FAST MULTI-PRECISION COMPUTATION OF SOME EULER PRODUCTS

S. ETTAHRI, O. RAMARÉ, AND L. SUREL

ABSTRACT. (File LoeschianConstant-16-Arxiv.tex) For every modulus $q \geqslant 3$, we define a family of subsets $\mathcal{A}$ of the multiplicative group $(\mathbb{Z}/q\mathbb{Z})^\times$ for which the Euler product $\prod_{p \bmod q \in \mathcal{A}}(1-p^{-s})$ can be computed in double exponential time, where $s > 1$ is some given real number. We provide a Sage script to do so, and extend our result to compute Euler products $\prod_{p\in\mathcal{A}} F(1/p)/G(1/p)$ where F and G are polynomials with real coefficients, when this product converges absolutely. This enables us to give precise values of several Euler products intervening in Number Theory.

1. INTRODUCTION

At the beginning of our query lie two constants that appear in the paper [2] by É. Fouvry, C. Levesque and M. Waldschmidt. On following this paper, they are

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

and

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

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 sequence A003136 of [10]) is given by

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

This accounts for our interest in the first constant. The second one occurs because the number of Loeschian numbers that are also sums of two squares (see sequence A301430 of [10]) is given by

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

The question we address here is devising a fast manner to compute the intervening Euler products. From sequence A301429 of [10], we know that $\alpha_0^{(3)} = 0.638909\ldots$ but we would like (much!) more digits. Similarly it is known that $\beta_0 = 0.30231614235\ldots$.

Theorem 1.1. *We have*

$$\begin{aligned}\alpha_0^{(3)} = 0.&63890\,94054\,45343\,88225\,49426\,74928\,24509\,37549\,75508\,02912\\ &33454\,21692\,36570\,80763\,10027\,64965\,82468\,97179\,11252\,86643\cdots\end{aligned}$$

Date: August 18th 2019.

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

and

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

Our method is more general and allows one to compute Euler products of the shape

$$\prod_{p\in\mathcal{A}\bmod q}(1-p^{-s})^{-1}$$

for any s with $\Re s > 1$ and some subsets $\mathcal{A}$ of $(\mathbb{Z}/q\mathbb{Z})^\times$. We use a set of identities that lead to fast convergent formulae. The use of a similar formula for scientific computations can be found in [14, equation (15)] by D. Shanks. This author's approach has been put in a general context by P. Moree & D. Osburn in [7, equation (3.2)]. On looking closely, we see that an accurate value of $\alpha_0^{(3)}$ already follows from this paper. The formulae we prove have a wider reach, though they fail to exhaust the problem. The reader may want to read subsection 2.2 now to understand the initial idea. In the simplest form, we produce a formula that links for instance $\zeta(s;12,1) = \prod_{p\equiv 1[12]}(1-p^{-s})^{-1}$ to $\zeta(2s;12,1)$. We then reuse this formula to change $2s$ in $4s$, and so on, and we finally use $\zeta(2^r s;12,1) = 1+\mathcal{O}(1/2^{s2^r})$. This is analogous to D. Shanks scheme in [14]. In the general case however, we link values at s with values at ds for some $d>1$, but these values are not the one of the same function, but of some *companion* functions. This means that we have to work simultaneously with several players. Let us first define these *companions*, which are all the products we propose to compute.

When K is a cyclic subgroup of $(\mathbb{Z}/q\mathbb{Z})^\times$, we denote by $A(K)$ the set of elements x from $(\mathbb{Z}/q\mathbb{Z})^\times$ such that the subgroup $\langle x\rangle$ generated by x is equal to K. We note that the sets $A(K)$, when K ranges though the set of cyclic subgroups of $(\mathbb{Z}/q\mathbb{Z})^\times$, determine a partition of $(\mathbb{Z}/q\mathbb{Z})^\times$. A subset $\mathcal{A}$ of $(\mathbb{Z}/q\mathbb{Z})^\times$ is said to be a *lattice-invariant* class if it is of the form $A(K)$ for some cyclic subgroup K of $(\mathbb{Z}/q\mathbb{Z})^\times$, i.e. if all its elements generate the same subgroup (see Definition 3.1 below). Here is a consequence of our approach.

Theorem 1.2. *Let q be some modulus and $\mathcal{A}$ be a* lattice-invariant *class of $(\mathbb{Z}/q\mathbb{Z})^\times$. For every $s>1$, the product*

$$\zeta(s;q,\mathcal{A}) = \prod_{p \bmod q\in\mathcal{A}}(1-p^{-s})^{-1}$$

can be computed in double-exponential time.

This theorem applies in particular to $\mathcal{A}=\{1\}$ and to $\mathcal{A}=\{-1\}$ and this is enough to compute β_0 and $\alpha_0^{(3)}$. The last section contains numerical examples. The material of this paper has been used to write the script

`LatticeInvariantEulerProducts-02.sage`

which we shorten below in `LIEP.sage` and which can be found on the second author website. We give some details about this script when developing the proof below.

We produce in Proposition 7.3 an explicit expression for the number $|G^\sharp| = |\mathscr{G}|$ of lattice-invariant classes. Though our formula is only a sum of non-negative summands that are multiplicative expressions, its order of magnitude is not obvious when q has numerous prime factors. We have for instance not been able to establish that $|G^\sharp| \ll_\epsilon q^\epsilon$ (for every positive ϵ) though this was our initial guess.

Notation. When $\mathcal{A}$ is a subset of $(\mathbb{Z}/q\mathbb{Z})^\times$, we define $\langle\mathcal{A}\rangle$ to be the (multiplicative) subgroup generated by $\mathcal{A}$, and when $\mathcal{A}=\{a\}$, we may shorten $\langle\{a\}\rangle$ in $\langle a\rangle$.

When additionally $P \geqslant 2$ is some real parameter, we define

$$\zeta(s;q,\mathcal{A}) = \prod_{\substack{p \bmod q \in \mathcal{A},\\ p\geqslant P}} (1-p^{-s})^{-1}. \tag{4}$$

This is in accordance with the notation of Theorem 1.2. We define further

$$L_P(s,\chi) = \prod_{p\geqslant P} (1-\chi(p)/p^s)^{-1}. \tag{5}$$

Precise statement of the main result. Let $q > 1$ be a modulus. Let G_0 be a subgroup of $G = (\mathbb{Z}/q\mathbb{Z})^\times$ and let $G_0^\perp$ be the subgroup of characters that take the value 1 on G_0. Let $s > 1$ be a real number and $P \geqslant 2$ be a parameter. We shall compute directly the contribution of the primes $< P$. We define, for any positive integer t:

$$\gamma_s(G_0,t) = \log \prod_{\chi\in G_0^\perp} L_P(ts,\chi). \tag{6}$$

The parameter P has disappeared from our notation and the reader may stick with $P = 2$. When s is a real number, the number $\prod_{\chi\in G_0^\perp} L_P(ts,\chi)$ is indeed a positive real number because, when χ belongs to $G_0^\perp$, so does $\overline{\chi}$.

We denote the set of *lattice-invariant* classes by $G^\sharp$ and the set of cyclic subgroups of G by $\mathscr{G}$. Both sets are in an obvious one-to-one correspondence. We consider the vector

$$\Gamma_s(t) = (\gamma_s(G_0,t))_{G_0\in\mathscr{G}}. \tag{7}$$

The rows of $\Gamma_s(t)$ are indexed by cyclic subgroups of G. It is computed by the function `GetGamma` of the script `LIEP.sage` from the values of the Hurwitz zeta function. See the implementation notes below. We next define

$$V_s(t) = \big(\log \zeta_P(s;q,\mathcal{A})\big)_{\mathcal{A}\in G^\sharp}. \tag{8}$$

The rows of $V_s(t)$ are indexed by classes. We control the size of our vectors with the norm

$$\|W\| = \max_i |W_i| \tag{9}$$

when W is the vector of coordinates W_i. We define the square matrix M_1^{-1} by

$$M_1^{-1}\big|_{i=\mathcal{A},j=K} = \begin{cases} \mu(|\langle\mathcal{A}\rangle/K|)/|G/K| & \text{when } K\subset\langle\mathcal{A}\rangle,\\ 0 & \text{otherwise}\end{cases} \tag{10}$$

where $\mathcal{A}$ ranges $G^\sharp$ while K ranges $\mathscr{G}$. It is unusual to define a matrix by its inverse. In the natural course of the proof, a matrix M_1 will occur, whose inverse is the one above; it is computed in Proposition 4.1. The reader will readily check that there are no circularity in our definitions. Let us recall that the *exponent* of G is the maximal order of an element in G and is denoted by $\exp G$. To each divisor $d > 1$ of $\exp G$, we associate the square matrix N_d whose columns and rows are indexed by cyclic subgroups of G and whose entries are given by

$$N_d\big|_{i=B_0,j=B_1} = \sum_{\substack{K\subset B_0,\\ |KB_1/K|=d}} \mu(|B_0/K|). \tag{11}$$

The sum is over subgroups K. The condition $|KB_1/K| = d$ can be replaced by the condition $|B_1/K\cap B_1| = d$. Here is our main theorem.

Theorem 1.3. *For any integer $r \geqslant 2$, we have*

$$(12)\quad \left\| V_s(1) - \sum_{0\leqslant v\leqslant r-1} (-1)^v \sum_{d_1\cdots d_v\leqslant 2^r} \frac{N_{d_1}}{d_1}\cdots\frac{N_{d_v}}{d_v} M_1^{-1}\Gamma_s(d_1\ldots d_v)\right\| \leqslant \frac{1}{2}\left(1+\frac{r-1}{|G^\sharp|}\right)\left(\frac{|G^\sharp|d(\exp G)}{2}\right)^{r-1}\frac{1+P/(s2^r-1)}{P^{s2^r}}$$

where $d_1,\ldots,d_r$ are all divisors of $\exp G$ excluding 1.

