

ROOTS OF UNITY AND NULLITY MODULO n

STEVEN FINCH, GREG MARTIN, AND PASCAL SEBAH

ABSTRACT. For a fixed positive integer ℓ , we consider the function of n that counts the number of elements of order ℓ in \mathbb{Z}_n^* . We show that the average growth rate of this function is $C_\ell(\log n)^{d(\ell)-1}$ for an explicitly given constant C_ℓ , where $d(\ell)$ is the number of divisors of ℓ . From this we conclude that the average growth rate of the number of primitive Dirichlet characters modulo n of order ℓ is $(d(\ell) - 1)C_\ell(\log n)^{d(\ell)-2}$ for $\ell \geq 2$. We also consider the number of elements of \mathbb{Z}_n whose ℓ th power equals 0, showing that its average growth rate is $D_\ell(\log n)^{\ell-1}$ for another explicit constant D_ℓ . Two techniques for evaluating sums of multiplicative functions, the Wirsing–Odoni and Selberg–Delange methods, are illustrated by the proofs of these results.

Let \mathbb{Z}_n^* denote the group (under multiplication modulo n) of integers relatively prime to n , and let ℓ denote a fixed positive integer. Define $a_\ell(n)$ to be the number of solutions of $x^\ell = 1$ in \mathbb{Z}_n^* . The value of $a_\ell(p)$, when p is prime, ranges over all divisors of ℓ ; however, $a_\ell(n)$ can be much larger than ℓ if n is composite. It is therefore interesting to ask how the function $a_\ell(n)$ behaves on average over n . We can ask the same about $\tilde{a}_\ell(n)$, which we let denote the number of solutions of $x^\ell = 1$ in \mathbb{Z}_n^* for which $x^m \neq 1$ for all $1 \leq m < \ell$: such an x is said to be of order ℓ in the group \mathbb{Z}_n^* . In other words, a_ℓ counts the ℓ th roots of unity modulo n , while \tilde{a}_ℓ counts the primitive ℓ th roots of unity modulo n .

The following theorem, which is proved in Section 2, gives the average rate of growth for both functions a_ℓ and \tilde{a}_ℓ for every positive integer ℓ . In the statement of the theorem, we employ the usual notation $p^j \parallel n$ to mean that $p^j \mid n$ but $p^{j+1} \nmid n$; we also use $d(\ell)$ to denote the number of divisors of ℓ .

Theorem 1. *For any positive integer ℓ and for any real number $\varepsilon > 0$,*

$$\sum_{n < N} a_\ell(n) = C_\ell N (\log N)^{d(\ell)-1} + O_{\ell, \varepsilon} (N (\log N)^{d(\ell)-2+\varepsilon}) \quad (1)$$

as $N \rightarrow \infty$. Furthermore, the same asymptotic formula holds for $\sum_{n < N} \tilde{a}_\ell(n)$. Here, the constant C_ℓ is given by the convergent (hence positive) product

$$C_\ell = \frac{\theta(\ell)}{(d(\ell) - 1)!} \prod_p \left(1 + \frac{(\ell, p-1)}{p-1} \right) \left(1 - \frac{1}{p} \right)^{d(\ell)}, \quad (2)$$

where $\theta(\ell)$ is defined as follows: if $\ell = 2^i \ell_0$ with ℓ_0 odd, then

$$\theta(\ell) = \left\{ \begin{array}{ll} 1, & \text{if } i = 0, \\ (i+5)/4, & \text{if } i \geq 1 \end{array} \right\} \prod_{p^j \parallel \ell_0} \left(1 + \frac{j(\ell, p-1)(p-1)}{p(p + (\ell, p-1) - 1)} \right). \quad (3)$$

Shanks [15, page 62] wrote, “... the whole subject of finite group theory may be thought of as a generalization of the theory of the roots of unity.” It is consequently surprising that no asymptotic study of $\sum_{n < N} a_\ell(n)$ or $\sum_{n < N} \tilde{a}_\ell(n)$, for general ℓ , seems to exist in the literature. Some other

relevant asymptotics, involving the average multiplicative order of elements of \mathbb{Z}_n^* as a function of n , were found recently by Luca and Shparlinksi [7] using different techniques.

Special cases of this result for $\ell = 2, 3, 4$ were examined in [3]. Leading coefficients are known to be the easily recognized $C_1 = 1$ and $C_2 = 6/\pi^2$, and the more complicated

$$C_3 = \frac{11}{6\pi\sqrt{3}} \prod_{p \equiv 1 \pmod{3}} \left(1 - \frac{2}{p(p+1)}\right) = 0.3170565167922841205670156 \dots \quad (4)$$

and

$$C_4 = \frac{7}{2\pi^3} \prod_{p \equiv 1 \pmod{4}} \left(1 - \frac{4}{(p+1)^2}\right) = 0.0954383605842642240056118 \dots \quad (5)$$

The expression (4) for C_3 is not new but was obtained earlier in [2] and [4]; a detailed exposition of the high-precision calculation of C_3 appears in [4]. We derive the expressions (4) and (5), as well as a similar expression (12) for C_6 , in Section 3.

Because the character group of a finite abelian group is isomorphic to the group itself, the function $a_\ell(n)$ also counts the number of Dirichlet characters $\chi \pmod{n}$ such that χ^ℓ equals the principal character χ_0 , while $\tilde{a}_\ell(n)$ counts the number of Dirichlet characters \pmod{n} of order ℓ . Therefore Theorem 1 is also a statement about the number of Dirichlet characters of order ℓ on average.

One might also be interested in studying $b_\ell(n)$, denoting the number of *primitive* Dirichlet characters $\chi \pmod{n}$ such that $\chi^\ell = \chi_0$, and the related function $\tilde{b}_\ell(n)$, denoting the number of *primitive* Dirichlet characters \pmod{n} of order ℓ . The following theorem, also proved in Section 2, gives the average growth rate of these functions.

Theorem 2. *For any integer $\ell \geq 2$ and for any real number $\varepsilon > 0$,*

$$\sum_{n < N} b_\ell(n) = (d(\ell) - 1)C_\ell N (\log N)^{d(\ell)-2} + O_{\ell,\varepsilon}(N(\log N)^{d(\ell)-3+\varepsilon}) \quad (6)$$

as $N \rightarrow \infty$, where C_ℓ is the constant defined in equation (2). Furthermore, the same asymptotic formula holds for $\sum_{n < N} \tilde{b}_\ell(n)$.

