HAL open science

FAST MULTI-PRECISION COMPUTATION OF SOME EULER PRODUCTS

Guillaume Bertoli, Christophe Besse, Gilles Vilmart

▶ **To cite this version:**

Guillaume Bertoli, Christophe Besse, Gilles Vilmart. FAST MULTI-PRECISION COMPUTATION OF SOME EULER PRODUCTS. Mathematics of Computation, 2021, 90 (331), pp.2247-2265. 10.1090/mcom/3630 . hal-03381427

HAL Id: hal-03381427

https://hal.science/hal-03381427v1

Submitted on 16 Oct 2021

HAL is a multi-disciplinary open access archive for the deposit and dissemination of scientific research documents, whether they are published or not. The documents may come from teaching and research institutions in France or abroad, or from public or private research centers.

L'archive ouverte pluridisciplinaire **HAL**, est destinée au dépôt et à la diffusion de documents scientifiques de niveau recherche, publiés ou non, émanant des établissements d'enseignement et de recherche français ou étrangers, des laboratoires publics ou privés.

MATHEMATICS OF COMPUTATION
Volume 00, Number 0, Pages 000–000
S 0025-5718(XX)0000-0

FAST MULTI-PRECISION COMPUTATION OF SOME EULER PRODUCTS

S. ETTAHRI, O. RAMARÉ, AND L. SUREL

Abstract. For every modulus $q \geq 3$, we define a family of subsets $\mathcal{A}$ of the multiplicative group $(\mathbb{Z}/q\mathbb{Z})^\times$ for which the Euler product $\prod_{p+q\mathbb{Z}\in\mathcal{A}}(1-p^{-s})$ can be computed with high numerical precision, where $s > 1$ is some given real number. We provide a Sage script to do so, and extend our result to compute Euler products $\prod_{p+q\mathbb{Z}\in\mathcal{A}} F(1/p^s)/H(1/p^s)$ where F and H are polynomials with real coefficients, when this product converges absolutely. This enables us to give precise values of several Euler products occurring in number theory.

1. Introduction

In formula (16) of [16], D. Shanks obtained the following closed expression to compute the Landau-Ramanujan constant:

$$\prod_{p\equiv 3[4]} \frac{1}{1-1/p^s} = \prod_{k\geq 0}\left(\frac{\zeta(2^k s)(1-2^{-2^k s})}{L(2^k s,\chi_{1,4})}\right)^{1/2^{k+1}} \tag{1.1}$$

where $s > 1$ and $\chi_{1,4}$ is the (only) non-principal Dirichlet character modulo 4. Since both $\zeta(2^k s)$ and $L(2^k s,\chi_{1,4})$ are $1+\mathcal{O}(1/2^{s2^k})$, we only need to compute $\mathcal{O}(\log D)$ values of L-functions (including the Riemann ζ-function) to obtain D decimal digits. In this paper, we generalize this process in several directions, but a main feature of our work is that it applies only to Euler products over primes belonging to some special subsets of $G = (\mathbb{Z}/q\mathbb{Z})^\times$ that we define below. We obtain closed formulas involving only values of L-functions of Dirichlet characters for rational Euler products over primes in these special sets and deduce fast ways to compute a more restricted class of such products. Let us first introduce the players.

Definition 1.1. *Two elements g_1 and g_2 of the abelian group G are said to be* lattice-invariant *if and only if they generate the same group. This defines an equivalence relation.*

We denote the set of lattice invariant *classes by $G^\sharp$ and the set of cyclic subgroups of G by $\mathscr{G}$. The map between $\mathscr{G}$ and $G^\sharp$ which, to a subgroup, associates the subset of its generators, is one-to-one.*

The cardinality of $G^\sharp$ can be swiftly inferred from [18, Theorem 3] or from [19, Theorem 1], both by L. Tóth. When $\mathcal{A}$ is a subset of $G = (\mathbb{Z}/q\mathbb{Z})^\times$, we define $\langle\mathcal{A}\rangle$ to be the (multiplicative) subgroup generated by $\mathcal{A}$.

2010 *Mathematics Subject Classification.* Primary 11Y60, Secundary 11N13, 05A.
Key words and phrases. Euler products, Loeschian numbers, Lal's constant.

©XXXX American Mathematical Society

For any Dirichlet character χ modulo q and any parameter $P \geq 2$, we define

$$L_P(s,\chi) = \prod_{p \geq P} (1 - \chi(p)/p^s)^{-1} \tag{1.2}$$

and correspondingly $\zeta_P(s) = \prod_{p \geq P}(1 - 1/p^s)^{-1}$.

Given K a subgroup of $G = (\mathbb{Z}/q\mathbb{Z})^\times$, we denote by $K^\perp$ the subgroup of Dirichlet characters modulo q that take the value 1 on K. When s is a real number, the number $\prod_{\chi \in K^\perp} L_P(s,\chi)$ is indeed a positive real number because, when χ belongs to $K^\perp$, so does $\overline{\chi}$.

Here is the central theorem of this paper.

Theorem 1.2. *Let q be some modulus and $\mathcal{A}$ be a* lattice-invariant *class of $G = (\mathbb{Z}/q\mathbb{Z})^\times$. Let $F, H \in \mathbb{R}[X]$ be two polynomials satisfying $F(0) = H(0) = 1$ and let $\Delta \geq 1$ be an integer such that $(F(X) - H(X))/X^\Delta \in \mathbb{R}[X]$. Let $\beta \geq 2$ be an upper bound for the maximum modulus of the inverses of the roots of F and of H. Let $\sigma_1, \sigma_2, \cdots, \sigma_{\deg F}$ be the roots of F (a multiple root appears as many times as its multiplicity), and similarly, let $\rho_1, \rho_2, \cdots, \rho_{\deg H}$ be the roots of H. For any non-negative integer d, we set*

$$s_{H/F}(d) = \sum_{1 \leq i \leq \deg H} \rho_i^{-d} - \sum_{1 \leq j \leq \deg F} \sigma_j^{-d}. \tag{1.3}$$

Let P and $s > 1/\Delta$ be two real parameters such that $P^s \geq 2\beta$. We define, for any cyclic subgroup K of G and any positive integer m,

$$C_{\mathscr{A}}(K, m, F/H) = \sum_{t \mid m} \mu(t) s_{H/F}(m/t) \sum_{\substack{L \in \mathscr{G}, \\ L^{[t]} = \langle \mathscr{A} \rangle, \\ K \subset L}} \frac{\mu(|L|/|K|)}{|G/K|} \tag{1.4}$$

where $L^{[t]} = \{x^t, x \in L\}$ and $\langle \mathscr{A} \rangle$ is the subgroup generated by $\mathscr{A}$. We have

$$\prod_{\substack{p \geq P, \\ p + q\mathbb{Z} \in \mathcal{A}}} \frac{F(1/p^s)}{H(1/p^s)} = \prod_{m \geq \Delta} \prod_{K \in \mathscr{G}} \Big(\prod_{\chi \in K^\perp} L_P(ms, \chi) \Big)^{C_{\mathscr{A}}(K,m,F/H)/m}. \tag{1.5}$$

For any positive real-valued parameter M, the following bound holds true:

$$\pm \log \prod_{m \geq M+1} \prod_{K \in \mathscr{G}} \Big(\prod_{\chi \in K^\perp} L_P(ms, \chi) \Big)^{\frac{C_{\mathscr{A}}(K,m,F/H)}{m}} \leq 4(\deg F + \deg H)|\mathscr{G}|^2 (s + P) \Big(\frac{\beta}{P^s} \Big)^{M+1}. \tag{1.6}$$

In the case $H/F = 1 - X$, the relevant identity is proved in Theorem 2.6 and is the heart of this paper. Our result applies in particular to $\mathcal{A} = \{1\}$ and to $\mathcal{A} = \{-1\}$. When $q = 4$ and $\mathcal{A} = \{-1\}$, we readily find that only $t = 1$ matters in (1.4), that $C_{\{-1\}}(\{1\}, 2^k, 1/(1-X)) = -1/2$ and that $C_{\{-1\}}(\{\pm 1\}, 2^k, 1/(1-X)) = 1$. On recalling Lemma 2.4, this results in (1.1).