When $v=0$, we use $d_1\ldots d_v = 1$ and $N_{d_1}\cdots N_{d_v} = \mathrm{Id}$. We provide in Section 5 the numerical datas modulo 7 that will enable the reader to follow the proof step by step in this case. This example may also be used to check our routines.

Extending the computations. Now that we know how to compute some Euler products $\zeta_P(s;q,\mathcal{A})$ in a fast manner, we can extend these computations to more general Euler products, though still on the same sets of primes. To do so, we add a definition:

$$(13)\quad (\log\zeta_P(s;q,\mathcal{A}|r))_{\mathcal{A}\in G^\sharp} = \sum_{0\leqslant v\leqslant r-1}(-1)^v\sum_{d_1\cdots d_v\leqslant 2^r}\frac{N_{d_1}}{d_1}\cdots\frac{N_{d_v}}{d_v}M_1^{-1}\Gamma_s(d_1\ldots d_v)$$

Theorem 1.4. *Let $F, G\in\mathbb{R}[X]$ be two coprime polynomials satisfying $F(0) = G(0) = 1$ such that $(F(X)-G(X))/X^2\in\mathbb{R}[X]$. Let $\beta\geqslant 2$ be an upper bound for the maximum modulus of the inverses of the roots of F and of G. Let $P\geqslant 2\beta$ be a parameter. Then, for any parameters $J\geqslant 3$ and $r\geqslant 2$, we have*

$$\prod_{\substack{p\geqslant P,\\ p\in\mathcal{A}}}\frac{F(1/p)}{G(1/p)} = \prod_{2\leqslant j\leqslant J}\zeta_P(j;q,\mathcal{A}|r)^{b_G(j)-b_F(j)}\times I,$$

where the integers $b_G(j)$ and $b_F(j)$ are defined in Lemma 6.1 and

$$|\log I| \leqslant \max(\deg F,\deg G)\left(\left(\frac{|G^\sharp|d(\exp G)}{2}\right)^{r-1}\frac{r\beta^2}{P^{2^{r+1}}}(1+2^{-r}P)+\frac{4\beta^{J+1}}{JP^J}\right).$$

Remark 1.5. Inequality (39) gives a more precise bound for $|\log I|$ which we will use in the actual script.

Remark 1.6. Lemma 6.3 ensures that we may select

$$\beta = \max\Big(1, \sum_{1\leqslant k\leqslant \deg F}|a_k|, \sum_{1\leqslant k\leqslant\deg G}|b_k|\Big)$$

when $F(X) = 1 + a_1X + \ldots + a_\delta X^\delta$ and $G = 1 + b_1X + \ldots + b_{\delta'}X^{\delta'}$.

Remark 1.7. The function `GetEulerProds(q, F, G, nbdecimals)` gives all these Euler products. The polynomials F and G are to be given as polynomial expressions with the variable x.

D. Shanks in [15] (resp. [16], resp. [17]) has already been able to compute an Euler product over primes congruent to 1 modulo 8 (resp. to 1 modulo 4, resp. 1 modulo 8), by using an identity (Lemma of section 2 for [15], equation (5) in [16] and the Lemma of section 3 in [17]) that is a precursor of our Lemma 6.1.

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 interval arithmetic package at that time, the relative weakness of the computers and the absence of a proper study concerning the error term. We thus complement these results by giving the first hundred decimals.

Corollary 1.8 (Shank's Constant)**.** *We have*

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

And thus Shank's constant satisfies

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

As explained in [16], the number of primes $\leqslant X$ of the form m^4+1 is conjectured to be asymptotic to $I\cdot X^{1/4}/\log X$. The name "Shank's Constant" comes from Chapter 2, page 90 of [1]. When using the script that we introduce below, this value is obtained with the call

GetEulerProds(8, $1-2*x-7*x^2-4*x^3$, $1-2*x+x^2$, 150, 400).

Corollary 1.9 (Lal's Constant)**.** *We have*

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

And thus Lal's constant satisfies

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

As explained in [17], the number of primes $\leqslant X$ of the form $(m+1)^2+1$ and such that $(m-1)^2+1$ is also a prime is conjectured to be asymptotic to $\lambda\cdot X^{1/2}/(\log X)^2$. The name "Lal's Constant" comes from the papers [5] and [17]. When using the script that we introduce below, the first value is obtained with the call

GetEulerProds(8, $1-8*x$, $1-8*x+16*x^2$, 100, 400).

We close this section by mentioning another series of challenging constants. In [8], P. Moree computes inter alia the series of constants A_χ defined six lines after Lemma 3, page 452, by

$$A_\chi = \prod_{p\geqslant 2}\left(1+\frac{(\chi(p)-1)p}{(p^2-\chi(p))(p-1)}\right) \tag{14}$$

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

Thanks. The authors thank M. Waldschmidt for having drawn their attention of this question, P. Moree and É. Fouvry for helpful discussions on how to improve this paper and X. Gourdon for free exchanges concerning some earlier computations.

2. A general mechanism

We start by presenting the mechanism of Shanks in [13] is a general setting.

Lemma 2.1. *Let $\mathcal{P}$ be a set of prime numbers and let f be a function from $\mathcal{P}$ to $\{\pm 1\}$. For every s with $\Re s > 1$, we have*

$$\prod_{\substack{p\in\mathcal{P},\\ f(p)=-1}} (1-p^{-s})^2 = \frac{\prod_{p\in\mathcal{P}}(1-p^{-s})}{\prod_{p\in\mathcal{P}}(1-f(p)p^{-s})} \prod_{\substack{p\in\mathcal{P},\\ f(p)=-1}} (1-p^{-2s}).$$

Proof. The proof is straightforward. We simply write

$$\prod_{\substack{p\in\mathcal{P},\\ f(p)=-1}} \frac{(1-p^{-s})^2}{1-p^{-2s}} = \prod_{\substack{p\in\mathcal{P},\\ f(p)=-1}} \frac{1-p^{-s}}{1+p^{-s}} = \prod_{\substack{p\in\mathcal{P},\\ f(p)=-1}} \frac{1-p^{-s}}{1-f(p)p^{-s}}$$
$$= \prod_{p\in\mathcal{P}} \frac{1-p^{-s}}{1-f(p)p^{-s}}$$

as required. □

Shanks's method is efficient to deal with product of primes belonging to a coset modulo a quadratic character. We generalize it as follows.

Lemma 2.2. *Let $q > 1$ be a modulus. We set G_0 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 the the subgroup generated by b modulo q. We have*

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

and, for any element $a\notin G_0$ of order 2, we have

$$\prod_{\chi\in G_0^\perp} L_P(s,\chi)^{\chi(a)} = \prod_{\substack{G_0\subset K\subset G,\\ a\in K}} \prod_{\substack{p\geqslant P,\\ \langle p\rangle G_0 = K}} \left(\frac{(1-p^{|K/G_0|s/2})^2}{1-p^{-|K/G_0|s}}\right)^{-|G/K|}$$

where $\hat{G}$ is the set of characters of G.

Case $G_0 = \{1\}$ of the first identity is classical in Dedekind zeta function theory, and can be found in [12, Proposition 13] in a rephrased form. Case $a \neq 1$ will not be required for the general theory. It may however lead quickly to efficient formulae.

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

$$f(\psi) = \sum_{\substack{\chi\in G_0^\perp,\\ \chi|H=\psi}} \chi(a). \tag{15}$$

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

$$\prod_{\chi\in G_0^\perp} (1-\chi(p)z)^{\chi(a)} = \prod_{\substack{\psi'\in\widehat{HG_0},\\ \psi'|G_0=1}} (1-\psi(p)z)^{f'(\psi')}$$

where

$$f'(\psi') = \sum_{\substack{\chi\in G_0^\perp,\\ \chi|HG_0=\psi}} \chi(a). \tag{16}$$

When a lies outside HG_0, this sum vanishes; otherwise it equals $|G/(HG_0)|\psi'(a)$. The characters of HG_0 that are trivial on G_0 are canonically identified with the characters of the cyclic group $(HG_0)/G_0$. We thus have

$$\prod_{\substack{\psi'\in\widehat{HG_0},\\ \psi'|G_0=1}}(1-\psi(p)z) = 1 - z^{|(HG_0)/G_0|}$$

and this proves our first formula.

When $a^2\equiv 1[q]$ and $a\notin G_0$, and since $(HG_0)/G_0$ is cyclic, of (even) order h say, the characters are given by $\chi(p^x)=e(cx/h)$ since p is a generator and where c ranges $\{0,\cdots,h-1\}$. We thus have, when $a\in H$,

$$\begin{aligned}\prod_{\psi'\in\widehat{(HG_0)/G_0}}(1-\psi'(p)z)^{\psi'(a)} &= \prod_{c \bmod h}(1-e(c/h)z)^{e(c/2)}\\ &= \prod_{0\leqslant d\leqslant\frac{h-2}{2}}\Big(1-e\Big(\frac{2d}{h}z\Big)\Big)\prod_{0\leqslant d\leqslant\frac{h-2}{2}}\Big(1-e\Big(\frac{2d+1}{h}z\Big)\Big)^{-1}\\ &= \frac{1-z^{h/2}}{1-(e(1/h)z)^{h/2}} = \frac{1-z^{h/2}}{1+z^{h/2}} = \frac{(1-z^{h/2})^2}{1-z^h}.\end{aligned}$$

The reader will readily complete the proof by setting $K = HG_0$. □

2.1. A special case.

Let us select for G_0 the kernel of a given quadratic character χ_1. The subgroup K can take only two values, G_0 or G. We thus get

$$L(s,\chi_1)L(s,\chi_0) = \prod_{\chi_1(p)=1}(1-p^{-s})^2\prod_{\chi_1(p)=-1}(1-p^{-2s})$$

which gets converted into

$$L(s,\chi_1)L(s,\chi_0) = L(s,\chi_0)^2\prod_{\chi_1(p)=-1}(1-p^{-s})^{-2}\prod_{\chi_1(p)=-1}(1-p^{-2s}). \tag{17}$$

Lemma 2.1 can also be used to obtain the same result.

