, $\mathrm{Prob}\big(q_p(a) = 0\big) < \mathrm{Prob}\big(m_p(0) \geqslant h\big) \approx C_\infty(a) \times \frac{1}{p^h}\binom{p-1}{h}$, où $h := \big\lfloor \frac{\log(p)}{\log(a)} \big\rfloor$ (Lemme 4.7 (ii)).

Lemme 4.8. *Soit $a \geqslant 2$ fixé. La série $\displaystyle\sum_{p>2} \frac{1}{p^h}\binom{p-1}{h}$ est convergente.*

Démonstration. On a $\frac{1}{p^h}\binom{p-1}{h} = \frac{1}{h!} \times \frac{(p-1)\cdots(p-h)}{p^h}$ que l'on peut majorer par $\frac{1}{h!}$. En outre, on a par définition $\frac{\log(p)}{\log(a)} - 1 < h < \frac{\log(p)}{\log(a)}$. Pour tenir compte de ce fait, et afin d'utiliser analytiquement $\frac{\log(p)}{\log(a)}$ au lieu de h dans les formules, on utilise la majoration $\frac{1}{p^h}\binom{p-1}{h} < \frac{h}{h!}$, où l'on a remplacé $\frac{h}{h!}$ par $\frac{\log(p)}{\log(a)}\big/\big(\frac{\log(p)}{\log(a)}\big)!$ où h désigne maintenant $\frac{\log(p)}{\log(a)}$ et $\frac{h}{h!} = \frac{1}{\Gamma(h)}$.

On a $\Gamma(h) = \sqrt{2\pi} \times h^{h-\frac{1}{2}}\, e^{-h} \times (1 + O(\frac{1}{h}))$, d'où en prenant le logarithme:

$$\begin{aligned}
\log\big(\Gamma(h)\big) &= \log\big(\sqrt{2\pi}\big) + \Big(h - \frac{1}{2}\Big)\log(h) - h + \log\Big(1 + O\big(\frac{1}{h}\big)\Big) \\
&= h(\log(h) - 1) - \frac{1}{2}\log(h) + \log(\sqrt{2\pi}) + O\big(\frac{1}{h}\big) \\
&= \frac{1}{\log(a)}\log(p)\Big(\log_2(p) - \log_2(a) - 1\Big) \\
&\quad - \frac{1}{2}\Big(\log_2(p) - \log_2(a)\Big) + \log(\sqrt{2\pi}) + O\big(\frac{1}{\log(p)}\big) \\
&= \Big[\frac{1}{\log(a)}\Big(\log_2(p) - \log_2(a) - 1\Big) \\
&\quad - \frac{1}{2}\frac{1}{\log(p)}\Big(\log_2(p) - \log_2(a)\Big) + O\big(\frac{1}{\log(p)}\big)\Big]\log(p) =: Y \times \log(p).
\end{aligned}$$

D'où $\frac{h}{h!}=\frac{1}{p^Y}$, où $Y=\frac{\log_2(p)}{\log(a)}+O(1)$ tend vers l'infini comme $\frac{\log_2(p)}{\log(a)}$, et la convergence de la série initiale. Pour toute constante $E>1$, il existe p_0 assez grand tel que $Y>E$ et $\frac{h}{h!}<\frac{1}{p^E}$ pour tout $p\geqslant p_0$. ■

Rappelons que l'on parle de solutions abondantes si le nombre $m_p(0)$ de $z\in[2,p-1[$ tels que $q_p(z)=0$ est au moins $O(\log(p))$. Les calculs précédents obtenus avec $h_p(a)$ sont valables pour toute expression en $O(\log(p))$ et on peut énoncer:

Théorème 4.9. *Soit $a\geqslant 2$ fixé. Si l'Heuristique 4.4 est vraie (existence d'une loi de probabilité binomiale pour $m_p(0)$), on a la majoration:*

$$\mathrm{Prob}\big(q_p(a)=0\big)<C_\infty(a)\times\frac{1}{p^h}\binom{p-1}{h}<C_\infty(a)\times p^{-\left(\frac{\log_2(p)}{\log(a)}-\frac{\log_2(a)+1}{\log(a)}+O\left(\frac{\log_2(p)}{\log(p)}\right)\right)},$$

pour $p\to\infty$, où $h=\left\lfloor\frac{\log(p)}{\log(a)}\right\rfloor$ (partie entière) et $e^{-1}<C_\infty(a)<1$.