Let \mathbb{Z}_n denote the ring of integers modulo n . This is not a group under multiplication; nevertheless we can still define $\alpha_\ell(n)$ to be the number of solutions of $x^\ell = 0$ in \mathbb{Z}_n . Define also $\tilde{\alpha}_\ell(n)$ to be the number of solutions of $x^\ell = 0$ in \mathbb{Z}_n for which $x^m \neq 0$ for all $1 \leq m < \ell$. We can establish the average rates of growth of these functions as well, extending earlier work [4] that addressed the cases $\ell = 2$ and $\ell = 3$.

Theorem 3. *For any positive integer ℓ ,*

$$\sum_{n < N} \alpha_\ell(n) = D_\ell N (\log N)^{\ell-1} + O_\ell(N(\log N)^{\ell-2})$$

as $N \rightarrow \infty$. Furthermore, the same asymptotic formula holds for $\sum_{n < N} \tilde{\alpha}_\ell(n)$. Here, the constant D_ℓ is given by the convergent (hence positive) product

$$D_\ell = \frac{1}{\ell!(\ell-1)!} \prod_p \left(1 + \frac{\ell-1}{p}\right) \left(1 - \frac{1}{p}\right)^{\ell-1}. \quad (7)$$

The exact values $D_1 = 1$ and $D_2 = 3/\pi^2$ are easy to read off from the definition; we compare other values of D_ℓ to the values of C_ℓ after the proof of the theorem in Section 4.

As it turns out, the proof of Theorem 3 employs the Selberg–Delange method [17], while the more restrictive Wirsing–Odoni method [16] is sufficient for proving Theorem 1. In this sense, studying roots of unity is less difficult than studying roots of nullity. In the next section we describe these two methods precisely, in the context of this paper.

1. TWO ASYMPTOTIC METHODS

The proofs of our theorems use two different known methods of asymptotically evaluating sums of nonnegative multiplicative functions $f(n)$. The first, the “Wirsing–Odoni Method”, is elementary (in the technical sense of avoiding complex analysis) but requires an asymptotic formula for $\sum_{p < P} f(p)$, as well as a growth condition on the values $f(p^r)$ at prime powers. The second, the “Selberg–Delange Method”, applies in principle to any nonnegative multiplicative function but requires some analytic continuation of the associated Dirichlet series $\sum_{n=1}^{\infty} f(n)n^{-s}$, a condition that can be difficult to confirm in practice (see [9] for example).

The first result that we cite was given, in essentially this form, by Spearman and Williams [16], using what Odoni [11, 12] called “Halberstam’s refinement of Wirsing’s method”. An alternative approach might employ Moree and Cazanar’s reinterpretation [9] of the Levin–Fainleib procedure [6].

Proposition 4 (Wirsing–Odoni Method). *Let f be a multiplicative function. Suppose that there exist constants u and v such that $0 \leq f(p^r) \leq ur^v$ for all primes p and all positive integers r . Suppose also that there exist real numbers $\xi > 0$ and $0 < \beta < 1$ such that*

$$\sum_{p < P} f(p) = \xi \frac{P}{\log P} + O\left(\frac{P}{(\log P)^{1+\beta}}\right)$$

as $P \rightarrow \infty$. Then the product over all primes

$$C_f = \frac{1}{\Gamma(\xi)} \prod_p \left(1 + \frac{f(p)}{p} + \frac{f(p^2)}{p^2} + \frac{f(p^3)}{p^3} + \dots\right) \left(1 - \frac{1}{p}\right)^\xi$$

converges (hence is positive), and

$$\sum_{n < N} f(n) = C_f N (\log N)^{\xi-1} + O_f(N (\log N)^{\xi-1-\beta})$$

as $N \rightarrow \infty$.

This statement differs from [16, Proposition 5.5] in only two respects. First, their statement has the more restrictive hypothesis that $f(n) \leq 1$ for all n ; however, the two prior propositions in their paper, from which they directly derive Proposition 5.5, allow the weaker hypothesis $f(p^r) \leq ur^v$. Second, they give the value of C_f as

$$C_f = \frac{e^{-\gamma\xi}}{\Gamma(\xi)} \lim_{P \rightarrow \infty} \frac{1}{(\log P)^\xi} \prod_{p < P} \left(1 + \frac{f(p)}{p} + \frac{f(p^2)}{p^2} + \frac{f(p^3)}{p^3} + \dots\right).$$

However, Mertens’ formula (see [8, Theorem 2.7(e)]) tells us that

$$\lim_{P \rightarrow \infty} e^\gamma \log P \prod_{p < P} \left(1 - \frac{1}{p}\right) = 1,$$

which allows us to convert the expression for C_f into

$$C_f = \frac{1}{\Gamma(\xi)} \lim_{P \rightarrow \infty} \prod_{p < P} \left(1 + \frac{f(p)}{p} + \frac{f(p^2)}{p^2} + \frac{f(p^3)}{p^3} + \dots \right) \left(1 - \frac{1}{p} \right)^\xi;$$

therefore the product on the right-hand side converges, since C_f is known to exist and be positive. This discussion shows that Proposition 4 does indeed follow from the work of Spearman and Williams.

The second result that we cite is a variant of the Selberg–Delange Method as described by Tenenbaum [17], which involves factoring out powers of the Riemann zeta-function $\zeta(s)$ to cancel a (possibly high-order) pole of a Dirichlet series at $s = 1$. We have found it useful (and believe others might as well) to phrase this result in a seemingly more general way, where we allow the extraction of factors of the form $\zeta(\rho_j s - (\rho_j - 1))$ rather than just $\zeta(s)$. We show in Section 5, however, that our statement does in fact follow from the form of the Selberg–Delange Method given in [17].

Proposition 5 (Selberg-Delange Method). *Let f be a nonnegative multiplicative function, and define $F(s) = \sum_{n=1}^{\infty} f(n)n^{-s}$. Let κ be a positive integer, and assume that there exist positive integers $\rho_1, \rho_2, \dots, \rho_\kappa$ and positive real numbers $z_1, z_2, \dots, z_\kappa$ such that the Dirichlet series*

$$H(s) = F(s) \left(\prod_{j=1}^{\kappa} \zeta(\rho_j s - (\rho_j - 1))^{z_j} \right)^{-1} = \sum_{n=1}^{\infty} h(n)n^{-s}$$

converges absolutely on some right half-plane $\Re(s) > c$, where $c < 1$. Then

$$D_f = \frac{H(1)}{\Gamma(\xi) \prod_{j=1}^{\kappa} \rho_j^{z_j}} = \frac{1}{\Gamma(\xi) \prod_{j=1}^{\kappa} \rho_j^{z_j}} \prod_p \left(1 + \frac{h(p)}{p} + \frac{h(p^2)}{p^2} + \frac{h(p^3)}{p^3} + \dots \right)$$

converges to a positive real number, where $\xi = \sum_{j=1}^{\kappa} z_j$. Furthermore,

$$\sum_{n < N} f(n) = D_f N (\log N)^{\xi-1} + O_f(N (\log N)^{\xi-2})$$

as $N \rightarrow \infty$.