2.2. More details modulo 12.

Here is the character table modulo 12:

	1	5	7	11
$\chi_{0,12}$	1	1	1	1
$\chi_{1,12}$	1	-1	1	-1
$\chi_{2,12}$	1	1	-1	-1
$\chi_{3,12}$	1	-1	-1	1

First Identity. This table enables us to write:

p mod 12	1	5	7	11
$(1-\chi_{0,12}(p)z)$	$1-z$	$1-z$	$1-z$	$1-z$
$(1-\chi_{1,12}(p)z)$	$1-z$	$1+z$	$1-z$	$1+z$
$(1-\chi_{2,12}(p)z)$	$1-z$	$1-z$	$1+z$	$1+z$
$(1-\chi_{3,12}(p)z)$	$1-z$	$1+z$	$1+z$	$1-z$
$\prod_\chi\cdots$	$(1-z)^4$	$(1-z^2)^2$	$(1-z^2)^2$	$(1-z^2)^2$

And thus

$$\prod_\chi L(s,\chi) = \prod_{p\geqslant 5}\frac{1}{(1-p^{-2s})^2}\prod_{\substack{p\geqslant 5,\\ p\equiv 1[12]}}\frac{(1-p^{-2s})^2}{(1-p^{-s})^4},$$

which gives rise to the formula

$$\prod_{\substack{p\geqslant 5,\\ p\equiv 1[12]}}\frac{1}{(1-p^{-s})^4}=\prod_{\substack{p\geqslant 5,\\ p\equiv 1[12]}}\frac{1}{(1-p^{-2s})^2}\frac{\prod_\chi L(s,\chi)}{((1-2^{-2s})(1-3^{-2s})\zeta(2s))^2}.$$

This identity reduces the computation of $\zeta(s;12,1)$ to the one of $\zeta(2s;12,1)$ and we can iterate this formula. Note that we can take the required fourth root as only real numbers are involved, when the terms are properly grouped.

Second Identity. Similarly, we find that

p	1	5	7	11
$(1-\chi_{0,12}(p)z)$	$1-z$	$1-z$	$1-z$	$1-z$
$(1-\chi_{1,12}(p)z)^{-1}$	$(1-z)^{-1}$	$(1+z)^{-1}$	$(1-z)^{-1}$	$(1+z)^{-1}$
$(1-\chi_{2,12}(p)z)^{-1}$	$(1-z)^{-1}$	$(1-z)^{-1}$	$(1+z)^{-1}$	$(1+z)^{-1}$
$(1-\chi_{3,12}(p)z)$	$1-z$	$1+z$	$1+z$	$1-z$
$\prod_\chi \cdots$	1	1	1	$\dfrac{(1-z)^4}{(1-z^2)^2}$

whence

$$\frac{L(s,\chi_{0,12})L(s,\chi_{3,12})}{L(s,\chi_{1,12})L(s,\chi_{2,12})}=\prod_{\substack{p\geqslant 5,\\ p\equiv 11[12]}}\frac{(1-p^{-s})^2}{(1-p^{-2s})},$$

which we finally write in the form

$$\prod_{\substack{p\geqslant 5,\\ p\equiv 11[12]}}\frac{1}{(1-p^{-s})^2}=\frac{L(s,\chi_{0,12})L(s,\chi_{3,12})}{L(s,\chi_{1,12})L(s,\chi_{2,12})}\prod_{\substack{p\geqslant 5,\\ p\equiv 11[12]}}\frac{1}{(1-p^{-2s})^2}.$$

This identity again reduces the computation of $\zeta(s;12,11)$ to the one of $\zeta(2s;12,11)$ and we can iterate this formula. Again, we can take the required fourth rooths as only real numbers are involved, when the terms are properly grouped.

Third Identity. We also find that

p	1	5	7	11
$(1-\chi_{0,12}(p)z)$	$1-z$	$1-z$	$1-z$	$1-z$
$(1-\chi_{1,12}(p)z)^{-1}$	$(1-z)^{-1}$	$(1+z)^{-1}$	$(1-z)^{-1}$	$(1+z)^{-1}$
$(1-\chi_{2,12}(p)z)$	$1-z$	$1-z$	$1+z$	$1+z$
$(1-\chi_{3,12}(p)z)^{-1}$	$(1-z)^{-1}$	$(1+z)^{-1}$	$(1+z)^{-1}$	$(1-z)^{-1}$
$\prod_\chi \cdots$	1	$\dfrac{(1-z)^4}{(1-z^2)^2}$	1	1

whence

$$\frac{L(s,\chi_{0,12})L(s,\chi_{2,12})}{L(s,\chi_{1,12})L(s,\chi_{3,12})}=\prod_{\substack{p\geqslant 5,\\ p\equiv 5[12]}}\frac{(1-p^{-s})^2}{(1-p^{-2s})},$$

We are exactly in the same position as with the second identity. We again finally write in the form

$$\prod_{\substack{p\geqslant 5,\\ p\equiv 5[12]}}\frac{1}{(1-p^{-s})^2}=\frac{L(s,\chi_{0,12})L(s,\chi_{2,12})}{L(s,\chi_{1,12})L(s,\chi_{3,12})}\prod_{\substack{p\geqslant 5,\\ p\equiv 5[12]}}\frac{1}{(1-p^{-2s})^2}.$$

This identity again reduces the computation of $\zeta(s;12,5)$ to the one of $\zeta(2s;12,5)$ and we can iterate this formula. Again, we can take the required fourth rooths as only real numbers are involved, when the terms are properly grouped.

Fourth Identity. We can easily produce a similar formula linking $\zeta(s;12,7)$ to $\zeta(2s;12,7)$ or use the fact that the product $\zeta(s;12,1)\zeta(s;12,5)\zeta(s;12,7)\zeta(s;12,11)$ equals $L(s,\chi_{0,12})$, and thus is known, to infer such a formula from the ones above.

3. Products obtained in general

We want to compute Euler products of the shape $\zeta(s;q,\mathcal{A})$ for $s>1$ and some subset $\mathcal{A}$ of $(\mathbb{Z}/q\mathbb{Z})^\times$. Computing $L(s,\chi)$ is easier as it can be reduced to sums over integers is some arithmetic progressions. Equation (17) reduces in a special case the computations of $\zeta(s;q,\mathcal{A})$ to the one of $\zeta(s;q,\mathcal{A})$, and we can continue the process. We soon reach $\prod_{p\in\mathcal{A} \bmod q}(1-1/p^{2^N s})$ with a large enough N which can be approximated by $1+\mathcal{O}(2^{-2^N s})$. The object of this section is to devise a setting to understand which sums we relate together.

Definition 3.1. *Two elements g_1 and g_2 of the abelian group G are said to be* lattice-invariant *if and only if they generates the same group.*

The map between the set of cyclic subgroups of G and the set of lattice-invariant-*classes which, to a subgroup, associates the subset of its generators, is one-to-one.*

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 subgroup.

Any two elements of $(\mathbb{Z}/q\mathbb{Z})^\times$ equivalent according to it cannot be distinguished by using the formulae of Lemma 2.2. Conversely, the question is to know whether we are indeed able to distinguish each class. To each class $\mathcal{A}$, we attach the enumerable collection of symbols $(x^r_{\mathcal{A}})_{r\geqslant 1}$. We shall replace each of them according to the rule

$$x^r_{\mathcal{A}} \mapsto -\log \prod_{\substack{p+q\mathbb{Z}\in\mathcal{A},\\ p\geqslant P}} \left(1-p^{-rs}\right). \tag{18}$$

We consider the module of finite formal combinations

$$\sum_{\substack{\mathcal{A}\in G^\sharp,\\ r\geqslant 1}} \alpha_{\mathcal{A},r} x^r_{\mathcal{A}}$$

with coefficients $\alpha_{\mathcal{A},r}\in\mathbb{Z}$ and indeterminates $x^r_{\mathcal{A}}$. The superscript r is *not* a power. We consider the following special elements. Let $G_0\subset K\subset G$ be two subgroups such that K/G_0 is cyclic. We define

$$g(G_0,K,t) = \sum_{\mathcal{A}\in G^\sharp, \mathcal{A}G_0=K} x_{\mathcal{A}}^{t|K/G_0|}. \tag{19}$$

With that, we find that

$$\gamma(G_0,t) = \sum_{G_0\subset K\subset G} |G/K| g(G_0,K,t). \tag{20}$$

4. Iterating the formula

The first identity of Lemma 2.2 gives us as many identities as there are subgroups G_0; we know by Definition 3.1 that the number of *lattice-invariant*-classes equals the one of cyclic subgroups. It turns out that it is enough to restrict our attention to cyclic subgroups G_0. Let $\mathscr{G}$ be the subset of such subgroups, which we order by inclusion. On recalling definition (7), we may rewrite (20) in the form

$$\Gamma(t) = \sum_{d||G|} M_d V_s(dt) \tag{21}$$

where (this is the case $K = G_0$)

$$M_1\big|_{i=G_0, j=\mathcal{A}} = \begin{cases} |G/K| & \text{if } \mathcal{A} \subset G_0, \\ 0 & \text{otherwise,} \end{cases} \tag{22}$$

and, where, when $d > 1$ (i.e. $G_0 \subsetneq K$), we have

$$M_d\big|_{i=G_0, j=\mathcal{A}} = \begin{cases} |G/\mathcal{A}G_0| & \text{if } |\mathcal{A}G_0|/|G_0| = d, \\ 0 & \text{otherwise.} \end{cases} \tag{23}$$

Equation (21) gives us a relation between $M_1 V_s(t)$ and $M_d V_s(dt)$ for several d's that are strictly larger than 1. Our roadmap is to invert the matrix M_1 and to iterate this formula. We compute explicitly M_1^{-1} by using some generalised Moebius inversion, which we first put in place.