Sous le principe de Borel–Cantelli, le nombre de p tels que l'on ait un cas de solutions abondantes dans $[2,p-1[$ est fini; a fortiori, le nombre de p tels que l'on ait $q_p(a)=0$ est fini.

Remarques 4.10.

(i) Les majorations utilisées pour le Lemme 4.8 sont assez bonnes car, pour $a=2$, les séries $\sum_{p\geqslant 2}\mathrm{Prob}\big(m_p(0)\geqslant h\big)$, $\sum_{p\geqslant 2}\frac{1}{p^h}\binom{p-1}{h}$, et $\sum_{p\geqslant 2}\frac{h}{h!}$, convergent respectivement vers 1.65613..., 2.09444..., 6.27613.... Lorsque a augmente, la limite de la série $\sum_{p\geqslant 2}\mathrm{Prob}\big(m_p(0)\geqslant h\big)$ (censée donner une approximation du nombre de solutions) devient assez grande en raison du terme négatif dans l'exposant $\frac{\log_2(p)}{\log(a)}-\frac{\log_2(a)+1}{\log(a)}+O\big(\frac{\log_2(p)}{\log(p)}\big)$. Un calcul exact de $\binom{p-1}{h}$ via la fonction Γ donne:
$Y=\dfrac{\log_2(p)}{\log(a)}-\dfrac{\log_2(a)+1}{\log(a)}+\dfrac{1}{2}\dfrac{\log_2(p)}{\log(p)}-\dfrac{1}{2}\dfrac{\log_2(a)-\log(2\,\pi)}{\log(p)}+\dfrac{O(1)}{\log^2(p)}$.

(ii) Le fait que l'on puisse choisir E arbitrairement grande dans la preuve du lemme (à condition de sommer à partir d'un p_0 extrêmement grand) montrerait une loi de raréfaction brutale des solutions pour $p\to\infty$. En utilisant l'expression de Y ci-dessus, on obtient les exemples suivants (mais p_0 dépend beaucoup de l'approximation choisie pour Y):
Si $a=2$ et si l'on veut atteindre $E=1$, il suffit d'avoir $p_0\geqslant 17$; pour $E=2$, il faut $p_0\geqslant 577$. Pour $a=3$, il suffit d'avoir $p_0\geqslant 1399$ (resp. $p_0\geqslant 46505941763$). Pour $a=5$ et $E=1$, $p_0=168991001$, et pour $E=2$, on obtient $p_0\approx 4.817...\times 10^{45}$. Dès que a augmente, p_0 devient inaccessible: pour $a=13$, on a $p_0\approx 6.607...\times 10^{36}$ pour $E=1+10^{-6}$, et $p_0\approx 6.268...\times 10^{507}$ pour $E=2$; pour $a=23$, on a $p_0\approx 4.476...\times 10^{81}$ pour $E=1+10^{-6}$ et $p_0\approx 3.491...\times 10^{1952}$ pour $E=2$.

Cette rapide croissance de p_0, pour E raisonnable, laisse la possibilité d'avoir $q_p(a) = 0$ pour de très grands $p < p_0$, inaccessibles par ordinateur, mais en nombre conjecturalement fini; on peut y voir un rapport avec l'exemple donné au § 3.7 ($a = 5, p = 188748146801$) car si l'on calcule Y pour ces données, on trouve $Y = 1.17773...$ qui, de façon remarquable, définit une probabilité seulement en $\frac{1}{p^{1.17773...}}$.

(iii) Pour tout p assez grand on a, en posant $\mathrm{Prob}\big(m_p(0) \geqslant h\big) = \frac{1}{p^{1+\epsilon(p,a)}}$, $\epsilon(p,a) < Y-1 \approx \frac{\log_2(p)}{\log(a)} - 1 - \frac{\log_2(a)+1}{\log(a)}$. La constante $\theta(a) := \frac{\log_2(a)+1}{\log(a)}$ prend les valeurs approchées suivantes: $\theta(2) \approx 0.914...$, $\theta(3) \approx 0.996...$, $\theta(4) \approx 0.957...$, $\theta(5) \approx 0.917...$, $\theta(6) \approx 0.884...$, ...