Remark 1.3. Lemma 3.3 ensures that we may select

$$\beta = \max\Big(2, \sum_{1 \leq k \leq \deg F} |a_k|, \sum_{1 \leq k \leq \deg H} |b_k|\Big)$$

when $F(X) = 1 + a_1X + \ldots + a_\delta X^\delta$ and $H(X) = 1 + b_1X + \ldots + b_{\delta'}X^{\delta'}$. Notice that our assumptions imply that $b_i = a_i$ when $i < \Delta$.

Remark 1.4. The numbers $s_{H/F}(n)$ may be computed via the Girard-Newton relations recalled in Lemma 3.1.

Remark 1.5. We prove in Lemma 3.4 that, when K and $\mathscr{A}$ are fixed, the quantity $\sum_{\substack{L\in\mathscr{G},\\ L^{[t]}=\langle\mathscr{A}\rangle,\\ K\subset L}} \mu(|L|/|K|)$ depends only on $\gcd(t, \varphi(q))$.

Remark 1.6. We have $C_{\mathscr{A}}(K, m, F/H) = -C_{\mathscr{A}}(K, m, H/F)$, a property we shall use to simplify the typography.

Remark 1.7. There is some redundancy in our formula as a same character χ may appear in several sets $K^\perp$ (for instance, the principal character appears in all of them). Disentangling these contributions leads to a slightly more complicated formula. We first have to introduce, for any cyclic subgroup S, the subset $S^{\perp\circ} \subset S^\perp$ constituted of those elements that do not belong to any $T^\perp$, for $T \subsetneq S$. It can be readily checked that any $K^\perp$ is the union of $S^{\perp\circ}$ where S ranges the subgroups that are included in K. We then define

$$C^\circ_{\mathscr{A}}(S, m, F/H) = \sum_{t|m} \mu(t) s_{H/F}(m/t) \sum_{\substack{L\in\mathscr{G},\\ L^{[t]}=\langle\mathscr{A}\rangle,\\ S\subset L}} \frac{\varphi(|L|/|S|)}{|G/S|}. \tag{1.7}$$

Formula (1.5) becomes:

$$\prod_{\substack{p\geq P,\\ p+q\mathbb{Z}\in\mathcal{A}}} \frac{F(1/p^s)}{H(1/p^s)} = \prod_{m\geq\Delta} \prod_{S\in\mathscr{G}} \Bigg(\prod_{\chi\in S^{\perp\circ}} L_P(ms, \chi) \Bigg)^{C^\circ_{\mathscr{A}}(S,m,F/H)/m} \tag{1.8}$$

and the bound (1.6) holds to estimate the tail of this product, as we only shuffled terms with a fixed index m.

Super fast evaluations.

Corollary 1.8. *For every positive integer m, the constant $C_{\mathscr{A}}(K, m, 1 - X)$ vanishes when one prime factor of m is coprime with $\varphi(q)$. As a consequence and under the hypotheses of Theorem 1.2 with $\Delta = 1$, the products*

$$\prod_{\substack{p\geq P,\\ p+q\mathbb{Z}\in\mathcal{A}}} \left(1 - \frac{1}{p^s}\right)$$

may be computed by $\mathcal{O}((\log D)^r)$ computations of L-functions to get D-decimal digits, where r is the number of prime factors of $\varphi(q)$. The implied constant in the $\mathcal{O}$-symbol may depend on q.

This leads to very fast computations, and we were for instance able to produce 100 (resp. 1000, resp. 5000) digits of these products when $q = 3$ in a third of a second (resp. 12 seconds, resp. 35 minutes with $P = 400$) on a usual desktop computer. See the implementation notes at the end of this paper. Notice however that the number of L-values required is not the only determinant: when q increases, the dependence in q matters as the character group increases in size, and when the required precision increases, each computation of an L-value may take a long time. We do not address

the issue of these computations here. We present some timing data at the end of this paper.

Proof of Corollary 1.8. Lemma 2.4 tells us that $C_{\mathscr{A}}(K, m, 1-X)$ vanishes when one prime factor of m is coprime with $\varphi(q)$. Let us decompose $\varphi(q)$ in prime factors: $\varphi(q) = p_1^{\alpha_1} \cdots p_r^{\alpha_r}$. Any integer $m \le M$ such that all its prime factors divide q, can be written as $m = p_1^{\beta_1} \cdots p_r^{\beta_r}$ with $\beta_i \le (\log M)/\log p_i$ for $i \le r$. In particular, there are at most $((\log M)/\log 2)^r$ such integers. By (1.6), the contribution of the integers $m > M$ to the Euler product to be computed is $1 + \mathcal{O}((\beta/P^s)^M)$, which is $1+\mathcal{O}(2^{-M})$ by the assumption $P^s \ge 2\beta$. We want this error term to be $1+\mathcal{O}(10^{-D})$ to get about $D + \mathcal{O}(1)$ decimal digits. This is ensured by $M \log 2 \ge D \log 10$, i.e. it is enough to take $M = 4D$. □

In order to extend this property to other Euler products, many of the coefficients $C_{\mathscr{A}}(K, m, F/H)$ should vanish when m varies. This is however not likely to happen, except when F/H is a product/quotient of cyclotomic polynomials. Indeed the coefficients $s_{H/F}(m)$ satisfy a linear recurrence (of degree at most $\max(\deg F, \deg H)$) and as such are expected to grow exponentially fast if they are not roots of unity. When for instance the coefficients of the recurrence belong to some number field, this is proved by Evertse in [3] and independently by van der Poorten and Schlickewei in [20]. This is the case where we may expect cancellations to happen. Since the sum defining $C_{\mathscr{A}}(K, m, F/H)$ is of the form $\sum_{t|m} \mu(t) r_0(t) s_{H/F}(m/t)$ for some function $r_0(t)$ that remains bounded (it takes only a finite set of values), it is dominated by the term $t = 1$ when m is large enough; no cancellation due to the Möbius factor can be expected either. We are then left with the case of cyclotomic polynomials, but they can be easily dealt with using Corollary 1.8; indeed, if we denote by Φ_n the n-th cyclotomic polynomial, the identity $\prod_{d|n} \Phi_d(X) = X^n - 1$ gets inverted to $\Phi_n(X) = \prod_{d|n} (X^d - 1)^{\mu(n/d)}$.

A Sage script. The material of this paper has been used to write a Sage script *using Python 3* which can be found on the webpage of the second author:
`http://iml.univ-mrs.fr/~ramare/Maths/LatticeInvariantEulerProducts-06.sage`
We shorten this name throughout this paper in `LIEP.sage`. We give some details about this script when developing the proof below. We also provide on the second author's webpage the first hundred digits of several Euler products:
`http://iml.univ-mrs.fr/~ramare/Maths/SomeEulerProducts-02.pdf`
The function `GetEulerProds(q, s, F, H, nbdecimals)` gives all these Euler products. The polynomials F and H are to be given as polynomial expressions with the variable x. The special function `GetVs(q, s, nbdecimals)` gives all the Euler products of Corollary 1.8.

Some historical pointers. D. Shanks in [14] (resp. [15], resp. [17]) has already been able to compute an Euler product over primes congruent to 1 modulo 4 (resp. to 1 modulo 8 in both instances), by using an identity (Lemma of section 2 for [14], Equation (5) in [15] and the Lemma of section 3 in [17]) that is a precursor of our Lemma 3.1.

In these three examples, the author has only been able to compute the first five digits, and this is due to three facts: the lack of an interval arithmetic package at that time, the relative weakness of the computers and the absence of a proper study

of the error term. We thus complement these results by giving the first hundred decimals.

Complementary to the published papers, three influent preprints on how to compute Euler products with high accuracy have been floating on the web: [5] a memo started in 1990 in its 1996 version by Ph. Flajolet and I. Vardi, [1] by H. Cohen and [7] by X. Gourdon and P. Sebah. Comparing the desired constant with zeta-values is the overarching idea. The set of zeta-values is extended to L-values of (some) quadratic characters in the three, in some way or another, and to the values of Dedekind zeta-function in [1]. No complete error term analysis is presented, sometimes because the series used are simple enough to make this analysis rather easy. These three sources also deal with constants that are sums over primes and a similar extension of our work is possible, but kept for later. It should be noticed that Equation (20) from [5] is in fact the formula given as Equation (16) in [16] for the Landau-Ramanujan constant.