The Moebius function associated to $\mathscr{G}$. We follow closely the exposition of Rota in [11]. On the algebra of functions f on couples (K, L) of points of $\mathscr{G}$ such that $K \subset L$ (the so-called *incidence algebra*, see [11, Section 3]), we define the convolution product

$$(f \star g)(K, L) = \sum_{K \subset H \subset L} f(K, H) g(H, L).$$

We consider the $\mathscr{G}$-zeta function which is defined by

$$\zeta_{\mathscr{G}}(K, L) = \begin{cases} 1 & \text{when } K \subset L, \\ 0 & \text{otherwise.} \end{cases}$$

This function is shown to be invertible in the above algebra and its inverse is called the $\mathscr{G}$-Moebius function, denoted by $\mu_{\mathscr{G}}$. By definition, we have the two Moebius inversion formulas:

$$\sum_{K \subset H \subset L} f(K, H) = g(K, L) \implies f(K, L) = \sum_{K \subset H \subset L} g(K, H) \mu_{\mathscr{G}}(H, L) \tag{24}$$

and

$$\sum_{K \subset H \subset L} f(H, L) = g(K, L) \implies f(K, L) = \sum_{K \subset H \subset L} \mu_{\mathscr{G}}(K, H) g(H, L). \tag{25}$$

We end this reminder with a formula giving the value of $\mu_{\mathscr{G}}(K, H)$.

Computing $\mu_{\mathscr{G}}(K, H)$. Let $C_p(K, H)$ be the number of chains of length p going from K to H, i.e. the number of $p+1$-uples $K = A_0 \subsetneq A_1 \subsetneq A_2 \subsetneq \ldots \subsetneq A_p = H$. Then (cf [11, Proposition 6])

$$\mu_{\mathscr{G}}(K, H) = \sum_{p \geqslant 0} (-1)^p C_p(K, H). \tag{26}$$

Since the subgroups of a cyclic group are all cyclic, we only have to consider the chains in H/K. There is one and only one subgroup for each divisor of $|H/K|$, and any two such subgroups L_1 and L_2 are included according to whether $|L_1|\big||L_2|$ or not. This transfers the problem on a problem on integers. Let $c_\ell(n)$ be the number of $\ell + 1$-divisibility chains between 1 and n. We have $c_0(n) = 1_{n=1}$ while $c_1(n) = 1_{n \geqslant 2}$ and $c_{p+1}(n) = (c_\ell \star c_1)(n)$. This proves that $c_\ell(n) = d_\ell^*(n)$, the number of p-tuples $(d_1, d_2, \ldots, d_\ell)$ of divisors of n that are such that $d_i \neq 1$ and $d_1 d_2 \cdots d_\ell = n$. We have

$$\sum_{n \geqslant 1} d_\ell^*(n)/n^s = (\zeta(s) - 1)^\ell$$

and thus the generating series of $\sum_{p\geqslant 0}(-1)^p d_\ell^*(n)$ is

$$\sum_{\ell\geqslant 0}(-1)^\ell(\zeta(s)-1)^\ell = \frac{1}{1+\zeta(s)-1} = 1/\zeta(s).$$

We have proved that

$$\mu_{\mathscr{G}}(K,H) = \mu(|H/K|). \tag{27}$$

Inverting the matrix M_1.

Proposition 4.1. *The matrix M_1 is invertible and the coefficients of its inverse are given by*

$$M_1^{-1}\big|_{i=\mathcal{A},j=K} = \begin{cases}\mu(|\langle\mathcal{A}\rangle/K|)/|G/K| & \textit{when } K\subset\langle\mathcal{A}\rangle,\\ 0 & \textit{otherwise.}\end{cases}$$

Proof. We find that

$$M_1V = (|G/K|\sum_{\mathcal{A}\subset K} v_{\mathcal{A}})_K.$$

We replace $\mathcal{A}$ by the subgroup $B=\langle\mathcal{A}\rangle$ it generates. Inverting $f(K)=|G/K|\sum_{B\subset K}v_B$ is done with the Moebius function of $\mathscr{G}$. To do so, simply consider the more general function

$$F(H,K) = |G/K|\sum_{H\subset B\subset K} v^*(H,B) = |G/K|(v^*\star\zeta_{\mathscr{G}})(H,K)$$

where $v^*(H,B)=v_B$. This gets inverted in

$$v^*(H,B) = \sum_{H\subset K\subset B} F(H,K)|G/K|^{-1}\mu_{\mathscr{G}}(K,B)$$

which yield, by specializing $H=\{1\}$

$$v_B = \sum_{K\subset B} f(K)|G/K|^{-1}\mu_{\mathscr{G}}(K,B).$$

We could also have applied [11, Proposition 2 (**)]. This gives us

$$M_1^{-1}\big|_{i=B,j=K} = \begin{cases}\mu_{\mathscr{G}}(K,B)/|G/K| & \text{if } K\subset B,\\ 0 & \text{otherwise.}\end{cases}$$

Our proposition is proved. □

The function `GetM1Inverse` of the script `LIEP.sage` computes M_1^{-1}.

The recursion formula. We start from (21) and deduce that

$$V_s(t) = -\sum_{\substack{d\,|\,|G|,\\ d\neq 1}} M_1^{-1}M_dV_s(dt) + M_1^{-1}\Gamma(t). \tag{28}$$

We readily find that $N_d = dM_1^{-1}M_d$ is given by (11).

Proof. Indeed we have

$$N_d\big|_{i=B_0,j=B_1} = d\sum_{\substack{K\subset B_0,\\ K\subset B_1,\\ |KB_1/K|=d}} \mu(|B_0/K|)|G/K|^{-1}|G/B_1|.$$

This is exactly what we have written in (11). □

By considering the exact sequence

$$1 \longrightarrow K \cap B_1 \xrightarrow[k \mapsto (k, k^{-1})]{} K \times B_1 \xrightarrow[(k,b_1) \mapsto k b_1]{} KB_1 \longrightarrow 1, \tag{29}$$

one shows that $|KB_1/K| = |B_1|/|K \cap B_1|$. As a consequence, we see that only the d that divides the *exponent* of G appear. The function `GetNds` of the script `LIEP.sage` computes $(N_d)_d$.

$$V_s(t) = -\sum_{\substack{d|\exp G,\\ d\neq 1}} \frac{N_d}{d} V_s(dt) + M_1^{-1}\Gamma(t). \tag{30}$$

Unfolding the recursion. Let $z \geqslant 1$ and $r \geqslant 1$ be two parameters. We have

$$\begin{aligned} V_s(t) = (-1)^r \sum_{d_1 \cdots d_r \leqslant z} \frac{N_{d_1}}{d_1} \ldots \frac{N_{d_r}}{d_r} V_s(d_1 \ldots d_r t) \\ + \sum_{1 \leqslant v \leqslant r} (-1)^v \sum_{\substack{d_1 \cdots d_{v-1} \leqslant z,\\ d_1 \cdots d_{v-1} d_v > z}} \frac{N_{d_1}}{d_1} \ldots \frac{N_{d_v}}{d_v} V_s(d_1 \ldots d_v t) \\ + \sum_{1 \leqslant v \leqslant r-1} (-1)^v \sum_{d_1 \cdots d_v \leqslant z} \frac{N_{d_1}}{d_1} \ldots \frac{N_{d_v}}{d_v} M_1^{-1}\Gamma(d_1 \ldots d_v t) + M_1^{-1}\Gamma(t) \end{aligned} \tag{31}$$

where $d_1, \ldots, d_r$ are all divisors of $\exp G$ excluding 1. We can incorporate the last summand in the one before by considering as the value for $s = 0$.

Proof. Let us prove this formula by recursion. Case $r = 1$ is just (30). Let us see precisely what happens for $r = 2$. We start from

$$V_s(t) = -\sum_{\substack{d_1|\exp G,\\ d_1\neq 1}} \frac{N_{d_1}}{d_1} V_s(d_1 t) + M_1^{-1}\Gamma(t)$$

which we rewrite as

$$V_s(t) = -\sum_{\substack{d_1|\exp G,\\ d_1\neq 1,\\ d_1 \leqslant z}} \frac{N_{d_1}}{d_1} V_s(d_1 t) - \sum_{\substack{d_1|\exp G,\\ d_1\neq 1,\\ d_1 > z}} \frac{N_{d_1}}{d_1} V_s(d_1 t) + M_1^{-1}\Gamma(t).$$

We use again this equation on $V_s(d_1 t)$ when $d_1 \leqslant z$, and z/d_1 rather than z, getting

$$\begin{aligned} V_s(t) = \sum_{\substack{d_1|\exp G,\\ d_1\neq 1,\\ d_1 \leqslant z}} \sum_{\substack{d_2|\exp G,\\ d_2\neq 1,\\ d_1 d_2 \leqslant z}} \frac{N_{d_1}}{d_1} \frac{N_{d_2}}{d_2} V_s(d_1 d_2 t) \\ + \sum_{\substack{d_1|\exp G,\\ d_1\neq 1,\\ d_1 \leqslant z}} \sum_{\substack{d_2|\exp G,\\ d_2\neq 1,\\ d_1 d_2 > z}} \frac{N_{d_1}}{d_1} \frac{N_{d_2}}{d_2} V_s(d_1 d_2 t) - \sum_{\substack{d_1|\exp G,\\ d_1\neq 1,\\ d_1 > z}} \frac{N_{d_1}}{d_1} V_s(d_1 t) \\ - \sum_{\substack{d_1|\exp G,\\ d_1\neq 1,\\ d_1 \leqslant z}} \frac{N_{d_1}}{d_1} M_1^{-1}\Gamma(t) + M_1^{-1}\Gamma(t). \end{aligned}$$

To go from r to $r+1$, we select the divisors d_r that are such that $d_1 d_2 \cdots d_r \leqslant z$ and employ (30) on $V_s(d_1 \cdots d_r t)$. □

Lemma 4.2. *The coefficients of a product $N_{d_1}N_{d_2}\cdots N_{d_v}$ are at most (in absolute value) equal to $|G^\sharp|^{v-1}$, where $G^\sharp$ is the set of* lattice-invariant *classes (which is also the number of cyclic subgroups of G).*

End of the proof of Theorem 1.3. The formula (33) with $t=1$ contains most of our proof. We only have to control the error term, which is our next task.