4.6. Densité des entiers A de quotients de Fermat $\neq 0$

D'après les résultats du § 2.3, appliqués à $A \in \mathbb{N}$, on est amené à considérer (par simple commodité) le produit infini formel $\widetilde{\mathcal{P}}(A) := \prod_{m \geqslant 1} \widetilde{\Phi}_m(A)$ qui est tel que tout nombre premier p impair, $p \nmid A$, en est un diviseur, à savoir $p \mid \widetilde{\Phi}_m(A)$ pour l'unique indice $m = o_p(A)$ (Lemmes 2.4, 2.5); on a alors $q_p(A) \neq 0$ si et seulement si p^2 ne divise pas $\widetilde{\mathcal{P}}(A)$ (Théorème 2.6). Pour $p = 2$, $q_2(A) \neq 0$ si et seulement si $A \equiv 3 \pmod 4$.

Comme $p^2 \mid \widetilde{\mathcal{P}}(A)$ équivaut à $p^2 \mid \widetilde{\Phi}_{o_p(A)}(A)$ ($p \neq 2$), la densité des $A \in \mathbb{N}$ tels que $p^2 \mid \widetilde{\mathcal{P}}(A)$ est égale à $\frac{\phi(o_p(A))}{p^2}$; en sommant sur tous les ordres $o_p(A)$ possibles, on obtient la densité $\frac{p-1}{p^2}$; la densité contraire ($p^2 \nmid \widetilde{\mathcal{P}}(A)$) est égale à $D_p := 1 - \frac{p-1}{p^2} = 1 - \frac{1}{p} + \frac{1}{p^2}$ (valable pour $p = 2$).

On note que ces p-densités sont indépendantes (en raison des propriétés des $\widetilde{\Phi}_m(A)$) et que la densité correspondant à plusieurs p est donnée par le produit des densités locales; en particulier, le produit $\prod_{p \leqslant x} D_p$ donne la densité des $A \in \mathbb{N}$ tels que $p^2 \nmid \widetilde{\mathcal{P}}(A)$ pour tout $p \leqslant x$.

Remarque 4.11. De fait il existe un calcul direct de cette densité par dénombrement de type théorème chinois (Remarque 3.10) avec cette fois des Z_p^j tels que $q_p(Z_p^j) \neq 0$, et ceci pour la suite des nombres premiers $p \leqslant x$. Si $y = \prod_{p \leqslant x} p^2$, un calcul standard montre que le nombre de $A \in [1, y[$ tels que $q_p(A) \neq 0$ pour tout $p \leqslant x$ est exactement $\prod_{p \leqslant x}(p^2 - p + 1)$; d'où la densité précédente, exacte sur les intervalles de la forme $\big[1, \prod_{p \leqslant x} p^2\big[$.

Ecrivons $1 - \frac{1}{p} + \frac{1}{p^2} = \big(1 - \frac{1}{p}\big)\big(1 + \frac{1}{p(p-1)}\big)$. On a $\prod\limits_{p \leqslant x} \big(1 - \frac{1}{p}\big) = \frac{e^{-\gamma}}{\log(x)} \times \big(1 + O\big(\frac{1}{\log(x)}\big)\big)$, où $\gamma \approx 0,577215...$ est la constante d'Euler (cf. [T1], § I.1.6, formule de Mertens), et $\prod\limits_{p \leqslant x} \big(1 + \frac{1}{p(p-1)}\big) \approx 1.9436...$, pour x assez grand, d'où $\prod\limits_{p \leqslant x} D_p = \frac{1.9436... \times e^{-\gamma}}{\log(x)} \times \big(1 + O\big(\frac{1}{\log(x)}\big)\big) = \frac{1.09125...}{\log(x)} \times \big(1 + O\big(\frac{1}{\log(x)}\big)\big)$. On a donc le résultat analytique suivant:

Théorème 4.12. *La densité des $A \in \mathbb{N}$ tels que $q_p(A) \neq 0$ pour tout nombre premier $p \leqslant x$, est égale à $O\Big(\frac{1}{\log(x)}\Big)$. De façon précise, pour x assez grand on a*

$$\lim_{y\to\infty} \frac{1}{y} \times \Big|\big\{A \leqslant y, \quad q_p(A) \neq 0, \ \forall p \leqslant x\big\}\Big| \approx \frac{1.09125...}{\log(x)}.$$

Bien que y doive être pris très grand par rapport à x, on peut tester la répartition des solutions sur de petits intervalles; par exemple, pour $2 \leqslant A \leqslant y = 10^4$, on trouve 665 valeurs de A telles que $q_p(A) \neq 0$ pour tout $p \leqslant x = 10^7$. Or $10^4 \times \frac{1.09...}{\log(10^7)} \approx 676...$ et le résultat est assez satisfaisant.

Prenons $x \approx 10^{10}$, accessible aux calculs; on a $\frac{1.09...}{\log(10^{10})} \approx 0.05....$ Pour les entiers $A \in \mathbb{N}$, il y en a 95% tels que $q_p(A) = 0$ pour au moins un $p \leqslant 10^{10}$. Mais dans ces calculs $A \to \infty$ et, par exemple, $\frac{\log_2(p_0)}{\log(A)} \approx E > 1$ équivaut à $p_0 \approx \exp(A^E)$ si l'on fait référence à l'aspect probabilités.

Ceci est compatible avec une heuristique de finitude pour a fixé; les cas de $a = 47$ et 72 semblent être intéressants de ce point de vue (cf. § 3.7).

Par programme on obtient 2.76 solutions $p < 3 \times 10^9$ en moyenne pour $2 \leqslant a \leqslant 101$. On obtient 2.8 solutions $p < 10^{10} + 5 \times 10^9$ en moyenne pour $a \in \{5, 7, 11, 13, 17, 19, 23, 29, 31, 37\}$.

5. Conclusion

L'Heuristique 3.7, majorant $\mathrm{Prob}\big(q_p(a) = 0\big)$ par $\frac{1}{p\,(p-1)^2} \sum_{d\,|\,p-1} \phi(d)^2 < \frac{1}{p}$, est très raisonnable, mais est insuffisante pour conclure à la finitude des p tels que $q_p(a) = 0$ (a fixé). Si elle est exacte, elle montre que la probabilité $\frac{1}{p}$, souvent admise, pose problème.

L'Heuristique 4.4, qui stipule l'existence d'une loi de probabilité binomiale pour $\mathrm{Prob}\big(m_p(0) \geqslant n\big)$, $n \ll p$, et qui implique la finitude des p conduisant à des solutions abondantes dans $[2, p-1[$ (Théorème 4.9), reste le point crucial pour interpréter l'existence possible de couples (a, p), $a \ll p$, tels que $q_p(a) = 0$, induisant une répartition exceptionnelle des $p-1$ solutions $Z \in [1, p^2[$.

Mais différentes observations justifient cette heuristique:

- Le tableau du § 4.1 montre l'adéquation avec les probabilités théoriques relatives au nombre de solutions à $q_p(z) = 0$, $z \in [2, p-1[$.
- L'étude numérique des §§ 4.2, 4.3, montre que le nombre $m_p(0)$ des répétitions $q_p(z_i) = 0$, $z_i \in [2, p-1[$ pour $i = 1, \ldots, m_p(0)$, est aussi $O(\log(p))$ (solutions abondantes) pour de rares nombres premiers p et n'est pas nécessairement dû au cas "$a \ll p$ & $q_p(a) = 0$", un peu comme s'il était dû à une circonstance cachée analogue, non triviale, reposant sur la construction même des $q_p([g^k]_p)$, $1 \leqslant k \leqslant p-1$, lorsque g est une racine primitive et $[\ ]_p$ la fonction résidu modulo p.
- Les résultats numériques du §§ 4.3, justifient la différence (importante) qu'il y a entre la situation précédente où $m_p(0) = O(\log(p))$ (solutions abondantes),

et la probabilité que ce $m_p(0)$ provienne de solutions exceptionnelles avec $a \ll p$ et $q_p(a) = 0$ $(a = 2, 3, \ldots)$. Autrement dit, rien n'empêche que la probabilité d'avoir $q_p(a) = 0$ ne soit très inférieure à celle d'avoir des solutions abondantes dans $[1, p[$, et une heuristique forte de finitude pourrait être que, en moyenne, $q_p(a) = 0$ pour 3 nombres premiers p.