On the methodology. We decided to prove Theorem 1.2 directly, by giving the formula and shuffling terms. This gives a short and self-contained proof. However, we did not come up with the coefficients $C_{\mathscr{A}}(K, m, F/H)$ by some lucky strike! There is a path leading from abelian field theory to our expression that is much closer to D. Shanks's approach. We say more on this subject in section 4.

Application to some constants. This paper has been inspired by the wish to compute with high numerical precision two constants that appear in the paper [6] by É. Fouvry, C. Levesque and M. Waldschmidt. In the notation of that paper, they are

$$\alpha_0^{(3)} = \frac{1}{3^{1/4}\sqrt{2}} \prod_{p\equiv 2[3]} \left(1 - \frac{1}{p^2}\right)^{-1/2} \tag{1.9}$$

and

$$\beta_0 = \frac{3^{1/4}\sqrt{\pi}}{2^{5/4}} \frac{\log(2+\sqrt{3})^{1/4}}{\Gamma(1/4)} \prod_{p\equiv 5,7,11[12]} \left(1 - \frac{1}{p^2}\right)^{-1/2}. \tag{1.10}$$

Both occur in number theory as densities. The number of integers n of the shape $n = x^2 - xy + y^2$, where x and y are integers (these are the so-called Loeschian numbers, see the sequence A003136 entry in [12]) is asymptotically approximated by

$$N(x) = \alpha_0^{(3)} \frac{x(1+o(1))}{\sqrt{\log x}}. \tag{1.11}$$

This motivates our interest in the first constant. The second one arises in counting the number of Loeschian numbers that are also sums of two squares (see sequence A301430 entry of [12]), namely we have

$$N'(x) = \beta_0 \frac{x(1+o(1))}{(\log x)^{3/4}}.$$

From the sequence A301429 entry in [12], we know that $\alpha_0^{(3)} = 0.638909\ldots$ but we would like to know (many!) more digits. Similarly it is known that $\beta_0 = 0.30231614235\ldots$.

Corollary 1.9. *We have*

$$\alpha_0^{(3)} = 0.63890\,94054\,45343\,88225\,49426\,74928\,24509\,37549\,75508\,02912 \\ 33454\,21692\,36570\,80763\,10027\,64965\,82468\,97179\,11252\,86643\cdots$$

and

$$\beta_0 = 0.30231\,61423\,57065\,63794\,77699\,00480\,19971\,56024\,12795\,18936 \\ 96454\,58867\,84128\,88654\,48752\,41051\,08994\,87467\,81397\,92727\cdots$$

This follows from Theorem 1.2 with the choices $q = 3$ and $\mathcal{A} = \{2\}$ for $\alpha_0^{(3)}$, and $q = 12$ and $\mathcal{A} = \{5, 7, 11\}$ for β_0. The other parameters are uniformly selected as $F(X) = 1 - X^2$, $H(X) = 1$, $\Delta = 2$, $\beta = 2$ and $s = 1$.

Corollary 1.10 (Shanks' Constant)**.** *We have*

$$\prod_{p\equiv 1[8]} \left(1 - \frac{4}{p}\right)\left(\frac{p+1}{p-1}\right)^2 = 0.95694\,53478\,51601\,18343\,69670\,57273\,89182\,87531 \\ 74977\,2913914789\,05432\,60424\,60170\,16444\,88885 \\ 94814\,40512\,03907\,95084\cdots$$

As a consequence Shanks' constant satisfies

$$I = \frac{\pi^2}{16\log(1+\sqrt{2})} \prod_{p\equiv 1[8]} \left(1 - \frac{4}{p}\right)\left(\frac{p+1}{p-1}\right)^2 \\ = 0.66974\,09699\,37071\,22053\,89224\,31571\,76440\,66883\,70157\,43648 \\ 24185\,73298\,52284\,52467\,99956\,45714\,72731\,50621\,02143\,59373\cdots$$

We deduce this Corollary from Theorem 1.2 by selecting the parameters $q = 8$, $\mathcal{A} = \{1\}$, $F(X) = 1 - 2X - 7X^2 - 4X^3$, $H(X) = 1 - 2X + X^2$, $s = 1$, $\Delta = 2$ and $\beta = 4$. As explained in [15], the number of primes $\leq X$ of the form $m^4 + 1$ is conjectured to be asymptotically equal to $I \cdot X^{1/4}/\log X$. The name "Shanks' constant" comes from Chapter 2, page 90 of [4].

When using the script that we introduce below, this value is obtained by multiplying by $\frac{\pi^2}{16\log(1+\sqrt{2})}$ the value obtained with the call

```
GetEulerProds(8, 1, 1-2*x-7*x^2-4*x^3, 1-2*x+x^2, 110, 50, 2, 1).
```

A note is required here: the script evaluates loosely the required working precision in order to get say 100 correct digits at the end. The results are however presented with the precision obtained, and if we had been asking initially for 100 decimal digits, the script would issue only 94 of them. We could have implemented a mechanism that increases the precision until the result satisfies the request, but we have prefered to let the users increase the precision by themselves. When asking for 110 decimal digits, the script is able to compute 106 of them. We can get a thousand decimals for this constant in about 2 minutes on a usual desktop computer (by asking for 1010 decimal digits), see the implementation notes at the end of this paper.

Corollary 1.11 (Lal's Constant)**.** *We have*

$$\prod_{p\equiv 1[8]} \frac{p(p-8)}{(p-4)^2} = 0.88307\,10047\,43946\,67141\,78342\,99003\,10853\,46768 \\ 88834\,88097\,34707\,19295\,15939\,52119\,46990\,65659 \\ 68857\,99383\,28603\,79164\cdots$$

As a consequence Lal's constant satisfies

$$\begin{aligned}\lambda &= \frac{\pi^4}{2^7\log^2(1+\sqrt{2})}\prod_{p\equiv 1[8]}\left(\frac{p+1}{p-1}\right)^4\left(1-\frac{8}{p}\right)\\ &= \frac{\pi^4}{2^7\log^2(1+\sqrt{2})}\prod_{p\equiv 1[8]}\left(1-\frac{4}{p}\right)^2\left(\frac{p+1}{p-1}\right)^4\prod_{p\equiv 1[8]}\frac{p(p-8)}{(p-4)^2}\\ &= 0.79220\,82381\,67541\,66877\,54555\,66579\,02410\,11289\,32250\,98622\\ &\qquad 11172\,27973\,45256\,95141\,54944\,12490\,66029\,53883\,98027\,52927\cdots\end{aligned}$$

We deduce the first value given in this Corollary by using Theorem 1.2 with the parameters $q=8$, $\mathcal{A}=\{1\}$, $F(X)=1-8X$, $H(X)=1-8X+16X^2$, $s=1$, $\Delta=2$ and $\beta=8$. The value of Lal's constant λ is then deduced by combining the value obtained in Corollary 1.10 together with this one. This splitting of the computation in two introduces smaller polynomials and this leads to a lesser running time. As explained in [17], the number of primes $\le X$ of the form $(m+1)^2+1$ and such that $(m-1)^2+1$ is also prime, is conjectured to be asymptotic to $\lambda\cdot X^{1/2}/(\log X)^2$. The name "Lal's Constant" comes from the papers [8] and [17]. When using the script that we introduce below, the first value is obtained with the call

```
GetEulerProds(8, 1, 1-8*x, 1-8*x+16*x^2, 110, 50, 2, 1).
```

If this call requires about 2 seconds on a usual desktop computer, this time increases to 4 minutes when we ask for a thousand digits. We did not try to get 5000 digits as we did for the products of Corollary 1.8.

We close this section by mentioning another series of challenging constants. In [10], P. Moree computes inter alia the series of constants A_χ defined six lines after Lemma 3, page 452, by

$$A_\chi = \prod_{p\ge 2}\left(1+\frac{(\chi(p)-1)p}{(p^2-\chi(p))(p-1)}\right), \tag{1.12}$$

where χ is a Dirichlet character. Our theory applies only when χ is real valued.