The number of possible d's is at most the number of divisors of $\exp G$ minus 1, so at most $d(\exp G)$. The coefficients of a typical product $N_{d_1}\cdots N_{d_v}$ are of size at most $|G^\sharp|^{v-1}$, we divide each coefficient by $d_1\cdots d_v$ which is at least z, and we have at most $d(\exp G)^v$ v-tuples $(d_1,\ldots,d_v)$. As a consequence, each coordinate, says y, of the vector

$$\sum_{1\leqslant v\leqslant r-1}(-1)^v\sum_{\substack{d_1\cdots d_{v-1}\leqslant z,\\ d_1\cdots d_{v-1}d_v>z}}\frac{N_{d_1}}{d_1}\ldots\frac{N_{d_v}}{d_v}V_s(d_1\ldots d_v t)$$

satisfies

$$|y|\leqslant (r-1)\,\frac{\big(|G^\sharp|d(\exp G)\big)^{r-1}}{z|G^\sharp|}\max_{D\geqslant 2^r}\|V_s(Dt)\|.$$

We deal similarly with the coordinates of the vector

$$(-1)^r\sum_{d_1\cdots d_r\leqslant z}\frac{N_{d_1}}{d_1}\ldots\frac{N_{d_r}}{d_r}V_s(d_1\ldots d_r t)$$

except that the denominator $d_1\cdots d_r$ is not especially larger than z; we however select $z=2^r$ to ensure this condition. This means that only $d_1=d_2=\ldots=d_r=2$ is admissible. So, on combining both, we see that

$$(32)\quad \Big\|V_s(1)-\sum_{0\leqslant v\leqslant r-1}(-1)^v\sum_{d_1\cdots d_v\leqslant 2^r}\frac{N_{d_1}}{d_1}\ldots\frac{N_{d_v}}{d_v}M_1^{-1}\Gamma_s(d_1\ldots d_v)\Big\|$$
$$\leqslant\frac{1}{2}\Big(1+\frac{r-1}{|G^\sharp|}\Big)\Big(\frac{|G^\sharp|d(\exp G)}{2}\Big)^{r-1}\max_{D\geqslant 2^r}\|V_s(D)\|.$$

To complete the proof, we simply need a bound for $\max_{D\geqslant 2^r}\|V_s(D)\|$ and such a bound is provided by the next lemma.

Lemma 4.3. *Let $\mathcal{A}$ be a subset of the $G=(\mathbb{Z}/q\mathbb{Z})^\times$. Let $f>1$ be a real parameter. We have*

$$\big|\log\zeta_P(f;q,\mathcal{A})\big|\leqslant\frac{1+P/(f-1)}{P^f}.$$

Proof. We use

$$\log\zeta_P(f;q,\mathcal{A})=-\sum_{\substack{p\in\mathcal{A},\\ p\geqslant P}}\sum_{k\geqslant 1}\frac{1}{kp^{kf}}$$

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

$$\Big|\log\zeta_P(f;q,\mathcal{A})\Big|\leqslant\sum_{n\geqslant P}\frac{1}{n^f}\leqslant\frac{1}{P^f}+\int_P^\infty\frac{dt}{t^f}$$

□

5. A detailed example modulo 7

Wet set $G=(\mathbb{Z}/7\mathbb{Z})^\times$. We find that

$$\mathscr{G}=\big\{\{1\},\{1,6\},\{1,2,4\},\{1,2,3,4,5,6\}\big\}$$

(indexed in this order) and that

$$G^\sharp=\big\{\{1\},\{6\},\{2,4\},\{3,5\}\big\},$$

also indexed in that order. There are 6 Dirichlet characters whose values are given by (with $\zeta_6 = \exp(2i\pi/6)$)

	1	2	3	4	5	6
χ_0	1	1	1	1	1	1
χ_1	1	ζ_6^2	ζ_6	$-\zeta_6$	$-\zeta_6^2$	-1
χ_2	1	$-\zeta_6$	ζ_6^2	ζ_6^2	$-\zeta_6$	1
χ_3	1	1	-1	1	-1	-1
χ_4	1	ζ_6^2	$-\zeta_6$	$-\zeta_6$	ζ_6^2	1
χ_5	1	$-\zeta_6$	$-\zeta_6^2$	ζ_6^2	ζ_6	-1

We obtain this list with the command

```
[[e(n) for n in xrange(1,7)] for e in GetStructure(7)[5]]
```

and the remark $\zeta_6 - 1 = \zeta_6^2$. The 8th component of `GetStructure(7)` gives the index of the characters that are trivial on the above subgroups, its value is thus

$$[[0, 1, 2, 3, 4, 5], [0, 2, 4], [0, 3], [0]].$$

The vector $\Gamma_s(t)$ is given by (it is defined by (7))

$$\Gamma_s(t) = \left| \begin{array}{l} \log \prod_{0\leqslant i\leqslant 5} L_P(ts, \chi_i) \\ \log \prod_{i\in\{0,2,4\}} L_P(ts, \chi_i) \\ \log(L_P(ts, \chi_0) L_P(ts, \chi_3)) \\ \log L_P(ts, \chi_0) \end{array} \right.$$

while

$$V_s(t) = \left| \begin{array}{l} -\log \prod_{\substack{p\equiv 1[7], \\ p\geqslant P}} (1 - 1/p^{ts}) \\ -\log \prod_{\substack{p\equiv 6[7], \\ p\geqslant P}} (1 - 1/p^{ts}) \\ -\log \prod_{\substack{p\equiv 2,4[7], \\ p\geqslant P}} (1 - 1/p^{ts}) \\ -\log \prod_{\substack{p\equiv 3,5[7], \\ p\geqslant P}} (1 - 1/p^{ts}) \end{array} \right.$$

Now that the players and the surrounding environment has been described, let us turn towards the main step of our proof: the recursion (21). We first check that

$$\begin{aligned} \gamma(\{1\}, t) &= 6x_{\{1\}}^t + 3x_{\{6\}}^{2t} + 2x_{\{2,4\}}^{3t} + x_{\{3,5\}}^{6t}, \\ \gamma(\{1, 6\}, t) &= 3x_{\{1\}}^t + 3x_{\{6\}}^t + x_{\{2,4\}}^{3t} + x_{\{3,5\}}^{3t}, \\ \gamma(\{1, 2, 4\}, t) &= 2x_{\{1\}}^t + x_{\{6\}}^{2t} + 2x_{\{2,4\}}^t + x_{\{3,5\}}^{2t}, \\ \gamma(\{1, 2, 3, 4, 5, 6\}, t) &= x_{\{1\}}^t + x_{\{6\}}^t + x_{\{2,4\}}^t + x_{\{3,5\}}^t. \end{aligned}$$

Whence the relation

$$\Gamma_s(t) = M_1 V_s(t) + M_2 V_s(2t) + M_3 V_s(3t) + M_6 V_s(6t)$$

with

$$M_1 = \begin{pmatrix} 6 & 0 & 0 & 0 \\ 3 & 3 & 0 & 0 \\ 2 & 0 & 2 & 0 \\ 1 & 1 & 1 & 1 \end{pmatrix}, \quad M_2 = \begin{pmatrix} 0 & 3 & 0 & 0 \\ 0 & 0 & 0 & 0 \\ 0 & 1 & 0 & 1 \\ 0 & 0 & 0 & 0 \end{pmatrix}$$

$$M_3 = \begin{pmatrix} 0 & 0 & 2 & 0 \\ 0 & 0 & 1 & 1 \\ 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 \end{pmatrix}, \quad M_6 = \begin{pmatrix} 0 & 0 & 0 & 1 \\ 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 \end{pmatrix}.$$

The call `GetM1Inverse(7,GetStructure(7))^(-1)` produces the matrix M_1. The matrices $N_d = dM_1^{-1}M_d$ are obtained by `GetNds(7,GetStructure(7))`. They are

$$N_2 = \begin{pmatrix} 0 & 1 & 0 & 0 \\ 0 & -1 & 0 & 0 \\ 0 & -1 & 0 & 1 \\ 0 & 1 & 0 & -1 \end{pmatrix}, \quad N_3 = \begin{pmatrix} 0 & 0 & 1 & 0 \\ 0 & 0 & -1 & 1 \\ 0 & 0 & -1 & 0 \\ 0 & 0 & 1 & -1 \end{pmatrix}, \quad N_6 = \begin{pmatrix} 0 & 0 & 1 & -1 \\ 0 & 0 & 0 & -1 \\ 0 & 0 & 0 & -1 \\ 0 & 0 & 0 & 1 \end{pmatrix}.$$

In order to check our script, we mention that the call

```
GetM1Inverse(7,GetStructure(7))^(-1)*GetNd(2,7,GetStructure(7))/2
```

gives M_2 for instance (and one can replace the parameter 2 that occurs twice with 3 or 6 to get M_3 and M_6). We have reached

$$V_s(t) = M_1^{-1}\Gamma_s(t) - \frac{N_2}{2}V_s(2t) - \frac{N_3}{3}V_s(3t) - \frac{N_6}{6}V_s(6t).$$

Our objective is $V_s(1)$ and we know how to compute $\Gamma_s(t)$ while, when d is large, $V_s(dt)$ vanishes approximately; it is thus enough to iterate the above formula. We end the numerical example here.