- Enfin le nombre $M_p = \sup_{u\in[0,p[}\big(m_p(u)\big)$ est très stable en $O(\log(p))$ *pour tout nombre premier* $p \geqslant 2$, ce qui constitue certainement le phénomène le plus intéressant (voir en complément le calcul heuristique de [Gr2]). Une preuve de ce fait serait importante car elle entraînerait trivialement que $m_p(0)$ ne dépasse jamais $O(\log(p))$ ce qui renforcerait les observations précédentes.

Ceci dit, cette étude ainsi que les expérimentations numériques, me confortent dans la pertinence des conjectures de finitude que j'ai formulées dans le cadre très général du régulateur p-adique (normalisé) d'un élément η d'un corps de nombres K, Galoisien sur $\mathbb{Q}$ (cf. [Gr1], § 8). De plus, l'équivalent probabiliste

$$p^{-\left(\frac{\log_2(p)}{\log(a)} - \frac{\log_2(a)+1}{\log(a)} + O\left(\frac{\log_2(p)}{\log(p)}\right)\right)}, \qquad p \to \infty,$$

est universel pour tout corps K et tout élément η (engendrant un Galois module de $\mathbb{Z}$-rang $[K : \mathbb{Q}]$) en remplaçant a par le maximum des valeurs absolues des conjugués de η ([Gr1], Théorème 1.1).

Remerciements. Je remercie Gérald Tenenbaum pour sa contribution [T2], ainsi que l'Editeur de la revue pour ses suggestions de publication, et le Rapporteur pour ses remarques.

Références

[CDP] R. Crandall, K. Dilcher, and C. Pomerance, *A search for Wieferich and Wilson primes*, Math. Comp. 66, 217 (1997), 433–449.

[EM] R. Ernvall and T. Metsänkylä, *On the p-divisibility of Fermat quotients*, Math. Comp. **66** (1997), no. 219, 1353–1365.

[G] A. Granville, *ABC allows us to count squarefrees*, Internat. Math. Res. Notices **19** (1998), 991–1009.

[Gr1] G. Gras, *Les θ-régulateurs locaux d'un nombre algébrique – Conjectures p-adiques*, Canadian Journal of Mathematics, to appear (2016). http://dx.doi.org/10.4153/CJM-2015-026-3

[Gr2] G. Gras, *Complément : Estimation numérique de M_p pour la loi de probabilité binomiale de paramètres* $(p-1, \frac{1}{p})$. https://www.researchgate.net/publication/277588496

[Gr3] G. Gras, *Programmes PARI*, https://www.researchgate.net/publication/294260146

[GM] H. Graves and M.R. Murty, *The abc conjecture and non-Wieferich primes in arithmetic progressions*, Journal of Number Theory **133** (2013), 1809–1813.

[Hat] K. Hatada, *Mod 1 distribution of Fermat and Fibonacci quotients and values of zeta functions at* $2-p$, Comment. Math. Univ. St. Pauli **36** (1987), 41–51.

[Hat] K. Hatada, *Chi-square tests for mod 1 distribution of Fermat and Fibonacci quotients*, Sci. Rep. Fac. Educ., Gifu Univ., Nat. Sci. **12** (1988), 1–2.

[H-B] R. Heath-Brown, *An Estimate For Heilbronn's Exponential Sum*, In: Conference in honor of Heini Halberstam, Analytic Number Theory **2** (1996), Birkhüser 1996. http://eprints.maths.ox.ac.uk/157/1/heilbron.pdf

[KR] W. Keller and J. Richstein, *Solutions of the congruence* $a^{p-1} \equiv 1 \pmod{p^r}$, Math. Comp. **74** (2004), no. 250, 927–936.