A closed formula for primitive roots. Let us recall that a *primitive root* n modulo q is an integer such that the class of n generates $G=(\mathbb{Z}/q\mathbb{Z})^\times$. It is a classical result that such an element exists if and only if q is equal to 2 or 4, or is equal to a prime power of an odd prime or to twice such a prime power.

Corollary 1.12. *Let $\mathscr{A}_0$ be the subset of $G=(\mathbb{Z}/q\mathbb{Z})^\times$ consisting of all the multiplicative generators of G. Assume q is such that such an $\mathscr{A}_0$ is not empty. For any real parameter $P\ge 2$ and $s>1$, we have*

$$\zeta_P(s;q,\mathscr{A}_0) = \prod_{m|q^\infty}\prod_{S\in\mathscr{G}}\left(\prod_{\chi\in K^{\perp\circ}} L_P(ms,\chi)\right)^{e(m,q,S)},$$

where $m|q^\infty$ means that all the prime factors of m divide q and where $e(m,q,S)=\frac{|S|\varphi(q/|S|)}{m\varphi(q)}$.

Proof. Indeed, since $\mathscr{A}_0$ generates G, the only index t in (1.7) is $t=1$. Hence, only $L=G$ is possible. □

Thanks. The authors thank M. Waldschmidt for having drawn their attention to this question, P. Moree and É. Fouvry for helpful discussions on how to improve this paper and X. Gourdon for exchanges concerning some earlier computations. The referees are also to be warmly thanked for their very careful reading and for ideas on how to improve both the presentation and the corresponding script.

2. Proof of Theorem 1.2 when $F/H = 1/(1-X)$

We follow the notation introduced in (1.4). Since here $F/H = 1/(1-X)$, this leads us to consider, for any cyclic subgroup $K \in \mathscr{G}$, any class $\mathscr{A}$ in $G^\sharp$ and any positive integer m, the coefficient

$$C_{\mathscr{A}}(K, m, 1-X) = \sum_{t|m} \mu(t) \sum_{\substack{L\in\mathscr{G},\\ L^{[t]}=\langle\mathscr{A}\rangle}} \frac{\mu(|L|/|K|)}{|G/K|} \tag{2.1}$$

where $L^{[t]} = \{x^t, x \in L\}$. Notice that it is also a cyclic subgroup of G. Let us first note a simple property.

Lemma 2.1. *In a finite cyclic group L, the map that associates to a subgroup of L its cardinality is a one-to-one map between the set of divisors of $|L|$ and the set of its subgroups. Furthermore, any subgroup of a cyclic group is cyclic.*

Proof. We can assume that $L = (\mathbb{Z}/\ell\mathbb{Z}, +)$. For each $d|\ell$, the unique subgroup of order d is $\{(\ell/d)n, 0 \le n \le d-1\}$. □

Here is the fundamental property satisfied by these coefficients.

Proposition 2.2. *For any positive integer ℓ, any prime p and any lattice-invariant class $\mathscr{A}$, we have*

$$\sum_{hm=\ell} \sum_{\substack{K\in\mathscr{G},\\ \chi\in K^\perp}} \chi(p^h) C_{\mathscr{A}}(K, m, 1-X) = \mathbf{1}_{p\in\mathscr{A}}.$$

Proof. Let S be the left-hand side sum to be evaluated. Let B be the subgroup generated by p. By using the orthogonality of characters, we readily obtain

$$S = \sum_{hm=\ell} \sum_{\substack{K\in\mathscr{G},\\ B^{[h]}\subset K}} |G/K| C_{\mathscr{A}}(K, m, 1-X).$$

Next, we introduce the expression given in (2.1), shuffle the summations and get

$$S = \sum_{hm=\ell} \sum_{t|m} \mu(t) \sum_{\substack{L\in\mathscr{G},\\ L^{[t]}=\langle\mathscr{A}\rangle}} \sum_{\substack{K\in\mathscr{G},\\ B^{[h]}\subset K}} \mu(|L|/|K|).$$

By Lemma 2.1 and the Möbius function characteristic property, the last summation vanishes when $B^{[h]} \neq L$ and takes the value 1 otherwise. Since $(B^{[h]})^{[t]} = B^{[ht]}$, this gives us

$$S = \sum_{hm=\ell} \sum_{\substack{t|m,\\ B^{[ht]}=\langle A\rangle}} \mu(t).$$

We continue in a more classical way:

$$S = \sum_{\substack{ath=\ell,\\ B^{[ht]}=\langle A\rangle}} \mu(t) = \sum_{\substack{ab=\ell,\\ B^{[b]}=\langle A\rangle}} \sum_{t|b} \mu(t) = \mathbf{1}_{B=\langle A\rangle},$$

concluding the proof. □

Corollary 2.3. *For any prime p, any positive real number s and any lattice-invariant class $\mathscr{A}$, we have*

$$\prod_{m\geq 1}\prod_{K\in\mathscr{G}}\Big(\prod_{\chi\in K^\perp}(1-\chi(p)p^{-ms})\Big)^{-C_{\mathscr{A}}(K,m,1-X)/m} = \begin{cases}(1-p^{-s})^{-1} & \text{when } p\in\langle\mathscr{A}\rangle,\\ 1 & \text{otherwise.}\end{cases}$$

Proof. We first check that, for any positive integer m and any subgroup K, we have

$$\exp\sum_{\chi\in K^\perp}\sum_{h\geq 1}\frac{\chi(p^h)}{hp^{mhs}} = \prod_{\chi\in K^\perp}\Big(1-\frac{\chi(p)}{p^{ms}}\Big)^{-1}.$$

Since s is a positive real number, the right-hand side is also positive, and so can be raised to some rational power, say c. The sum inside the exponential is also a real number and the equation $\exp x = y$ leads obviously to $\exp(cx) = y^c$. The right-hand side of our lemma may thus be written $\exp S(p)$ where

$$S(p) = \sum_{m\geq 1}\sum_{K\in\mathscr{G}}\sum_{\chi\in K^\perp}\sum_{h\geq 1}\frac{\chi(p^h)C_{\mathscr{A}}(K,m,1-X)}{mhp^{mhs}}.$$

We set $\ell = mh$ and appeal to Proposition 2.2 to infer that

$$S(p) = \sum_{\ell\geq 1}\frac{1}{\ell p^{\ell s}}\mathbf{1}_{p\in\mathscr{A}},$$

from which our corollary follows readily. □

Lemma 2.4. *If m has a prime factor that does not divide $\varphi(q)$, we have $C_{\mathscr{A}}(K,m,1-X) = 0$.*

Proof. When $F/H = 1-X$, we have $s_{H/F}(m) = -1$ uniformly in m. If $m = m_1p^a$ for some m_1 prime to p and p prime to the order $\varphi(q)$ of G, any divisor t of m factors in t_1p^b where $t_1|m_1$ and $b\leq a$. The Möbius coefficient reduces these choices to $b = a$ or to $b = a-1$ and since we have $L^{[t]} = L^{[t_1]}$, both are possible. If we denote the contribution of p^at_1 to $C_{\mathscr{A}}(K,m,1-X)$ by S_1 say, the contribution or $p^{a-1}t_1$ is $-S_1$, and on pairing them we get zero. □

Lemma 2.5. *Let $f > 1$ be a real parameter. We have*

$$\big|\log\zeta_P(f)\big| \leq \frac{1+P/(f-1)}{P^f}.$$

Proof. We use

$$\log\zeta_P(f) = -\sum_{p\geq P}\sum_{k\geq 1}\frac{1}{kp^{kf}}$$

hence, by using a comparison to an integral, we find that

$$\Big|\log\zeta_P(f)\Big| \leq \sum_{n\geq P}\frac{1}{n^f} \leq \frac{1}{P^f} + \int_P^\infty\frac{dt}{t^f} = \Big(\frac{f-1}{P}+1\Big)\frac{1}{(f-1)P^{f-1}}.$$ □

Theorem 2.6. *For every $s > 1$ and every $P \geq 2$, we have*

$$\zeta_P(s; q, \mathcal{A}) = \prod_{\substack{p+q\mathbb{Z}\in\mathcal{A},\\ p\geq P}} (1-p^{-s})^{-1} = \prod_{m\geq 1}\prod_{K\in\mathscr{G}}\Bigl(\prod_{\chi\in K^\perp} L_P(ms,\chi)\Bigr)^{C_{\mathscr{A}}(K,m,1-X)/m}.$$

Proof. This is a simple consequence of Corollary 2.3. Indeed, we may shuffle our series to our fancy by the absolute summability ensured by the condition $s > 1$ and the bounds $|C_{\mathscr{A}}(K,k)/k| \leq |G|$, as well as $|\mathscr{G}| \leq |G|$. This last bound follows from the fact that there are at most as many cyclic subgroups as there are possible generators. □

3. Proof of Theorem 1.2 in general

Let us recall the Witt decomposition. The readers will find in [9, Lemma 1] a result of the same flavour. We have simply modified the proof and setting as to accomodate polynomials having real numbers for coefficients.