2. PROOF OF THEOREM 1

The number $a_\ell(n)$ of solutions of $x^\ell = 1$ in \mathbb{Z}_n^* is a multiplicative function of n by the Chinese remainder theorem. We start by recording a formula for $a_\ell(n)$ when n is a prime power. The following lemma contains well-known results in elementary number theory: for instance, it is a special case of [10, Corollaries 2.42 and 2.44].

Lemma 6. *Let ℓ be a positive integer.*

- (a) *Let p be an odd prime, and let $j \geq 0$ be the integer such that $p^j \parallel \ell$. For any $r \geq 1$, we have $a_\ell(p^r) = p^{\min\{j, r-1\}}(\ell, p-1)$.*
- (b) *We always have $a_\ell(2) = 1$, and if ℓ is odd then $a_\ell(2^r) = 1$ for any positive integer r . If ℓ is even, then let $j \geq 1$ be the integer such that $2^j \parallel \ell$; in this case, we have $a_\ell(2^r) = 2^{\min\{j+1, r-1\}}$ for any $r \geq 2$.*

Armed with this information, we can determine the average value of a_ℓ on primes.

Lemma 7. *We have $\sum_{p < P} a_\ell(p) = d(\ell)P / \log P + O_\ell(P / (\log P)^2)$ as $P \rightarrow \infty$.*

Proof. We use the prime number theorem for arithmetic progressions in the form

$$\#\{p < P : p \equiv k \pmod{\ell}\} = \frac{P}{\phi(\ell) \log P} + O_\ell\left(\frac{P}{(\log P)^2}\right)$$

for any k that is relatively prime to ℓ , where $\phi(\ell) = \#\mathbb{Z}_\ell^*$ is the Euler phi-function; since ℓ is fixed, this statement follows easily from the classical Siegel–Walfisz theorem (see [8, Corollary 11.21]).

By Lemma 6, we know that $a_\ell(p) = (\ell, p-1) = (\ell, k-1)$ if $p \equiv k \pmod{\ell}$; therefore

$$\begin{aligned} \sum_{p < P} a_\ell(p) &= \sum_{\substack{1 \leq k \leq \ell \\ (k, \ell) = 1}} (\ell, k-1) \sum_{\substack{p < P \\ p \equiv k \pmod{\ell}}} 1 + O_\ell(1) \\ &= \frac{P}{\phi(\ell) \log P} \sum_{\substack{1 \leq k \leq \ell \\ (k, \ell) = 1}} (\ell, k-1) + O_\ell\left(\frac{P}{(\log P)^2}\right). \end{aligned}$$

The remaining sum is known ([10, problem 4.2.25]; see also [13, page 21]) to equal

$$\sum_{\substack{1 \leq k \leq \ell \\ (k, \ell) = 1}} (\ell, k-1) = \phi(\ell) d(\ell),$$

which establishes the lemma. \square

There is another approach to proving the fact that the function a_ℓ has $d(\ell)$ as its average value on primes, which, while not shorter or simpler, might be illuminating. The polynomial $x^\ell - 1$ is the product of $d(\ell)$ distinct irreducible (over the integers) polynomials, namely the cyclotomic polynomials $\Phi_k(x)$ for k dividing ℓ . Each such irreducible factor has one zero on average over primes, by the prime ideal theorem of Landau (see for example [5, page 67, equation (3.3)]); moreover, two distinct irreducible polynomials have a common root $(\bmod p)$ for only finitely many primes p (namely those dividing their resultant). Consequently, $x^\ell - 1$ has $d(\ell)$ zeros on average over primes.

Proof of Theorem 1. We apply the Wirsing–Odoni method to the multiplicative function $f(n) = a_\ell(n)$. Note that Lemma 6 implies that $a_\ell(p^r) \leq \ell^2$ for any prime power p^r . Together with Lemma 7, this shows that the hypotheses of Proposition 4 are satisfied with $u = \ell^2$ and $v = 0$, and $\xi = d(\ell)$ and $\beta = 1 - \varepsilon$ for any $\varepsilon > 0$. We conclude from Proposition 4 that

$$\sum_{n < N} a_\ell(n) = C_\ell N (\log N)^{d(\ell)-1} + O_{\ell, \varepsilon}(N (\log N)^{d(\ell)-2+\varepsilon}),$$

where

$$C_\ell = \frac{1}{\Gamma(d(\ell))} \prod_p \left(1 + \frac{a_\ell(p)}{p} + \frac{a_\ell(p^2)}{p^2} + \dots\right) \left(1 - \frac{1}{p}\right)^{d(\ell)}. \quad (8)$$

By Lemma 6, we see that $a_\ell(p^r) = (\ell, p-1)$ for all $r \geq 1$ whenever $p \nmid \ell$; for such primes, we have

$$1 + \frac{a_\ell(p)}{p} + \frac{a_\ell(p^2)}{p^2} + \dots = 1 + (\ell, p-1) \left(\frac{1}{p} + \frac{1}{p^2} + \dots\right) = 1 + \frac{(\ell, p-1)}{p-1}.$$

Therefore we write equation (8) as

$$C_\ell = \frac{\theta(\ell)}{\Gamma(d(\ell))} \prod_p \left(1 + \frac{(\ell, p-1)}{p-1}\right) \left(1 - \frac{1}{p}\right)^{d(\ell)},$$

where we have set

$$\theta(\ell) = \prod_{p|\ell} \left(1 + \frac{(\ell, p-1)}{p-1}\right)^{-1} \left(1 + \frac{a_\ell(p)}{p} + \frac{a_\ell(p^2)}{p^2} + \dots\right). \quad (9)$$