6. Rational Euler Products

Let us recall the Witt decomposition. The readers will find in [6, 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 6.1. *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*

$$s_F(k) + a_1 s_F(k-1) + \ldots + a_{k-1}s_F(1) + ka_k = 0, \tag{33}$$

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

$$b_F(k) = \frac{1}{k}\sum_{d|k}\mu(k/d)s_F(d). \tag{34}$$

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

$$F(t) = \prod_{j=1}^{\infty}(1 - t^j)^{b_F(j)} \tag{35}$$

where the convergence is uniform in the given segment.

And how does the mathematician E. Witt enter the scene? In the paper [18] on Lie algebras, Witt produced in equation (11) therein a decomposition that is the prototype of the above expansion.

Proof. Since we follow the proof of [6, Lemma 1], we shall be rather sketchy. We write $F(t) = \prod_i (1 - \alpha_i t)$. We thus have

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

This series is absolutely convergent in any disc $|t| \leqslant b < 1/\beta$ where $\beta = \max_j(1/|\alpha_j|)$. We may also decompose $tF'(t)/F(t)$ in Lambert series as

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

as some series shuffling in any disc of radius $b < \min(1, 1/\beta)$ shows. The lemma follows readily by integrating the above relation. □

Lemma 6.2. *We use the hypotheses and notation of Lemma 6.1. Let $\beta \geqslant 2$ be larger than the inverse of the modulus of all the roots of $F(t)$. We have*

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

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

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

□

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 6.3. *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. Show that, either $|\rho| \geqslant 1$ or $1/|\rho| \leqslant |a_1| + |a_2| + \ldots + |a_\delta|$.*

Proof. The readers may first notice that

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

The conclusion is easy. □

Proof of Theorem 1.4. The proof requires several steps. The very first one is a direct consequence of (35), which leads to the identity

$$\frac{F(t)}{G(t)} = \prod_{j=2}^{\infty} (1 - t^j)^{b_F(j) - b_G(j)}. \tag{36}$$

The absence of the $j = 1$ term is due to our assumption that $(F(X) - G(X))/X^2 \in \mathbb{Z}[X]$. Up to this point (36) is only established as a formal identity. Our second step is to establish (36) for all $t \in \mathbb{C}$ with $|t| < 1/\beta$ and to control the rate of convergence. By Lemma 6.2, we know that $|b_F(j) - b_G(j)| \leqslant 2 \max(\deg F, \deg G)\beta^j/j$. Therefore, for any bound J, we have

$$\sum_{j \geqslant J+1} |t^j||b_F(j) - b_G(j)| \leqslant 2 \max(\deg F, \deg G) \frac{|t\beta|^{J+1}}{(1 - |t\beta|)(J+1)}, \tag{37}$$

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

$$\frac{F(t)}{G(t)} = \prod_{2 \leqslant j \leqslant J} (1 - t^j)^{b_F(j) - b_G(j)} \times I_1, \tag{38}$$

where $|\log I_1| \leqslant 2 \max(\deg F, \deg G)|t\beta|^{J+1}/[(1 - |t\beta|)(J+1)]$.

Now that we have the expansion (38) for each prime p, we may combine them. We readily get

$$\prod_{\substack{p \geqslant P, \\ p \in \mathcal{A}}} \frac{F(1/p)}{G(1/p)} = \prod_{\substack{p \geqslant P, \\ p \in \mathcal{A}}} \prod_{2 \leqslant j \leqslant J} (1 - p^{-j})^{b_G(j) - b_F(j)} \times I_2,$$

where I_2 satisfies

$$\begin{aligned}|\log I_2| &\leqslant 2\max(\deg F, \deg G)\sum_{p\geqslant P}\frac{\beta^{J+1}}{1-\beta/P}\frac{1}{(J+1)p^{J+1}}\\ &\leqslant \frac{2\max(\deg F,\deg G)\beta^{J+1}}{(1-\beta/P)(J+1)}\left(\frac{1}{P^{J+1}}+\int_P^\infty\frac{dt}{t^{J+1}}\right)\\ &\leqslant \frac{2\max(\deg F,\deg G)(\beta/P)^J\beta}{(1-\beta/P)(J+1)}\left(\frac{1}{P}+\frac{1}{J}\right),\end{aligned}$$

since $P\geqslant 2$ and $J\geqslant 3$. As announced earlier, we may rearrange the product over the primes p and get

$$\prod_{\substack{p\geqslant P,\\ p\in\mathcal{A}}}\frac{F(1/p)}{G(1/p)} = \prod_{2\leqslant j\leqslant J}\zeta_P(j;q,\mathcal{A})^{b_G(j)-b_F(j)}\times I_2.$$

The last step is to replace $\zeta_P(j;q,\mathcal{A})$ by the approximation, say $\zeta_P(j;q,\mathcal{A}|r)$ given by (13). We find that

$$\prod_{\substack{p\geqslant P,\\ p\in\mathcal{A}}}\frac{F(1/p)}{G(1/p)} = \prod_{2\leqslant j\leqslant J}\zeta_P(j;q,\mathcal{A}|r)^{b_F(j)-b_G(j)}\times I_3,$$

where I_3 satisfies

$$\begin{aligned}|\log I_3| &\leqslant C\sum_{2\leqslant j\leqslant J}|b_F(j)-b_G(j)|\frac{1+P/(2^rj-1)}{P^{j2^r}}+|\log I_2|\\ &\leqslant C\sum_{2\leqslant j\leqslant J}2\max(\deg F,\deg G)\frac{\beta^j}{j}\frac{1+2^{-r}P}{P^{j2^r}}+|\log I_2|.\end{aligned}$$

with

$$C=\frac{1}{2}\left(1+\frac{r-1}{|G^\sharp|}\right)\left(\frac{|G^\sharp|d(\exp G)}{2}\right)^{r-1}.$$

Therefore (and since $r\geqslant 2$)

$$\frac{|\log I_3|}{2\max(\deg F,\deg G)}\leqslant\frac{1}{4}\left(1+\frac{r-1}{|G^\sharp|}\right)\left(\frac{|G^\sharp|d(\exp G)}{2}\right)^{r-1}\frac{\beta^2}{P^{2^{r+1}}}\frac{1+2^{-r}P}{1-\beta/P^4} + \frac{(\beta/P)^J\beta}{(1-\beta/P)(J+1)}\left(\frac{1}{P}+\frac{1}{J}\right) \tag{39}$$

and this ends the proof. □

7. Counting the number of Lattice-Invariant Classes

It is of interest to count how many lattice-invariant classes there are, i.e. to determine the cardinality of $G^\sharp$ which is equally the number of cyclic subgroups, i.e. the cardinality of $\mathscr{G}$. We proceed in several steps.

Lemma 7.1. *Let $d\geqslant 1$ and $q\geqslant 1$ be two integers. The number $\rho(q;d)$ of solutions to the equation $x^d\equiv 1[q]$ is a multiplicative function of the variable q. When p is a prime, we find that*

$$\rho(p^\alpha;d)=\begin{cases}(d,p^{\alpha-1}(p-1)) & \text{if } p\neq 2,\\ 1 & \text{if } p=2 \text{ and } \alpha=1,\\ 1 & \text{if } p=2,\ \alpha\geqslant 2 \text{ and } d \text{ odd},\\ 2(d,2^{\alpha-2}) & \text{if } p=2,\ \alpha\geqslant 2 \text{ and } d \text{ even}.\end{cases}$$

The function $d\mapsto\rho(q;d)$ is also multiplicative.

Proof. The multiplicative character of $\rho(q;d)$ stems from the Chinese Remainder Theorem. In $\mathbb{Z}/p^\alpha\mathbb{Z}$ and $p\neq 2$, the equation $x^d\equiv 1[p^\alpha]$ has $(d,p^{\alpha-1}(p-1))$ as stated in [9, Corollary 2.42]; it is an easy consequence of the fact that $(\mathbb{Z}/p^\alpha\mathbb{Z})^\times$ is cyclic in this case.

When $p=2$, the equation $x^d\equiv 1[2]$ has exactly one solution, namely $x=1$. When $p=2$ and $\alpha\geqslant 2$, the multiplicative group $(\mathbb{Z}/p^\alpha\mathbb{Z})^\times$ is isomorphic to the direct product $(\mathbb{Z}/2\mathbb{Z},+)\times(\mathbb{Z}/2^{\alpha-2}\mathbb{Z},+)$. We find as a consequence of [4, Proposition 4.2.2] that $\rho(2^\alpha,d)=2(d,2^{\alpha-2})$.

The multiplicativity of the function $d\mapsto\rho(q;d)$ folows from the explicit expression of $\rho(q;d)$: it is a product (over prime factors of q) of multiplicative functions of the variable d. □

Lemma 7.2. *The number $\rho^*(q;d)$ of elements of order d in $(\mathbb{Z}/q\mathbb{Z})^\times$ is given by*

$$\sum_{\ell|d}\mu(d/\ell)\rho(q;\ell)$$

where $\rho(q;d)$ is defined and determined in Lemma 7.1.