Lemma 3.1. *Let $F(t) = 1 + a_1 t + \ldots + a_\delta t^\delta \in \mathbb{R}[t]$ be a polynomial of degree δ. Let $\alpha_1, \ldots, \alpha_\delta$ be the inverses of its roots. Put $s_F(k) = \alpha_1^k + \ldots + \alpha_\delta^k$. The $s_F(k)$ are integers and satisfy the Newton-Girard recursion*

$$s_F(k) + a_1 s_F(k-1) + \ldots + a_{k-1} s_F(1) + k a_k = 0, \tag{3.1}$$

where we have defined $a_{\delta+1} = a_{\delta+2} = \ldots = 0$. Put

$$b_F(k) = \frac{1}{k}\sum_{d|k} \mu(k/d) s_F(d). \tag{3.2}$$

Let $\beta \geq 1$ be such that $\beta \geq \max_j |1/\alpha_j|$. When t belongs to any segment $\subset (-\beta, \beta)$, we have

$$F(t) = \prod_{j=1}^{\infty} (1-t^j)^{b_F(j)} \tag{3.3}$$

where the convergence is uniform in the given segment.

Proof. Since we follow the proof of [9, Lemma 1], we shall be rather sketchy. We write $F(t) = \prod_i (1-\alpha_i t)$. By logarithmic differentiation, we obtain

$$\frac{tF'(t)}{F(t)} = \sum_i \frac{\alpha_i t}{1-\alpha_i t} = \sum_{k\geq 1} s_F(k) t^k.$$

This series is absolutely convergent in any disc $|t| \leq b < 1/\beta$ where $\beta = \max_j(1/|\alpha_j|)$. We proceed by expressing s_F in terms of b_F via (3.2) in a disc of radius $b < 1/\beta$. After some shuffling of the terms, we reach the expression

$$\frac{tF'(t)}{F(t)} = \sum_{j\geq 1} b_F(j) \frac{jt^j}{1-t^j}.$$

The lemma follows readily by integrating the above relation. □

How does the mathematician E. Witt enter the scene? In the paper [21] on Lie algebras, Witt produced in equation (11) therein a decomposition that is the prototype of the above expansion.

Lemma 3.2. *We use the hypotheses and notation of Lemma 3.1. Let $\beta \geq 2$ be larger than the inverse of the modulus of all the roots of $F(t)$. We have*

$$|b_F(k)| \leq 2 \deg F \cdot \beta^k / k.$$

Proof. We clearly have $|s_F(j)| \leq \deg F \cdot \beta^j$, so that

$$\begin{aligned} |b_F(k)| &\leq \frac{\deg F}{k} \sum_{1 \leq j \leq k} \beta^j \leq \frac{\deg F}{k} \beta \frac{\beta^k - 1}{\beta - 1} \\ &\leq \frac{\deg F}{k} \frac{\beta^k}{1 - 1/\beta} \leq 2 \deg F \frac{\beta^k}{k}. \end{aligned}$$

□

There are numerous easy upper estimates for the inverse of the modulus of all the roots of $F(t)$ in terms of its coefficients. Here is a simplistic one.

Lemma 3.3. *Let $F(X) = 1 + a_1 X + \ldots + a_\delta X^\delta$ be a polynomial of degree δ. Let ρ be one of its roots. Then either $|\rho| \geq 1$ or $1/|\rho| \leq |a_1| + |a_2| + \ldots + |a_\delta|$.*

Proof. On noticing that

$$(1/\rho)^\delta = -a_1 (1/\rho)^{\delta - 1} - a_2 (1/\rho)^{\delta - 2} - \ldots - a_\delta,$$

the conclusion follows. □

Lemma 3.4. *The sum $\sum_{L \in \mathcal{L}} \mu(|L|/|K|)$ where $\mathcal{L} = \{L \in \mathscr{G}/L^{[t]} = \langle \mathscr{A} \rangle$ and $K \subset L\}$ depends only on $\gcd(t, \varphi(q))$.*

Proof. Let us call this quantity $r_0(t)$. We first check that it depends only on $t \mod \varphi(q)$: this follows from the fact that the map $x \mapsto x^{\varphi(q)}$ reduces to the identity over G. Secondly, any prime factor of t, say p', that is prime to $\varphi(q)$, may be removed from t, i.e. $r_0(t) = r_0(t/p')$: the map $x \mapsto x^{p'}$ is one-to-one in L.

The lemma is an immediate consequence of these two remarks. □

Proof of Theorem 1.2. The proof requires several steps. The very first one is a direct consequence of (3.3), which leads to the identity

$$\frac{F(t)}{H(t)} = \prod_{j=\Delta}^{\infty} (1 - t^j)^{b_F(j) - b_H(j)}. \tag{3.4}$$

The absence of the term with $j < \Delta$ is due to our assumption that $(F(X) - H(X))/X^\Delta \in \mathbb{R}[X]$. Up to this point (3.4) is only established as a formal identity. Our second step is to establish (3.4) for all $t \in \mathbb{C}$ with $|t| < 1/\beta$. By Lemma 3.2, we know that $|b_F(j) - b_H(j)| \leq 4 \max(\deg F, \deg H) \beta^j / j$. Therefore, for any bound J, we have

$$\sum_{j \geq J+1} |t^j| |b_F(j) - b_H(j)| \leq 4 \max(\deg F, \deg H) \frac{|t\beta|^{J+1}}{(1 - |t\beta|)(J+1)}, \tag{3.5}$$

as soon as $|t| < 1/\beta$. We thus have

$$\frac{F(t)}{H(t)} = \prod_{\Delta \leq j \leq J} (1 - t^j)^{b_F(j) - b_H(j)} \times I_1, \tag{3.6}$$

where $|\log I_1| \le 4\max(\deg F, \deg H)|t\beta|^{J+1}/[(1-|t\beta|)(J+1)]$. Now that we have the expansion (3.6) for each prime p, we may combine them. We readily get

$$\prod_{\substack{p\ge P,\\ p+q\mathbb{Z}\in\mathcal{A}}} \frac{F(1/p^s)}{H(1/p^s)} = \prod_{\substack{p\ge P,\\ p+q\mathbb{Z}\in\mathcal{A}}} \prod_{\Delta\le j\le J} (1-p^{-js})^{b_F(j)-b_H(j)} \times I_2,$$

where I_2 satisfies

$$\begin{aligned}|\log I_2| &\le 4\max(\deg F, \deg H)\sum_{p\ge P}\frac{\beta^{J+1}}{1-\beta/P^s}\frac{1}{(J+1)p^{(J+1)s}}\\ &\le \frac{4\max(\deg F, \deg H)\beta^{J+1}}{(1-\beta/P^s)(J+1)}\left(\frac{1}{P^{(J+1)s}}+\int_P^\infty \frac{dt}{t^{(J+1)s}}\right)\\ &\le \frac{4\max(\deg F, \deg H)(\beta/P^s)^J\beta}{(1-\beta/P^s)(J+1)}\left(\frac{1}{P^s}+\frac{1}{Js+s-1}\right),\end{aligned}$$

since $P\ge 2$ and $J\ge 3$. Letting J go to infinity, we see that when $P^s>\beta$ and $s>1/\Delta$,

$$\prod_{\substack{p\ge P,\\ p+q\mathbb{Z}\in\mathcal{A}}} \frac{F(1/p^s)}{H(1/p^s)} = \prod_{j\ge\Delta}\prod_{\substack{p\ge P,\\ p+q\mathbb{Z}\in\mathcal{A}}} (1-p^{-js})^{b_F(j)-b_H(j)} = \prod_{j\ge 2}\zeta_P(js;q,\mathscr{A})^{b_H(j)-b_F(j)}$$

in the notation of Theorem 2.6. We use this theorem to infer that

$$\prod_{\substack{p\ge P,\\ p+q\mathbb{Z}\in\mathcal{A}}} \frac{F(1/p^s)}{H(1/p^s)} = \prod_{j\ge\Delta}\prod_{m\ge 1}\prod_{K\in\mathscr{G}}\Big(\prod_{\chi\in K^\perp} L_P(mjs,\chi)\Big)^{\frac{C_{\mathscr{A}}(K,m,1-X)}{m}(b_H(j)-b_F(j))}.$$