All that remains is to show that this expression for $\theta(\ell)$ is equal to the definition (3). For any odd prime p dividing ℓ , let $j \geq 1$ be the integer such that $p^j \parallel \ell$. Lemma 6(a) tells us that

$$\begin{aligned} 1 + \frac{a_\ell(p)}{p} + \frac{a_\ell(p^2)}{p^2} + \dots &= 1 + \left(\frac{(\ell, p-1)}{p} + \frac{p(\ell, p-1)}{p^2} + \dots + \frac{p^{j-1}(\ell, p-1)}{p^j}\right) \\ &\quad + \left(\frac{p^j(\ell, p-1)}{p^{j+1}} + \frac{p^j(\ell, p-1)}{p^{j+2}} + \dots\right) \\ &= 1 + (\ell, p-1) \left(\frac{j}{p} + \frac{1}{p-1}\right), \end{aligned}$$

whence

$$\left(1 + \frac{(\ell, p-1)}{p-1}\right)^{-1} \left(1 + (\ell, p-1) \left(\frac{j}{p} + \frac{1}{p-1}\right)\right) = 1 + \frac{j(\ell, p-1)(p-1)}{p(p + (\ell, p-1) - 1)}. \quad (10)$$

Similarly, if ℓ is even, then let $i \geq 1$ be the integer such that $2^i \parallel \ell$. Lemma 6(b) tells us that

$$1 + \frac{a_\ell(2)}{2} + \frac{a_\ell(2^2)}{2^2} + \dots = 1 + \left(\frac{1}{2} + \frac{2}{2^2} + \dots + \frac{2^i}{2^{i+1}}\right) + \left(\frac{2^{i+1}}{2^{i+2}} + \frac{2^{i+1}}{2^{i+3}} + \dots\right) = 1 + \frac{i+1}{2} + 1,$$

whence $(1 + 1/2)^{-1}(i+3)/2 = (i+5)/4$. Together with equation (10), this shows that the two expressions (3) and (9) for $\theta(\ell)$ are equivalent.

We have completed the proof of the asymptotic formula (1) for $\sum_{n < N} a_\ell(n)$, and we now establish the same asymptotic formula for $\sum_{n < N} \tilde{a}_\ell(n)$. Every ℓ th root of unity modulo n is a primitive k th root of unity modulo n for exactly one integer k dividing ℓ ; therefore for any fixed n ,

$$a_\ell(n) = \sum_{k|\ell} \tilde{a}_k(n).$$

The Möbius inversion formula [10, Theorem 4.8] thus yields

$$\tilde{a}_\ell(n) = \sum_{k|\ell} \mu\left(\frac{\ell}{k}\right) a_k(n),$$

where μ denotes the Möbius mu-function. We conclude that

$$\begin{aligned} \sum_{n < N} \tilde{a}_\ell(n) &= \sum_{n < N} \sum_{k|\ell} \mu\left(\frac{\ell}{k}\right) a_k(n) = \sum_{n < N} a_\ell(n) + O\left(\sum_{\substack{k|\ell \\ k < \ell}} \left|\mu\left(\frac{\ell}{k}\right)\right| \sum_{n < N} a_k(n)\right) \\ &= \sum_{n < N} a_\ell(n) + O_\ell\left(\sum_{\substack{k|\ell \\ k < \ell}} N(\log N)^{d(k)-1}\right), \end{aligned}$$

by the already established asymptotic formula (1). Since $d(k) \leq d(\ell) - 1$ for any proper divisor k of ℓ , we see that this last error term has order of magnitude at most $N(\log N)^{d(\ell)-2}$, which shows that the asymptotic formula (1) also holds for $\sum_{n < N} \tilde{a}_\ell(n)$ as asserted. \square

Proof of Theorem 2. As mentioned earlier, $a_\ell(n)$ is the number of Dirichlet characters $\chi \pmod{n}$ such that $\chi^\ell = \chi_0$. Since every Dirichlet character is induced by exactly one primitive character whose modulus divides n , we see that $a_\ell(n) = \sum_{d|n} b_\ell(d)$. From this identity we can recover all values of b_ℓ by the Möbius inversion formula, but for the purposes of this proof we need only note that $b_\ell(p^r) = a_\ell(p^r) - a_\ell(p^{r-1})$ for every prime power p^r . An examination of Lemma 6 shows that $0 \leq b_\ell(p^r) \leq \ell^2$; furthermore, it follows directly from Lemma 7 that

$$\sum_{p < P} b_\ell(p) = \sum_{p < P} (a_\ell(p) - a_\ell(1)) = \sum_{p < P} a_\ell(p) - \pi(P) = \frac{(d(\ell) - 1)P}{\log P} + O_\ell\left(\frac{P}{(\log P)^2}\right).$$

Here we use the assumption that $\ell \geq 2$, so that $d(\ell) - 1 > 0$: we conclude from Proposition 4 that

$$\sum_{n < N} b_\ell(n) = E_\ell N (\log N)^{d(\ell)-2} + O_{\ell, \varepsilon}(N (\log N)^{d(\ell)-3+\varepsilon}),$$

where

$$E_\ell = \frac{1}{\Gamma(d(\ell) - 1)} \prod_p \left(1 + \frac{b_\ell(p)}{p} + \frac{b_\ell(p^2)}{p^2} + \frac{b_\ell(p^3)}{p^3} + \dots\right) \left(1 - \frac{1}{p}\right)^{d(\ell)-1}.$$

Note, however, that

$$\left(1 + \frac{a_\ell(p)}{p} + \frac{a_\ell(p^2)}{p^2} + \frac{a_\ell(p^3)}{p^3} + \dots\right) \left(1 - \frac{1}{p}\right) = \left(1 + \frac{b_\ell(p)}{p} + \frac{b_\ell(p^2)}{p^2} + \frac{b_\ell(p^3)}{p^3} + \dots\right);$$

therefore

$$E_\ell = \frac{d(\ell) - 1}{\Gamma(d(\ell))} \prod_p \left(1 + \frac{a_\ell(p)}{p} + \frac{a_\ell(p^2)}{p^2} + \frac{a_\ell(p^3)}{p^3} + \dots\right) \left(1 - \frac{1}{p}\right)^{d(\ell)} = (d(\ell) - 1)C_\ell$$

from equation (8). This establishes the first assertion of Theorem 2, and the second assertion follows from the first exactly as the second assertion of Theorem 1 follows from its first assertion, in light of the identity $b_\ell(n) = \sum_{d|n} \tilde{b}_\ell(d)$. \square

3. BETTER CONVERGENCE FOR CERTAIN C_ℓ

The infinite product in the definition (2) of C_ℓ does not converge very quickly: assuming the generalized Riemann hypothesis, the truncation of the product at P is within roughly $P^{-1/2}$ of the limiting value. In principle, one can extract appropriate powers of $L(1, \chi)$, for χ ranging over the nonprincipal Dirichlet characters $\pmod{\ell}$, to leave a product that converges more quickly. For most ℓ the resulting expressions are quite unwieldy; however, when $\phi(\ell) = 2$, we can obtain rather tidy forms.