Proof. This is a consequence of the Moebius inversion formula as, by classifying the solution of $x^d\equiv 1[q]$ by their order, we find that $\rho(q;d)=\sum_{\ell|d}\rho^*(q;\ell)$. □

Proposition 7.3. *When $q\geqslant 3$, the number $|\mathscr{G}|$ of cyclic subgroups of $(\mathbb{Z}/q\mathbb{Z})^\times$ is given by*

$$|\mathscr{G}|=\prod_{\substack{p|\varphi(q),\\ p\neq 2}}\frac{p-2}{p-1}\sum_{\substack{d|\varphi(q),\\ 2|d}}\frac{\rho(q;d)}{\varphi(d)}\prod_{\substack{p|d,\\ p|\varphi(q)/d,\\ p\neq 2}}\frac{(p-1)^2}{p(p-2)}\prod_{\substack{p|d,\\ p\nmid\varphi(q)/d,\\ p\neq 2}}\frac{p-1}{p-2}\prod_{\substack{2|d,\\ 2|\varphi(q)/d}}\frac{1}{2}$$

where $\rho(q;d)$ is defined and determined in Lemma 7.1.

We have checked this expression with Sage via the function `CardClassList` of our script. The values have been checked against a direct count: we have the list of lattice-invariant classes, hence their number.

Proof. Each cyclic subgroup of order d has $\varphi(d)$ generators. Hence the number of cyclic subgroups of order d is equal to $\rho^*(q;d)/\varphi(d)$, whence, by Lemma 7.2,

$$\begin{aligned}|\mathscr{G}|&=\sum_{d|\varphi(q)}\frac{1}{\varphi(d)}\sum_{\ell|d}\mu(d/\ell)\rho(q;\ell)\\ &=\sum_{\ell|\varphi(q)}\rho(q;\ell)\sum_{\ell|d|\varphi(q)}\frac{\mu(d/\ell)}{\varphi(d)}.\end{aligned}$$

To evaluate the inner sum, write $\varphi(q)=h_1h_2h_3$, where h_1 is the product of the $p^{v_p(\varphi(q))}$ with $p|\ell$ and $p|\varphi(q)/\ell$, then h_2 is the product of the $p^{v_p(\varphi(q))}$ with $p|\ell$ but $p\nmid\varphi(q)/\ell$ and $(h_3,\ell)=1$ is what remains after division by h_1h_2. We readily find that

$$\sum_{\ell|d|\varphi(q)}\frac{\mu(d/\ell)}{\varphi(d)}=\frac{1}{\varphi(\ell)}\prod_{p|h_1}\Bigl(1-\frac{1}{p}\Bigr)\prod_{p|h_2}1\prod_{p|h_3}\Bigl(1-\frac{1}{p-1}\Bigr).$$

This vanishes when $2|h_3$, so we can restrict our attention to even ℓ's. In which case we get

$$\sum_{\ell|d|\varphi(q)}\frac{\mu(d/\ell)}{\varphi(d)}=\frac{1}{\varphi(\ell)}\prod_{\substack{p|\varphi(q),\\ p\neq 2}}\frac{p-2}{p-1}\prod_{\substack{p|h_1,\\ p\neq 2}}\frac{(p-1)^2}{p(p-2)}\prod_{\substack{p|h_2,\\ p\neq 2}}\frac{p-1}{p-2}\times\Bigl(\frac{1}{2}\text{when } 2^{v_2(\varphi(q))}\nmid\ell\Bigr).$$

We reverse to the variable d rather than ℓ to write our lemma. We have also used the condition $q\geqslant 3$ to ensure that $2|\varphi(q)$. □

8. Notes on the implementation

The parameter r is not very large, typically between 2 and 8. Since in (12), several products $d = d_1 \cdots d_v$ are equal, we store the computed values of $\Gamma_s(dt)$ in the dictionary `ComputedGammas` in the function `GetVs` of the script `LIEP.sage`. We proceed similarly with the dictionary `ComputedProductNdsM1Inverse` for the products $N_{d_1} \cdots N_{d_v} M_1^{-1}$ in . Since the *list* $[d_1, \cdots, d_v]$ cannot be a key for such a dictionary, we simply replace it by the *tuple* $(d_1, \cdots, d_v)$.

Concerning the general structure, the function `GetStructure` computes all the algebraical quantities that we need: the list of cyclic subgroups, the one of lattice-invariant classes, the exponent of our group, its character group, the set of invertible classes and, for each cyclic subgroup, the set of characters that are trivial on it.

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

$$\text{GetVs}(12, 2, 100, 300)$$

to compute modulo 12 the possible constants with $s = 2$, asking for 100 decimal digits and using $P = 300$. 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 (we observed no such phenomenon, but it may still happen!). A more precise treatment would first check the output and if the precision attained would not be enough, increase automatically this parameter. We prefer to let the users do that by themselves. The digits presented when `WithLaTeX` $= 1$ are always accurate. Note that we expect the final result to be of size roughly unity, so 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 list of the invariant classes and the one of the computed lower and upper values. When equal to 1, its default value, some information on the computation is given. At level 2, more informations is given, but that should not concern the casual user. When the parameter `Verbose` is at least 1 and `WithLaTeX` is 1, the values of the constants will be further presented in a format suitable for inclusion in a LaTeX-file. For instance, the call

$$\text{GetVs}(12, 2, 100, 100, 1, 1)$$

is the one used to prepare this document.

To compute the Euler products as explained in Theorem 1.4, we have the function `GetEulerProds(q, F, G, nbdecimals, bigP = 100, Verbose = 1, WithLaTeX = 0)`. Note that the parameter `bigP` may be increased during the run of the program to ensure that $P \geqslant 2\beta$ (a condition that is most of the time satisfied). We reused the same structure as the function `GetVs`, without calling it: this is to also keep all the precomputed datas. 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 manners. The co-authors of this paper have computed several of the next values via 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 Shank's and Lal's constants are known (Finch in [1] gives 10 digits) and we agree on those. Finally, the web site [3] by X. Gourdon and P. Sebah is nowadays difficult to decypher but a postscript version is available on the same page. They give in section 4.4 the first fifty digits of the constant they call A and which is

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

Our result match the one of [3].

9. Some results

In this part, we exhibit some results for $s = 2$ and small q's. We decided to produce 100 decimal digits each time. Each computation took at most five seconds and we selected uniformly $P = 100$.

Modulo 3.

$$\prod_{p\equiv 1[3]}(1-p^{-2})^{-1} = 1.03401\,48754\,14341\,88053\,90306\,44413\,04762\,85789\,65428\,48909\,98864\,16825\,03842\,12222\,45871\,09635\,80496\,21707\,98262\,05962\cdots$$

$$\prod_{p\equiv 2[3]}(1-p^{-2})^{-1} = 1.41406\,43908\,92147\,63756\,55018\,19079\,82937\,99076\,95069\,39316\,21750\,39924\,96242\,39281\,06992\,08849\,94537\,54858\,50247\,51141\cdots$$

Modulo 4.

$$\prod_{p\equiv 1[4]}(1-p^{-2})^{-1} = 1.05618\,21217\,26816\,14173\,79307\,65316\,21989\,05875\,80425\,46070\,80120\,04306\,19830\,27928\,16062\,22693\,04895\,12958\,37291\,59718\cdots$$

$$\prod_{p\equiv 3[4]}(1-p^{-2})^{-1} = 1.16807\,55854\,10514\,28866\,96967\,37064\,04040\,13646\,79021\,45554\,79928\,40563\,68111\,38106\,59377\,71094\,66904\,07472\,79588\,48702\cdots$$

Modulo 5.

$$\prod_{p\equiv 1[5]}(1-p^{-2})^{-1} = 1.01091\,51606\,01019\,52260\,49565\,84289\,51492\,09845\,38627\,58173\,85237\,32024\,20089\,25161\,37424\,56726\,37093\,96197\,69455\,89218\cdots$$

$$\prod_{p\equiv 2,3[5]}(1-p^{-2})^{-1} = 1.55437\,60727\,20889\,22081\,75902\,82565\,55177\,56056\,30147\,34257\,40072\,50077\,94457\,39239\,00871\,38641\,44091\,80733\,87878\,70683\cdots$$

$$\prod_{p\equiv 4[5]}(1-p^{-2})^{-1} = 1.00496\,03239\,22297\,55899\,37496\,24810\,25218\,47955\,10294\,18802\,28801\,99528\,37852\,15071\,27700\,70076\,98854\,32491\,36118\,00619\cdots$$

Modulo 7.

$$\prod_{p\equiv 1[7]}(1-p^{-2})^{-1} = 1.00222\,95338\,19740\,42627\,18641\,59138\,22019\,24486\,37565\,40128\,87922\,82973\,79678\,21741\,90308\,08041\,42707\,36575\,28295\,76151\cdots$$

$$\prod_{p\equiv 2,4[7]}(1-p^{-2})^{-1} = 1.34984\,62543\,65273\,20787\,74772\,44978\,62277\,76508\,69021\,24860\,12031\,69999\,35719\,21654\,93824\,75777\,02051\,36300\,53459\,76601\cdots$$

$$\prod_{p\equiv 3,5[7]}(1-p^{-2})^{-1} = 1.18274\,26007\,67364\,09208\,00286\,83933\,15918\,51718\,05360\,46335\,82633\,06344\,66854\,90324\,90537\,21799\,81486\,90001\,86365\,91391\cdots$$

$$\prod_{p\equiv 6[7]}(1-p^{-2})^{-1} = 1.00705\,20326\,03074\,04805\,67193\,52428\,88870\,69289\,36714\,73687\,58335\,65893\,11634\,74829\,60947\,12069\,41243\,26265\,99553\,53536\cdots$$