Notice that we have $s_H(j)-s_F(j)=0$ (and hence $b_H(j)-b_F(j)=0$) when $j<\Delta$ by our assumption on Δ. Let us glue the variables m and j in n. On using the definitions (2.1) and (3.2), we see that the functions $m\mapsto C_{\mathscr{A}}(K,m,1-X)/m$ and $j\mapsto(b_H(j)-b_F(j))$ are of the form $(1\star r)(m)/m$, respectively $(\mu\star(s_H-s_F))(j)/j$. Hence

$$n\sum_{jm=n}\frac{C_{\mathscr{A}}(K,m,1-X)}{m}(b_H(j)-b_F(j)) = \sum_{td=n} r(t)\big(s_H(d)-s_F(d)\big).$$

We replace $r(t)$ by its value to conclude that this sum is $C_{\mathscr{A}}(K,m,F/H)$, as defined by (1.4). We have reached

$$\prod_{\substack{p\ge P,\\ p+q\mathbb{Z}\in\mathcal{A}}} \frac{F(1/p^s)}{H(1/p^s)} = \prod_{n\ge\Delta}\prod_{K\in\mathscr{G}}\Big(\prod_{\chi\in K^\perp} L_P(ns,\chi)\Big)^{\frac{C_{\mathscr{A}}(K,n,F/H)}{n}}. \tag{3.7}$$

The final task is to control the tail of this product, but prior to that, we change the variable n in (3.7) in m again. To control the tail, we check that, by Lemma 2.5,

$$\begin{aligned}
\pm\log \prod_{m\geq M+1}\prod_{K\in\mathscr{G}}\Big(\prod_{\chi\in K^\perp} L_P(ms,\chi)\Big)^{\frac{C_{\mathscr{A}}(K,m,F/H)}{m}} &\\
&\leq \sum_{m\geq M+1}\sum_{K\in\mathscr{G}}\frac{|C_{\mathscr{A}}(K,m,F/H)|}{m}|G/K|\frac{ms-1+P}{P^{ms}}\\
&\leq \sum_{m\geq M+1}\sum_{K\in\mathscr{G}}\sum_{t|m}\mu^2(t)|\mathscr{G}|(\deg F+\deg H)\beta^{m/t}\frac{ms-1+P}{mP^{ms}}\\
&\leq (\deg F+\deg H)|\mathscr{G}|^2\sum_{m\geq M+1}\frac{\beta^m}{1-(1/\beta)}\frac{s+P}{P^{ms}}\\
&\leq (\deg F+\deg H)|\mathscr{G}|^2\frac{\beta(s+P)}{\beta-1}\frac{1}{1-(\beta/P^s)}\Big(\frac{\beta}{P^s}\Big)^{M+1}\\
&\leq 4(\deg F+\deg H)|\mathscr{G}|^2(s+P)\Big(\frac{\beta}{P^s}\Big)^{M+1}.
\end{aligned}$$

□

4. Link with two other sets of inequalities

In this section, we develop some elements that are contiguous to our topic.

A formula.

Lemma 4.1. *Let $q>1$ be a modulus. We set G_0 to be a subgroup of $G=(\mathbb{Z}/q\mathbb{Z})^\times$ and $G_0^\perp$ be the subgroup of characters that take the value 1 on G_0. For any integer b, we define $\langle b\rangle$ to be the subgroup generated by b modulo q. We have*

$$\prod_{\chi\in G_0^\perp} L_P(s,\chi)=\prod_{G_0\subset K\subset G}\prod_{\substack{p\geq P,\\ \langle p\rangle G_0=K}}\Big(1-p^{-|K/G_0|s}\Big)^{-|G/K|}.$$

The right-hand side of this formula contains products of the kind we seek and, if we were to start from such a set of formulas, the problem would be to *invert* them in some sense.

Proof. We note that $\prod_{\chi\in G_0^\perp}(1-\chi(p)z)^{\chi(a)}=\prod_{\psi\in\hat{L}}(1-\psi(p)z)^{f(\psi)}$ when $\langle p\rangle=L$ and where

$$f(\psi)=\sum_{\substack{\chi\in G_0^\perp,\\ \chi|L=\psi}}\chi(a). \tag{4.1}$$

The condition $\chi\in G_0^\perp$ can also be written as $\chi|G_0=1$, hence we can assume that $\psi|(L\cap G_0)=1$. We write

$$\prod_{\chi\in G_0^\perp}(1-\chi(p)z)^{\chi(a)}=\prod_{\substack{\psi'\in\widehat{LG_0},\\ \psi'|G_0=1}}(1-\psi(p)z)^{f'(\psi')},$$

where

$$f'(\psi') = \sum_{\substack{\chi \in G_0^{\perp}, \\ \chi|LG_0 = \psi}} \chi(a). \tag{4.2}$$

When a lies outside LG_0, this sum vanishes; otherwise it equals $|G/(LG_0)|\psi'(a)$. The characters of LG_0 that are trivial on G_0 are canonically identified with the characters of the cyclic group $(LG_0)/G_0$. We thus have

$$\prod_{\substack{\psi' \in \widehat{LG_0}, \\ \psi'|G_0 = 1}} (1 - \psi(p)z) = 1 - z^{|(LG_0)/G_0|},$$

and this proves our formula. □

Notes on the scope of Lemma 4.1. From a metholodogical viewpoint, a moment's thought discloses that two residue classes modulo q that fall inside the same lattice-invariant class cannot be distinguished by the set of identities of Lemma 4.1. This implies that we indeed extract the maximum information from our setting. This could be formalized in the following manner: consider the vector space $\mathscr{F}[G]$ of functions from G to $\mathbb{C}$, and the sub-space generated by $(\mathbf{1}_{G_0})_{G_0 \in \mathscr{G}}$. This subspace is clearly included in the subspace generated by $(\mathbf{1}_{\mathcal{A}})_{\mathcal{A} \in G^\sharp}$. These two spaces can be shown to be equal. We end this discussion here, as we do not need this fact.

Link with abelian field theory. The case $G_0 = \{1\}$ in the identity of Lemma 4.1 is classical in Dedekind zeta function theory for the field $\mathbb{Q}(\zeta_q)$, where $\zeta_q = \exp(2i\pi/q)$, and can be found in [13, Proposition 13] in a rephrased form. For the general case, we follow [11, Chapter 8] by Narkiewicz. The Dedekind zeta-function associated with an abelian field K is given by

$$\zeta_K(s) = \prod_{\chi \in X(K)} L(s, \chi) \tag{4.3}$$

as per [11, Theorem 8.6]. The group $X(K)$ is the group of characters attached to K, see [11, Proposition 8.4]. This equality (4.3) is proved prime per prime, and we can restrict to ideals whose norm is prime to some integer. In particular, we can restrict it to the primes that are prime to q, which excludes at least the ramified primes. Let $H_q(K)$ be the subgroup of the integers $r \mod q$ that are such that the automorphism of $\mathbb{Q}(\zeta_q)$ defined by $\zeta_q \mapsto \zeta_q^r$ is the identity on K. The sets $X(K)$ and $H_q(K)^\perp$ are almost equal: $X(K)$ is made only of primitive characters associated to the characters in $H_q(K)^\perp$. We may select $G_0 = H_q(K)$ in Lemma 4.1. Some work involving the decomposition law in abelian number fields, which may for instance be found in [11, Theorem 8.2], gives us, when the prime factors of q are all at most P, that

$$\prod_{\chi \in X(K)} L_P(s, \chi) = \prod_{H_q(K) \subset K \subset G_q} \prod_{\substack{p \geq P, \\ \langle p \rangle H_q(K) = K}} \left(1 - p^{-|K/H_q(K)|s}\right)^{-|G_q/K|}.$$

The proof we provide of Lemma 4.1 is much simpler, but the above analysis establishes that the identities stemming from both approaches are the same.