We thus assume for the rest of this section that $\ell = 3, 4$, or 6 , and we let χ_0 and χ_1 denote the principal and nonprincipal characters $\pmod{\ell}$, respectively. We also, for the sake of exposition, separate infinite products into two parts even when the products do not individually converge. For

example, for the values of ℓ under consideration, equation (2) can be rewritten as

$$C_\ell = \frac{\theta(\ell)}{(d(\ell) - 1)!} \prod_{p|\ell} \left(1 + \frac{(\ell, p-1)}{p-1}\right) \left(1 - \frac{1}{p}\right)^{d(\ell)} \\ \times \lim_{P \rightarrow \infty} \prod_{\substack{p < P \\ p \equiv 1 \pmod{\ell}}} \left(1 + \frac{\ell}{p-1}\right) \left(1 - \frac{1}{p}\right)^{d(\ell)} \prod_{\substack{p < P \\ p \equiv -1 \pmod{\ell}}} \left(1 + \frac{(\ell, 2)}{p-1}\right) \left(1 - \frac{1}{p}\right)^{d(\ell)} ;$$

we abuse notation by writing simply

$$C_\ell = \frac{\theta(\ell)}{(d(\ell) - 1)!} \prod_{p|\ell} \left(1 + \frac{(\ell, p-1)}{p-1}\right) \left(1 - \frac{1}{p}\right)^{d(\ell)} \\ \times \prod_{p \equiv 1 \pmod{\ell}} \left(1 + \frac{\ell}{p-1}\right) \left(1 - \frac{1}{p}\right)^{d(\ell)} \prod_{p \equiv -1 \pmod{\ell}} \left(1 + \frac{(\ell, 2)}{p-1}\right) \left(1 - \frac{1}{p}\right)^{d(\ell)}. \quad (11)$$

The idea is to use an appropriate combination of

$$L(1, \chi_1) = \prod_{p \equiv 1 \pmod{\ell}} \left(1 - \frac{1}{p}\right)^{-1} \prod_{p \equiv -1 \pmod{\ell}} \left(1 + \frac{1}{p}\right)^{-1}$$

and

$$L(2, \chi_0) = \prod_{p \equiv 1 \pmod{\ell}} \left(1 - \frac{1}{p^2}\right)^{-1} \prod_{p \equiv -1 \pmod{\ell}} \left(1 - \frac{1}{p^2}\right)^{-1}$$

to completely cancel the last product in equation (11); the resulting product over primes congruent to 1 (mod ℓ) will turn out to converge more quickly as well. The exact value of $L(1, \chi_1)$ can be calculated by classical formulas [8, page 134], as can the value $L(2, \chi_0) = \frac{\pi^2}{6} \prod_{p|\ell} (1 - p^{-2})$.

For example, when $\ell = 3$, we can rewrite equation (11) (recalling the definition (3) of $\theta(\ell)$) as

$$\frac{L(2, \chi_0)}{L(1, \chi_1)} C_3 = \frac{11/9}{(2-1)!} \left(1 + \frac{1}{3-1}\right) \left(1 - \frac{1}{3}\right)^2 \\ \times \prod_{p \equiv 1 \pmod{3}} \left(1 - \frac{1}{p^2}\right)^{-1} \left(1 - \frac{1}{p}\right) \cdot \left(1 + \frac{3}{p-1}\right) \left(1 - \frac{1}{p}\right)^2 \\ \times \prod_{p \equiv -1 \pmod{3}} \left(1 - \frac{1}{p^2}\right)^{-1} \left(1 + \frac{1}{p}\right) \cdot \left(1 + \frac{1}{p-1}\right) \left(1 - \frac{1}{p}\right)^2 \\ = \frac{22}{27} \prod_{p \equiv 1 \pmod{3}} \left(1 - \frac{2}{p(p+1)}\right);$$

since $L(1, \chi_1) = \pi/(3\sqrt{3})$ and $L(2, \chi_0) = 4\pi^2/27$, we recover the expression (4) for C_3 .

When $\ell = 4$, we rewrite equation (11) as

$$\begin{aligned} \frac{L(2, \chi_0)^2}{L(1, \chi_1)} C_4 &= \frac{7/4}{(3-1)!} \left(1 + \frac{1}{2-1}\right) \left(1 - \frac{1}{2}\right)^3 \\ &\quad \times \prod_{p \equiv 1 \pmod{4}} \left(1 - \frac{1}{p^2}\right)^{-2} \left(1 - \frac{1}{p}\right) \cdot \left(1 + \frac{4}{p-1}\right) \left(1 - \frac{1}{p}\right)^3 \\ &\quad \times \prod_{p \equiv -1 \pmod{4}} \left(1 - \frac{1}{p^2}\right)^{-2} \left(1 + \frac{1}{p}\right) \cdot \left(1 + \frac{2}{p-1}\right) \left(1 - \frac{1}{p}\right)^3 \\ &= \frac{7}{32} \prod_{p \equiv 1 \pmod{4}} \left(1 - \frac{4}{(p+1)^2}\right); \end{aligned}$$

since $L(1, \chi_1) = \pi/4$ and $L(2, \chi_0) = \pi^2/8$, we have established the expression (5) for C_4 .