[KR] W. Keller and J. Richstein, *The continuing search for Wieferich primes*, Math. Comp. **75** (2005), no. 251, 1559–1563.

[Mo] P. Moree, *Artin's Primitive Root Conjecture - A Survey*, In: The John Selfridge Memorial Volume, Integers **12** (2012), no. 6, 1305–1416.

[OS] A. Ostafe and I.E. Shparlinski, *Pseudorandomness and Dynamics of Fermat Quotients*, SIAM J. Discrete Math. **25** (2011), no. 1, 50–71.

[P] K. Belabas and al., *Pari/gp, Version 2.5.3*, Laboratoire A2X, Université de Bordeaux I. http://sagemath.org/

[Si] J.H. Silverman, *Wieferich's criterion and the abc-conjecture*, Journal of Number Theory **30** (1988), 226–237.

[Sh] I.E. Shparlinski, *On Vanishing Fermat Quotients and a Bound of the Ihara Sum*, Kodai Math. J. **36** (2013), no. 1, 99–108.

[T1] G. Tenenbaum, *Introduction à la théorie analytique et probabiliste des nombres*, 3^e édition revue et augmentée, Coll. Échelles, Belin 2008.

[T2] G. Tenenbaum, *Divergence d'une série liée aux nombres premiers.* https://www.researchgate.net/ publication/263200414

[W] M. Waldschmidt, *Lecture on the abc conjecture and some of its consequences*, Abdus Salam School of Mathematical Sciences (ASSMS), Lahore 6th World Conference on 21st Century Mathematics (2013). http://www.math.jussieu.fr/~miw/articles/pdf/abcLahore2013VI.pdf

[Wa] L.C. Washington, *Introduction to cyclotomic fields*, Graduate Texts in Math. 83, Springer enlarged second edition 1997.

Address: Georges Gras: Villa la Gardette, Chemin Château Gagnière, F–38520 Le Bourg d'Oisans, France.

E-mail: g.mn.gras@wanadoo.fr

Received: 19 November 2014; **revised:** 11 September 2015

INFORMATION FOR AUTHORS

Functiones et Approximatio Commentarii Mathematici publishes original papers in mathematics with special attention to analysis (in a broad sense) and number theory. Submission of a manuscript implies that the work has not been published before (except in the form of an abstract), that it is not under consideration for publication elsewhere, and that it will not be submitted elsewhere unless it has been rejected by the editors of Functiones et Approximatio. On the proof stage, the author will be asked to transfer copyright of the article to the publisher.

Manuscripts should be submitted electronically, preferably by sending a PDF file to fa@amu.edu.pl. Sending two hard copies is also possible, but electronic submission is preferred. On acceptance of the paper the authors will be also asked to transmit the TEX source file. The authors affiliation should be given at the end of the manuscript.

An abstract of not more than 200 words, 2010 Mathematical Subject Classification and key words are required.

References should be arranged in alphabetical order and labeled with numbers. The theorems, lemmas, ect. should be numbered consecutively within sections. The formulas must be numbered in similar but independent way. Figures must be arranged in a form suitable for direct reproducing, EPS (min. 1200 dpi) files are preferred. The use of very thin lines should be avoided.

The corresponding author may request 25 free offprints or the final PDF file of the article when sending the proof corrections.

Publikacja sfinansowana przez Wydział Matematyki i Informatyki UAM

Redaktor techniczny: Elżbieta Rygielska

Łamanie komputerowe: Łukasz Pańkowski

ISBN 978-83-232-3014-4
ISSN 0208-6573

WYDAWNICTWO NAUKOWE UNIWERSYTETU IM. ADAMA MICKIEWICZA W POZNANIU
61-701 POZNAŃ, UL. FREDRY 10
www.press.amu.edu.pl
Sekretariat: tel. 61 829 46 46, faks 61 829 46 47, e-mail: wydnauk@amu.edu.pl
Dział sprzedaży: tel. 61 829 46 40, e-mail: press@amu.edu.pl

Ark. wyd. 11,00. Ark. druk. 8,875.

DRUK I OPRAWA: EXPOL, WŁOCŁAWEK, UL. BRZESKA 4

ISBN 978-83-232-3014-4
ISSN 0208-6573