5. Timing and implementation notes

Let $s > 1$ be a real number and $P \geq 2$ be a parameter. We consider the vector, for any positive integer t:

$$\Gamma_{P,s}(t) = \Big(\log \prod_{\chi \in G_0^\perp} L_P(ts, \chi)\Big)_{G_0 \in \mathscr{G}}. \tag{5.1}$$

The rows of $\Gamma_{P,s}(t)$ are indexed by the cyclic subgroups of G. An approximate value of this vector is provided by the function `GetGamma` of the script `LIEP.sage` from the values of the Hurwitz zeta function. We next define

$$V_s(t) = \big(\log \zeta_P(ts; q, \mathcal{A})\big)_{\mathcal{A} \in G^\sharp}. \tag{5.2}$$

The rows of $V_s(t)$ are indexed by classes. We also define

$$\Gamma_{P,s}(t) = \Big(\log \prod_{\chi \in K^\perp} L_P(ts, \chi)\Big)_{K \in \mathscr{G}}. \tag{5.3}$$

The function `GetLatticeInvariantClasses` of the script `LIEP.sage` gives the two lists: the one of the cyclic subgroups and the one of their generators, ordered similarly and in increasing size of the subgroups.

The algorithm (function `GetVs`):

Input. Input the four parameters `q`, `s`, `nbdecimals` and `bigP` as well as the two parameters that control the output `Verbose` and `WithLaTeX`.

Precomputation-1. Compute and store the algebraic quantities that we need: the tuple of cyclic subgroups of $G = (\mathbb{Z}/q\mathbb{Z})^\times$, the tuple of its lattice-invariant classes, the exponent of G, its character group, an enumeration of the elements of G and, for each cyclic subgroup of G, the set of characters of G that are trivial on it. This is done by the function `GetStructure`.

Initialization. Find `M` so that the right-hand side of (1.6) is less than $10^{-\texttt{nbdecimals}-10}$.

Precomputation-2. Build the set $\mathscr{M}$ of integers m such that $m \leq M$ and all the prime factors of m divide q. Then compute the constants $(C_{\mathscr{A}}(K, m, 1-X))$ for every possible class $\mathscr{A}$ and every m in $\mathscr{M}$.

Main Loop. For $m \in \mathscr{M}$, add the contribution of this index to the sum approximating $V_s(1)$ from the right-hand side of (1.5) with $P = \texttt{bigP}$.

Post-computation. Complete the products with the values for primes $p < \texttt{bigP}$.

Output. Return the tuple of lattice-invariant classes and the tuple of couples of lower/upper bounds for the wanted Euler products.

Once the script is loaded via `load('LIEP.sage')`, a typical call will be

```
GetVs(12, 2, 100, 110)
```

to compute modulo 12 the possible constants with $s = 2$, asking for 100 decimal digits and using $P = 110$. The output is self explanatory. The number of decimal digits asked for is roughly handled and one may lose precision in between, but this is indicated at the end. Note that we expect the final result to be of size roughly

unity, so what we ask for is not the relative precision but the number of decimals. Hence, in the function `GetGamma`, we replace by an approximation of 0 the values that we know are insignificantly small. This is a true time-saver.

There are two subsequent optional parameters `Verbose` and `WithLaTeX`. The first one may take the values 0, 1 and 2; when equal to 0, the function will simply do its job and return the tuple of the invariant classes and the one of the computed lower and upper values. When equal to 1, the time taken will also be printed. And when equal to 2, its default value, some information on the computation is given. When the parameter `Verbose` is at least 2 and `WithLaTeX` is 1, the values of the constants will be further presented in a format suitable for inclusion in a LaTeX-file. The digits presented in LaTeX-format when `WithLaTeX` $= 1$ are always accurate. For instance, the call `GetVs(12, 2, 100, 100, 2, 1)` is the one used to prepare the addendum [2] in which we give the first hundred decimal digits of every Euler product over a lattice invariant class when the modulus is at most 16.

The computations of the Euler products of Theorem 1.2 (with $P = 2$, the parameter `bigP` being used to decide from which point onwards we use the usual Euler product or the expression of the theorem) is implemented in:
`GetEulerProds(q, s, F, H, nbdecimals, bigP = 100, Verbose = 2, WithLaTeX = 0)`.
The parameter `bigP` may be increased by the script to ensure that $P \geq 2\beta$ (a condition that is usually satisfied). We reused the same structure as the one for the function `GetVs` except that the set of indices m is now a full interval. Since the coefficients $|b_F(j) - b_G(j)|$ may increase like β^j, we increase the working precision by $J \log \beta / \log 2$.

Checking. The values given here have been checked in several ways. The co-authors of this paper have run several independent scripts. We also provide the function `GetVsChecker(q, s, borne = 10000)` which computes approximate values of the same Euler products by simply truncating the Euler product representation. We checked with positive result the stability of our results with respect of the variation of the parameter P. This proved to be a very discriminating test.

Furthermore, approximate values for Shanks' and Lal's constants are known (Finch in [4] gives 10 digits) and we agree with those. Finally, the web site [7] by X. Gourdon and P. Sebah, or the attached postscript file on the same page, gives in section 4.4 the first fifty digits of the constant they call A and which are

$$\frac{\pi^2}{2} \prod_{p \equiv 1[4]} \left(1 - \frac{4}{p}\right) \left(\frac{p+1}{p-1}\right)^2 = 1.95049\,11124\,46287\,07444\,65855\,65809\,55369\,25267\,08497\,71894\,30550\,80726\,33188\,94627\,61381\,60369\,39924\,26646\,98594\,38665 \cdots$$

Our result matches that of [7].

Some observations on the running time and complexity. We tried several large computations to get an idea of the limitations of our script with the choice $s = 2$ in Corollary 1.8. We present five tables:

- A first table for $3 \leq q \leq 100$ with the uniform choice $P = 100$ and asking for 100 decimal digits.
- Three further tables obtained with the choice $P = 200$ and asking for a thousand decimal digits. The cases retained are $q \leq 16$, $91 \leq q \leq 100$ and $200 \leq q \leq 220$. This last interval contains the first integer q such that $r = \omega(\varphi(q)) = 4$, namely $q = 211$.

- And finally a table for $q \in \{3, 5\}$ and asking for 5000 decimal digits. The running time is given with different choices of the parameter P.

Since we did not run each computation hundred times to get an average timing, these tables have to be taken with a pinch of salt. The processor was an Intel Core i5-2500 at 3.30 GHz. The first half of Table 1 may be reproduced with the call:

```
TablePerformance(3, 51, 100, 100)
```

In these tables, $r = \omega(\varphi(q))$ is the number of distinct prime divisors of q as in Corollary 1.8. The time is given in tenth of a second, indicated by "s/10". The column with the tag "$\#m's$" contains the number of indices $m \leq M$ such that $m|\varphi(q)^\infty$. We otherwise follow the notation of Theorem 1.2.

It seems likely, when looking at Tables 1, 2, 3 and 4 that the number of values of the Hurwitz zeta-function to be computed is the main determining factor of the time consumption. This number is controlled by $\varphi(q)$, since this is the number of characters, and by the number of m's required, a value that is on the whole controlled by $r = \omega(\varphi(q))$

Table 5 gives some data about the running time when asking for 5000 decimal digits, which essentially sets the horizon of the present method. The time is counted in minutes.