Finally, when $\ell = 6$, we rewrite equation (11) as

$$\begin{aligned} \frac{L(2, \chi_0)^3}{L(1, \chi_1)^2} C_6 &= \frac{2}{(4-1)!} \left(1 + \frac{1}{2-1}\right) \left(1 - \frac{1}{2}\right)^4 \left(1 + \frac{2}{3-1}\right) \left(1 - \frac{1}{3}\right)^4 \\ &\quad \times \prod_{p \equiv 1 \pmod{6}} \left(1 - \frac{1}{p^2}\right)^{-3} \left(1 - \frac{1}{p}\right)^2 \cdot \left(1 + \frac{6}{p-1}\right) \left(1 - \frac{1}{p}\right)^4 \\ &\quad \times \prod_{p \equiv -1 \pmod{6}} \left(1 - \frac{1}{p^2}\right)^{-3} \left(1 + \frac{1}{p}\right)^2 \cdot \left(1 + \frac{2}{p-1}\right) \left(1 - \frac{1}{p}\right)^4 \\ &= \frac{4}{243} \prod_{p \equiv 1 \pmod{6}} \left(1 - \frac{12p-4}{(p+1)^3}\right); \end{aligned}$$

since $L(1, \chi_1) = \pi/(2\sqrt{3})$ and $L(2, \chi_0) = \pi^2/9$, we have established the expression

$$C_6 = \frac{1}{\pi^4} \prod_{p \equiv 1 \pmod{6}} \left(1 - \frac{12p-4}{(p+1)^3}\right) = 0.0075925601722787610308508 \dots \quad (12)$$

Notice that the expressions (4), (5), and (12) involve infinite products whose factors are of the form $1 + O(p^{-2})$. Consequently, each of these expressions converges more quickly than the original formula (2): their truncations at P will be within a factor of roughly $(P \log P)^{-1}$ of their limiting values.

4. PROOF OF THEOREM 3

We use the Selberg–Delange method to address the average growth rate of the number of roots of nullity (mod n). The key observation is that the Dirichlet series corresponding to $\alpha_\ell(n)$ can be factored into a product of copies of the Riemann zeta function, multiplied by a Dirichlet series with a half-plane of convergence that includes the point $s = 1$.

Proof of Theorem 3. The number $\alpha_\ell(n)$ of solutions of $x^\ell = 0$ in \mathbb{Z}_n is again a multiplicative function of n by the Chinese remainder theorem. It is easy to see that $\alpha_\ell(p^r) = p^{\lfloor (\ell-1)r/\ell \rfloor}$ for any prime power p^r ; put another way, if $r = j\ell$ then $\alpha_\ell(p^r) = p^{j(\ell-1)}$, while if $r = j\ell + i$ with

$1 \leq i \leq \ell - 1$ then $\alpha_\ell(p^r) = p^{j(\ell-1)+i-1}$. Therefore

$$\begin{aligned} \sum_{n=1}^{\infty} \frac{\alpha_\ell(n)}{n^s} &= \prod_p \left(\sum_{r=0}^{\infty} \frac{\alpha_\ell(p^r)}{p^{rs}} \right) = \prod_p \left(\sum_{j=0}^{\infty} \sum_{i=0}^{\ell-1} \frac{\alpha_\ell(p^{j\ell+i})}{p^{(j\ell+i)s}} \right) \\ &= \prod_p \left(1 + \sum_{i=1}^{\ell-1} \frac{p^{i-1}}{p^{is}} \right) \sum_{j=0}^{\infty} \left(\frac{p^{\ell-1}}{p^{\ell s}} \right)^j \\ &= \prod_p \left(1 + \frac{1}{p^s} + \frac{1}{p^{2s-1}} + \cdots + \frac{1}{p^{(\ell-1)s-(\ell-2)}} \right) \left(1 - \frac{1}{p^{\ell s-(\ell-1)}} \right)^{-1}. \end{aligned}$$

Define

$$H_\ell(s) = \prod_p \left(1 + \frac{1}{p^s} + \frac{1}{p^{2s-1}} + \cdots + \frac{1}{p^{(\ell-1)s-(\ell-2)}} \right) \left(1 - \frac{1}{p^s} \right) \left(1 - \frac{1}{p^{2s-1}} \right) \cdots \left(1 - \frac{1}{p^{(\ell-1)s-(\ell-2)}} \right), \quad (13)$$

so that

$$\sum_{n=1}^{\infty} \frac{\alpha_\ell(n)}{n^s} = \zeta(s)\zeta(2s-1) \cdots \zeta(\ell s - (\ell-1)) H_\ell(s).$$

Notice that when each factor in the Euler product (13) defining $H_\ell(s)$ is expanded, every uncancelled term other than 1 is bounded by $1/p^{2(\ell-1)\sigma-2(\ell-2)}$ when $\sigma = \Re(s) \leq 1$. Since the exponent $2(\ell-1)\sigma - 2(\ell-2)$ exceeds 1 for $\sigma > (2\ell-3)/(2\ell-2)$, we conclude that the Euler product (13) converges uniformly on any compact subset of the half-plane $\Re(s) > (2\ell-3)/(2\ell-2)$, as will the corresponding Dirichlet series. Therefore the Selberg–Delange can be applied: we take $\kappa = \ell$, $\rho_j = j$, $z_j = 1$, and any $c > (2\ell-3)/(2\ell-2)$ in Proposition 5, obtaining

$$\sum_{n < N} \alpha_\ell(n) = D_\ell N (\log N)^{\ell-1} + O_\ell(N (\log N)^{\ell-2})$$

with

$$D_\ell = \frac{H_\ell(1)}{\Gamma(\ell) \prod_{j=1}^{\ell} j} = \frac{1}{(\ell-1)! \ell!} \prod_p \left(1 + \frac{\ell-1}{p} \right) \left(1 - \frac{1}{p} \right)^{\ell-1},$$

which establishes the first assertion of the theorem.

When $\ell = 1$, we trivially have $\tilde{\alpha}_1(n) = \alpha_1(n)$ for all positive integers n , so the second assertion of the theorem is equivalent to the first assertion in that case; we therefore assume $\ell \geq 2$. Since $\tilde{\alpha}_\ell(n)$ counts the number of solutions to $x^\ell \equiv 0 \pmod{n}$ that are not solutions to $x^{\ell-1} \equiv 0 \pmod{n}$, we have $\tilde{\alpha}_\ell(n) = \alpha_\ell(n) - \alpha_{\ell-1}(n)$; this implies that

$$\sum_{n < N} \tilde{\alpha}_\ell(n) = \sum_{n < N} \alpha_\ell(n) - \sum_{n < N} \alpha_{\ell-1}(n) = \sum_{n < N} \alpha_\ell(n) + O_\ell(N (\log N)^{\ell-2})$$

by an application of the first assertion of the theorem at $\ell - 1$. This establishes the second assertion of the theorem. \square

We remark that the function

$$\prod_p \left(1 + \frac{1}{p^s} + \frac{1}{p^{2s-1}} \right) = \frac{1}{\zeta(3s-2)} \sum_{n=1}^{\infty} \frac{\alpha_3(n)}{n^s} = \zeta(s)\zeta(2s-1)H_3(s),$$

in the notation of the above proof, appears also in [14] and [1], where the difficulty of determining the natural boundary of its meromorphic continuation is noted.

Notice that the definition (7) of D_ℓ is a reasonably quickly converging infinite product: the general factor is a polynomial in $1/p$ with no linear term, and so the product has the form $\prod_p(1 + O(p^{-2}))$. For example,

$$D_3 = \frac{1}{12} \prod_p \left(1 - \frac{3p-2}{p^3}\right) \quad \text{and} \quad D_4 = \frac{1}{144} \prod_p \left(1 - \frac{6p^2 - 8p + 3}{p^4}\right).$$

While these expressions are already serviceable for numerical calculations, we wish to record an interesting parallel with the constants C_ℓ defined in equation (2). Notice that

$$\left(1 + \frac{\ell-1}{p}\right) \left(1 - \frac{1}{p}\right)^{\ell-1} = \left(1 + \frac{\ell}{p-1}\right) \left(1 - \frac{1}{p}\right)^\ell,$$

which means that the general factor in the definition of D_ℓ is the same as the factor in the definition of C_ℓ corresponding to primes $p \equiv 1 \pmod{\ell}$. For example, if we take ℓ to be 3, 4, or 6 and extract appropriate powers of $\zeta(s)^{-1}$ from D_ℓ , we see that

$$\begin{aligned} D_3 &= \frac{1}{2\pi^2} \prod_p \left(1 - \frac{2}{p(p+1)}\right) \\ D_4 &= \frac{1}{4\pi^4} \prod_p \left(1 - \frac{4}{(p+1)^2}\right) \\ D_6 &= \frac{1}{400\pi^6} \prod_p \left(1 - \frac{12p-4}{(p+1)^3}\right); \end{aligned}$$

these expressions can be compared with the expressions (4), (5), and (12) for the respective C_ℓ .

5. VERIFICATION OF SELBERG–DELANGE

The following proposition is a consequence of the Selberg–Delange Method that is even more general than Proposition 5, in that we do not require the coefficients f_n to be multiplicative in n .

Proposition 8. *Let $F(s) = \sum_{n=1}^{\infty} f_n n^{-s}$ and $H(s) = \sum_{n=1}^{\infty} h_n n^{-s}$ be Dirichlet series, with $f_n \geq 0$. Suppose that there exists a positive integer κ , positive integers $\rho_1, \dots, \rho_\kappa$, and positive real numbers z_1, \dots, z_κ such that*

$$F(s) = H(s) \prod_{j=1}^{\kappa} \zeta(\rho_j s - (\rho_j - 1))^{z_j}$$

on some right half-plane. Suppose also that $\sum_{n=1}^{\infty} |h_n| n^{-\sigma_0}$ converges for some real number $\sigma_0 < 1$. Then

$$D_f = \frac{H(1)}{\Gamma(\xi) \prod_{j=1}^{\kappa} \rho_j^{z_j}} = \frac{\sum_{n=1}^{\infty} h_n/n}{\Gamma(\xi) \prod_{j=1}^{\kappa} \rho_j^{z_j}}.$$

is convergent, where $\xi = \sum_{j=1}^{\kappa} z_j$. Furthermore,

$$\sum_{n < N} f_n = D_f N (\log N)^{\xi-1} + O_f(N (\log N)^{\xi-2})$$

as $N \rightarrow \infty$.

We could allow the exponents z_j to be arbitrary complex numbers and still be able to derive the above proposition from the Selberg–Delange Method in [17], but at the cost of more technical details. (We note that our proof below goes through if all of the z_j have positive real parts.) In fact, we could even allow the coefficients f_n to be arbitrary complex numbers. We have chosen only to mention these extensions, since the resulting proof would have to be much longer, and because the given statement is sufficient for our purposes. The restriction that the ρ_j be positive integers is more fundamental, however, since we need the resulting factor $H(s)$ to be representable as a Dirichlet series.

Proof of Proposition 8. In this proof, we say that a statement involving the complex number s holds “on a suitable half-plane” if there exists a real number $\sigma_0 < 1$ such that the statement holds whenever $\Re s > \sigma_0$. For example, the last hypothesis of the lemma is equivalent [17, page 108, Theorem 3] to saying that the Dirichlet series $H(s) = \sum_{n=1}^{\infty} h_n n^{-s}$ converges absolutely on a suitable half-plane. For notational convenience we also set $R = \max\{\rho_1, \dots, \rho_\kappa\}$. We also use the notation $\Re s = \sigma$ and $\Im s = \tau$, so that $s = \sigma + i\tau$, and $\log^+(y) = \max\{0, \log y\}$.

Set

$$G(s) = F(s)\zeta(s)^{-\xi} = H(s) \frac{\prod_{j=1}^{\kappa} \zeta(\rho_j s - (\rho_j - 1))^{z_j}}{\zeta(s)^\xi}, \quad (14)$$

where $\xi = \sum_{j=1}^{\kappa} z_j$. Notice that a quotient $\zeta(\rho_j s - (\rho_j - 1))/\zeta(s)$ has a removable singularity at $s = 1$, and its value there is $1/\rho_j$. Therefore the fraction on the right-hand side of equation (14) has a removable singularity at $s = 1$, and its value there is $\prod_{j=1}^{\kappa} \rho_j^{-z_j}$. The zeta function has no zeros [17, page 157, Theorem 15] in a region of the shape

$$\sigma \geq 1 - \frac{c}{1 + \log^+ |\tau|}, \quad (15)$$

and hence the function $G(s)$ is holomorphic in the same region (as long as c is chosen small enough that $1 - c \geq \sigma$, so that $H(s)$ is defined throughout the region).