References

1. H. Cohen, *High precision computations of Hardy-Littlewood constants*, preprint (1996), 1–19.
2. Salma Ettahri, Olivier Ramaré, and Léon Surel, *Some Euler Products*, Preprint (2020), 4p, Addendum to 'Fast multi-precision computation of some Euler products'.
3. Jan-Hendrik Evertse, *On sums of S-units and linear recurrences*, Compositio Math. **53** (1984), no. 2, 225–244. MR 766298
4. Steven R. Finch, *Mathematical constants*, Encyclopedia of Mathematics and its Applications, vol. 94, Cambridge University Press, Cambridge, 2003. MR 2003519
5. P. Flajolet and I. Vardi, *Zeta function expansions of classical constants*, preprint (1996), 1–10.
6. Étienne Fouvry, Claude Levesque, and Michel Waldschmidt, *Representation of integers by cyclotomic binary forms*, Acta Arith. **184** (2018), no. 1, 67–86. MR 3826641
7. X. Gourdon and P. Sebah, *Constants from number theory*, `http://numbers.computation.free.fr/Constants/constants.html` (2010).
8. M. Lal, *Primes of the form $n^4 + 1$*, Math. Comp. **21** (1967), 245–247. MR 0222007
9. P. Moree, *Approximation of singular series constant and automata. with an appendix by gerhard niklasch.*, Manuscripta Matematica **101** (2000), no. 3, 385–399.
10. Pieter Moree, *On the average number of elements in a finite field with order or index in a prescribed residue class*, Finite Fields Appl. **10** (2004), no. 3, 438–463. MR 2067608
11. W. Narkiewicz, *Elementary and analytic theory of algebraic numbers*, third ed., Springer Monographs in Mathematics, Springer-Verlag, Berlin, 2004. MR 2078267 (2005c:11131)
12. OEIS Foundation Inc., *The on-line encyclopedia of integer sequence*, 2019, `http://oeis.org/`.
13. Jean-Pierre Serre, *Cours d'arithmétique*, Collection SUP: "Le Mathématicien", vol. 2, Presses Universitaires de France, Paris, 1970. MR 0255476
14. D. Shanks, *On the conjecture of Hardy & Littlewood concerning the number of primes of the form $n^2 + a$*, Math. Comp. **14** (1960), 320–332. MR 0120203
15. ———, *On numbers of the form $n^4 + 1$*, Math. Comput. **15** (1961), 186–189. MR 0120184
16. ———, *The second-order term in the asymptotic expansion of $B(x)$*, Math. Comp. **18** (1964), 75–86. MR 0159174
17. ———, *Lal's constant and generalizations*, Math. Comp. **21** (1967), 705–707. MR 0223315
18. L. Tóth, *Menon's identity and arithmetical sums representing functions of several variables*, Rend. Semin. Mat. Univ. Politec. Torino **69** (2011), no. 1, 97–110. MR 2884710
19. László Tóth, *On the number of cyclic subgroups of a finite Abelian group*, Bull. Math. Soc. Sci. Math. Roumanie (N.S.) **55(103)** (2012), no. 4, 423–428. MR 2963406
20. A. J. van der Poorten and H. P. Schlickewei, *Zeros of recurrence sequences*, Bull. Austral. Math. Soc. **44** (1991), no. 2, 215–223. MR 1126359

q	$\varphi(q)$	r	$\#m's$	$\lvert G^\sharp\rvert$	M	time s/10	q	$\varphi(q)$	r	$\#m's$	$\lvert G^\sharp\rvert$	M	time s/10
3	2	1	5	2	26	51	52	24	2	11	12	26	13
4	2	1	5	2	26	1	53	52	2	6	6	26	17
5	4	1	5	3	26	2	55	40	2	9	12	26	19
7	6	2	11	4	26	3	56	24	2	11	16	26	14
8	4	1	5	4	26	1	57	36	2	11	12	26	20
9	6	2	11	4	26	3	59	58	2	5	4	26	17
11	10	2	9	4	26	4	60	16	1	5	12	26	5
12	4	1	5	4	26	1	61	60	3	16	12	26	52
13	12	2	11	6	26	6	63	36	2	11	20	26	22
15	8	1	5	6	26	2	64	32	1	5	10	26	9
16	8	1	5	6	26	2	65	48	2	11	20	26	30
17	16	1	5	5	26	4	67	66	3	13	8	26	47
19	18	2	11	6	26	9	68	32	1	5	10	26	10
20	8	1	5	6	26	2	69	44	2	7	8	26	17
21	12	2	11	8	26	6	71	70	3	11	8	26	44
23	22	2	7	4	26	7	72	24	2	11	16	26	14
24	8	1	5	8	26	2	73	72	2	11	12	26	47
25	20	2	9	6	26	8	75	40	2	9	12	26	19
27	18	2	11	6	26	9	76	36	2	11	12	26	20
28	12	2	11	8	26	6	77	60	3	16	16	26	53
29	28	2	7	6	26	9	79	78	3	12	8	26	53
31	30	3	16	8	26	22	80	32	1	5	20	26	11
32	16	1	5	8	26	4	81	54	2	11	8	26	31
33	20	2	9	8	26	9	83	82	2	5	4	26	25
35	24	2	11	12	26	13	84	24	2	11	16	26	14
36	12	2	11	8	26	6	85	64	1	5	18	26	25
37	36	2	11	9	26	19	87	56	2	7	12	26	24
39	24	2	11	12	26	13	88	40	2	9	16	26	21
40	16	1	5	12	26	5	89	88	2	7	8	26	40
41	40	2	9	8	26	17	91	72	2	11	30	26	54
43	42	3	14	8	26	28	92	44	2	7	8	26	16
44	20	2	9	8	26	8	93	60	3	16	16	26	54
45	24	2	11	12	26	12	95	72	2	11	18	26	50
47	46	2	6	4	26	14	96	32	1	5	16	26	10
48	16	1	5	12	26	5	97	96	2	11	12	26	70
49	42	3	14	8	26	29	99	60	3	16	16	26	52
51	32	1	5	10	26	9	100	40	2	9	12	26	19

TABLE 1. Time used when asking for 100 digits

21. E. Witt, *Treue Darstellung Liescher Ringe*, J. Reine Angew. Math. **177** (1937), 152–160. MR 1581553

AIX MARSEILLE UNIV, CNRS, CENTRALE MARSEILLE, I2M, MARSEILLE, FRANCE
Email address: salma.ettahri@etu.univ-amu.fr

CNRS / AIX MARSEILLE UNIV. / CENTRALE MARSEILLE, I2M, MARSEILLE, FRANCE
Email address: olivier.ramare@univ-amu.fr

AIX MARSEILLE UNIV, CNRS, CENTRALE MARSEILLE, I2M, MARSEILLE, FRANCE
Email address: leon.surel@etu.univ-amu.fr

q	$\varphi(q)$	r	$\#m's$	$\lvert G^\sharp\rvert$	M	Time (s/10)
3	2	1	8	2	218	10
4	2	1	8	2	218	7
5	4	1	8	3	218	14
7	6	2	26	4	218	69
8	4	1	8	4	218	12
9	6	2	26	4	218	67
11	10	2	19	4	218	81
12	4	1	8	4	218	14
13	12	2	26	6	218	135
15	8	1	8	6	218	26
16	8	1	8	6	218	24

TABLE 2. Time used when asking for 1000 digits for $q \leq 16$

q	$\varphi(q)$	r	$\#m's$	$\lvert G^\sharp\rvert$	M	Time (s/10)
91	72	2	26	30	219	910
92	44	2	14	8	218	286
93	60	3	47	16	219	1388
95	72	2	26	18	218	912
96	32	1	8	16	218	114
97	96	2	26	12	218	1257
99	60	3	47	16	219	1399
100	40	2	19	12	218	363

TABLE 3. Time used when asking for 1000 digits for $90 < q \leq 100$

q	$\varphi(q)$	r	$\#m's$	$\lvert G^\sharp\rvert$	M	Time (s/10)
200	80	2	19	24	218	759
201	132	3	37	16	218	2543
203	168	3	42	24	219	3767
204	64	1	8	20	218	240
205	160	2	19	28	219	1573
207	132	3	37	16	218	2520
208	96	2	26	40	219	1259
209	180	3	47	24	219	4552
211	210	4	69	16	219	8406
212	104	2	14	12	218	743
213	140	3	31	16	218	2271
215	168	3	42	24	219	3807
216	72	2	26	24	219	930
217	180	3	47	40	219	4517
219	144	2	26	24	219	1970
220	80	2	19	24	218	753

TABLE 4. Time used when asking for 1000 digits for $200 \leq q \leq 220$

q	P	time
3	200	80m
3	400	35m
3	500	35m
5	500	72m
5	1000	70m
5	5000	72m

TABLE 5. Time used when asking for 5000 digits