Now $H(s)$ is bounded in a suitable half-plane (by the constant $\sum_{n=1}^{\infty} |h_n| n^{-\sigma_0}$). In the region (15), we also have the bound $1/\zeta(s) \ll \log |\tau|$ for $|\tau| \geq 3$ [17, page 158, Theorem 16]. Finally, for any positive number δ , the zeta function satisfies the bound $\zeta(s) \ll_\delta |\tau|^\delta$ for $\sigma \geq 1 - \delta$ and $|\tau| \geq 1$ [17, page 146, Theorem 7]. Consequently, choosing $\delta = \frac{1}{2\xi}$, we have the bound

$$\zeta(\rho_j s - (\rho_j - 1)) \ll_\xi |\rho_j \tau|^{1/2\xi} \ll_{\xi, R} |\tau|^{1/2\xi}$$

for $\rho_j \sigma - (\rho_j - 1) \geq 1 - \frac{1}{2\xi}$, which is the same as $\sigma \geq 1 - \frac{1}{2\xi\rho_j}$ and hence is implied by $\sigma \geq 1 - \frac{1}{2\xi R}$. We conclude that

$$G(s) \ll_{\xi, R, H} (\log |\tau|)^\kappa \prod_{j=1}^{\kappa} |\tau|^{z_j/2\xi} \ll_{\kappa, \xi, R, H} (1 + |\tau|)^{3/4},$$

say, in the region (15) (as long as c is chosen smaller than $\frac{1}{2\xi R}$). Note that the implicit constant depends simply upon the sequence f (the parameters κ , ξ , and R and the function H being determined by F). Note also that our derivation of the upper bound $G(s) \ll_f (1 + |\tau|)^{3/4}$ assumed that $|\tau| \geq 3$, but the inequality surely holds for the compact subset $|\tau| \leq 3$ of the region (15) as well.

We have thus shown, in the notation of [17, pages 184–185] that the function $F(s)$ has the property $\mathcal{P}(\xi; c_0, \frac{1}{4}, M)$ for some constants c_0 and M depending on f . Since the coefficients f_n are

nonnegative, the function $F(s)$ automatically has the property $\mathcal{T}(\xi, \xi; c_0, \frac{1}{4}, M)$ as well. Applying the Selberg–Delange method as given in [17, page 185, Theorem 3] with $N = 0$, we conclude that

$$\sum_{n < N} f_n = N(\log N)^{\xi-1} \left(\lambda_0(\xi) + O_f \left(\frac{1}{\log N} \right) \right),$$

where by [17, page 185, equation (15)],

$$\lambda_0(\xi) = \frac{1}{\Gamma(\xi)} G(1) \gamma_0(\xi) = \frac{1}{\Gamma(\xi)} \frac{H(1)}{\prod_{j=1}^{\kappa} \rho_j^{z_j}} 1 = D_f$$

as desired. (The fact that $\gamma_0(\xi) = 1$ follows from [17, page 182, Theorem 1] in combination with the last line of the prior page.) \square

6. ACKNOWLEDGEMENTS

We are grateful to Valentin Blomer for pointing out that $a_\ell(p^r) = (\ell, \phi(p^r))$ for odd p and integer $r \geq 1$, and to Gérald Tenenbaum and Pieter Moree for offering their expertise over many years.

REFERENCES

- [1] G. Bhowmik and J.-C. Schlage-Puchta, Natural boundaries of Dirichlet series, *Funct. Approx. Comment. Math.* 37 (2007) 17–29; <http://arxiv.org/abs/0704.3370>; MR2357306 (2008j:11116).
- [2] C. David, J. Fearnley and H. Kisilevsky, On the vanishing of twisted L -functions of elliptic curves, *Experiment. Math.* 13 (2004) 185–198; MR2068892 (2005e:11082).
- [3] S. Finch, Quartic and octic characters modulo n , <http://arxiv.org/abs/0907.4894>.
- [4] S. Finch and P. Sebah, Squares and cubes modulo n , <http://arxiv.org/abs/math/0604465>.
- [5] G. Greaves, *Sieves in Number Theory*, Springer-Verlag, Berlin, 2001; MR1836967 (2002i:11092).
- [6] B. V. Levin and A. S. Fainleib, Application of certain integral equations to questions of the theory of numbers (Russian), *Uspehi Mat. Nauk* v. 22 (1967) n. 3, 119–197; Engl. transl. in *Russian Math. Survey* v. 22 (1967) n. 3, 119–204; MR0229600 (37 #5174).
- [7] F. Luca and I. E. Shparlinski, Average multiplicative orders of elements modulo n , *Acta Arith.* 109 (2003) 387–411; MR2009051 (2004i:11113).
- [8] H. L. Montgomery and R. C. Vaughan, *Multiplicative number theory. I. Classical theory*, Cambridge University Press, Cambridge, 2007; MR2378655 (2009b:11001).
- [9] P. Moree and J. Cazanar, On a claim of Ramanujan in his first letter to Hardy, *Exposition. Math.* 17 (1999) 289–311; MR1734249 (2001c:11103).
- [10] I. Niven, H. S. Zuckerman and H. L. Montgomery, *An Introduction to the Theory of Numbers*, 5th ed., John Wiley & Sons, Inc., New York, 1991; MR1083765 (91i:11001).
- [11] R. W. K. Odoni, A problem of Rankin on sums of powers of cusp-form coefficients, *J. London Math. Soc.* 44 (1991) 203–217; MR1136435 (93d:11048).
- [12] R. W. K. Odoni, Solution of a generalised version of a problem of Rankin on sums of powers of cusp-form coefficients, *Acta Arith.* 104 (2002) 201–223; MR1914720 (2003m:11067).
- [13] J. H. Rickert, *Solutions Manual to Accompany NZM 5th ed.*, unpublished manuscript (available from H. L. Montgomery).
- [14] M. du Sautoy, Zeta functions of groups and natural boundaries, unpublished manuscript (2000), available at <http://people.maths.ox.ac.uk/~dusautoy/1hard/prepri.htm>.
- [15] D. Shanks, *Solved and Unsolved Problems in Number Theory*, 2nd ed., Chelsea Publishing Co., New York, 1978; MR0516658 (80e:10003).
- [16] B. K. Spearman and K. S. Williams, Values of the Euler phi function not divisible by a given odd prime, *Ark. Mat.* 44 (2006) 166–181; MR2237219 (2007j:11133).
- [17] G. Tenenbaum, *Introduction to Analytic and Probabilistic Number Theory*, Cambridge University Press, Cambridge, 1995; MR1342300 (97e:11005b).

E-mail address: Steven.Finch@inria.fr

DEPT. OF STATISTICS, HARVARD UNIVERSITY, CAMBRIDGE, MA, USA

E-mail address: gerg@math.ubc.ca

DEPARTMENT OF MATHEMATICS, UNIVERSITY OF BRITISH COLUMBIA, ROOM 121, 1984 MATHEMATICS ROAD, CANADA V6T 1Z2

E-mail address: PSebah@yahoo.fr

DS RESEARCH, DASSAULT SYSTÈMES, SURESNES, FRANCE