Modulo 8.

$$\prod_{p\equiv 1[8]}(1-p^{-2})^{-1} = 1.00483\,50650\,34191\,18711\,83598\,31169\,10411\,95979\,07317\,54340\,88789\,55156\,06711\,74639\,62051\,31056\,35207\,32105\,88068\,58783\cdots$$

$$\prod_{p\equiv 3[8]}(1-p^{-2})^{-1} = 1.13941\,87771\,08211\,51502\,70589\,30773\,34020\,88725\,59961\,09629\,48302\,25821\,27411\,02101\,65577\,60742\,91446\,59374\,91512\,33349\cdots$$

$$\prod_{p\equiv 5[8]}(1-p^{-2})^{-1} = 1.05109\,99849\,42183\,30793\,68775\,56006\,33505\,68012\,01018\,45817\,85080\,59912\,94207\,39729\,30485\,58783\,38889\,50479\,59255\,34495\cdots$$

$$\prod_{p\equiv 7[8]}(1-p^{-2})^{-1} = 1.02515\,03739\,25759\,17991\,61954\,35560\,94158\,79433\,11002\,76024\,41530\,69566\,94982\,17644\,97960\,41007\,90076\,26943\,14236\,43529\cdots$$

Modulo 9.

$$\prod_{p\equiv 1[9]}(1-p^{-2})^{-1} = 1.00403\,38350\,51288\,79798\,24781\,19924\,74748\,94825\,22895\,79877\,28822\,86701\,42359\,63409\,37977\,93839\,33608\,94316\,94860\,37141\cdots$$

$$\prod_{p\equiv 2,5[9]}(1-p^{-2})^{-1} = 1.40783\,70719\,96538\,05093\,52684\,03433\,79823\,18382\,56159\,80878\,18858\,21039\,93308\,74959\,08486\,21687\,68292\,75777\,90984\,34896\cdots$$

$$\prod_{p\equiv 4,7[9]}(1-p^{-2})^{-1} = 1.02986\,05876\,77826\,18491\,88642\,35135\,21663\,16312\,01666\,87293\,15881\,63094\,56123\,55333\,65628\,89969\,28513\,96515\,60005\,36245\cdots$$

$$\prod_{p\equiv 8[9]}(1-p^{-2})^{-1} = 1.00442\,33235\,64550\,15978\,66082\,58390\,58205\,39661\,19672\,30788\,17744\,79626\,23017\,18753\,96410\,76663\,34579\,95134\,16501\,66760\cdots$$

Modulo 11.

$$\prod_{p\equiv 1[11]}(1-p^{-2})^{-1} = 1.00232\,82408\,97736\,52733\,78057\,92469\,42582\,04345\,78064\,14879\,23124\,99895\,44150\,38255\,72926\,07516\,98484\,87460\,03110\,08712\cdots$$

$$\prod_{p\equiv 2,6,7,8[11]}(1-p^{-2})^{-1} = 1.38240\,11448\,05788\,71773\,39824\,35954\,70441\,91351\,16435\,84157\,13863\,06101\,70250\,01900\,59181\,34321\,25138\,72741\,06748\,64687\cdots$$

$$\prod_{p\equiv 3,4,5,9[11]}(1-p^{-2})^{-1} = 1.17640\,19224\,41514\,71776\,56838\,81699\,54785\,03151\,42210\,45715\,72819\,38133\,44304\,81040\,93008\,74341\,67383\,61950\,21979\,26318\cdots$$

$$\prod_{p\equiv 10[11]}(1-p^{-2})^{-1} = 1.00079\,37707\,14740\,00680\,22327\,79981\,38075\,30993\,79972\,81556\,86828\,01966\,59824\,89326\,65924\,56171\,20791\,11742\,28212\,98769\cdots$$

Modulo 12.

$$\prod_{p\equiv 1[12]}(1-p^{-2})^{-1} = 1.00761\,32452\,14144\,96616\,93493\,12247\,73229\,37895\,47142\,90433\,17666\,43368\,44819\,49208\,97861\,01855\,78530\,60579\,11129\,80649\cdots$$

$$\prod_{p\equiv 5[12]}(1-p^{-2})^{-1} = 1.04820\,19036\,00769\,93683\,49374\,34895\,79267\,34804\,13674\,49481\,52581\,07376\,14495\,24161\,71571\,43788\,23594\,04990\,88566\,94968\cdots$$

$$\prod_{p\equiv 7[12]}(1-p^{-2})^{-1} = 1.02620\,21468\,31233\,70070\,72018\,66966\,36157\,23611\,09321\,31334\,95148\,10400\,66496\,54603\,29393\,86454\,19299\,91782\,63867\,91609\cdots$$

$$\prod_{p\equiv 11[12]}(1-p^{-2})^{-1} = 1.01177\,86368\,50332\,58370\,51194\,10267\,33127\,80584\,01230\,89520\,87028\,35959\,40756\,15016\,41704\,56300\,54442\,19591\,32980\,62727\cdots$$

Modulo 13.

$$\prod_{p\equiv 1[13]}(1-p^{-2})^{-1} = 1.00065\,68661\,98289\,66605\,74722\,84730\,77197\,91777\,00717\,07399\,33554\,44837\,12988\,36602\,52536\,84343\,79642\,73590\,88077\,31673\cdots$$

$$\prod_{p\equiv 2,6,7,11[5]}(1-p^{-2})^{-1} = 1.38005\,21671\,19142\,93623\,73358\,95833\,59312\,88490\,63922\,76216\,00813\,27801\,96170\,83570\,07037\,00666\,02382\,19997\,07055\,85939\cdots$$

$$\prod_{p\equiv 3,9[13]}(1-p^{-2})^{-1} = 1.12706\,12738\,77030\,37596\,05291\,90459\,70008\,03562\,53668\,12081\,48604\,51380\,13290\,89754\,69987\,12664\,24897\,64722\,52303\,29593\cdots$$

$$\prod_{p\equiv 4,10[13]}(1-p^{-2})^{-1} = 1.00628\,51383\,85264\,35654\,79220\,78630\,88874\,03212\,24553\,50607\,59162\,40959\,77321\,01204\,89381\,53735\,74182\,12805\,59112\,51752\cdots$$

$$\prod_{p\equiv 5,8[13]}(1-p^{-2})^{-1} = 1.04384\,79529\,58163\,48325\,64453\,12135\,62867\,13038\,05109\,49630\,56435\,71738\,46465\,77456\,29690\,71263\,29350\,03766\,17988\,29979\cdots$$

$$\prod_{p\equiv 12[13]}(1-p^{-2})^{-1} = 1.00019\,47228\,43353\,09720\,12251\,29852\,70839\,19867\,65951\,93000\,49665\,62593\,02690\,92410\,34974\,82067\,06364\,88262\,34074\,53639\cdots$$

Modulo 15.

$$\prod_{p\equiv 1[15]}(1-p^{-2})^{-1} = 1.00148\,97422\,73492\,93695\,62022\,82152\,29804\,06202\,71822\,24183\,85046\,92061\,06460\,33370\,47461\,16170\,34094\,66709\,13158\,03303\cdots$$

$$\prod_{p\equiv 2,8[15]}(1-p^{-2})^{-1} = 1.34246\,04551\,54995\,30799\,30100\,63345\,72665\,24298\,78723\,72380\,96524\,03928\,73058\,62457\,83670\,07480\,09151\,10334\,06933\,31380\cdots$$

$$\prod_{p\equiv 4[15]}(1-p^{-2})^{-1} = 1.00317\,84700\,07976\,58539\,76886\,54009\,35749\,55893\,69169\,67588\,37351\,26980\,45622\,46578\,84368\,96080\,28447\,94669\,19055\,69351\cdots$$

$$\prod_{p\equiv 7,13[15]}(1-p^{-2})^{-1} = 1.02920\,54524\,88970\,30487\,46169\,68199\,34620\,53972\,85734\,20801\,87576\,81344\,73863\,39397\,51683\,30560\,76995\,20714\,09590\,99521\cdots$$

$$\prod_{p\equiv 11[15]}(1-p^{-2})^{-1} = 1.00941\,13977\,70415\,34074\,11140\,07967\,71715\,31828\,38502\,83487\,41065\,68439\,10926\,98429\,51008\,47969\,06005\,15885\,02338\,55701\cdots$$

$$\prod_{p\equiv 14[15]}(1-p^{-2})^{-1} = 1.00177\,62082\,89544\,73626\,10915\,43079\,96283\,15610\,57061\,98467\,19519\,14691\,39870\,02036\,75682\,26376\,90944\,75824\,69831\,96091\cdots$$

Modulo 16.

$$\prod_{p\equiv 1[16]}(1-p^{-2})^{-1} = 1.00378\,12963\,11174\,37714\,94711\,72280\,61816\,45658\,26785\,28441\,57268\,63521\,48911\,54134\,99502\,87194\,19254\,71100\,10645\,46873\cdots$$

$$\prod_{p\equiv 3,11[16]}(1-p^{-2})^{-1} = 1.13941\,87771\,08211\,51502\,70589\,30773\,34020\,88725\,59961\,09629\,48302\,25821\,27411\,02101\,65577\,60742\,91446\,59374\,91512\,33349\cdots$$

$$\prod_{p\equiv 5,13[16]}(1-p^{-2})^{-1} = 1.05109\,99849\,42183\,30793\,68775\,56006\,33505\,68012\,01018\,45817\,85080\,59912\,94207\,39729\,30485\,58783\,38889\,50479\,59255\,34495\cdots$$

$$\prod_{p\equiv 7[16]}(1-p^{-2})^{-1} = 1.02325\,48781\,97407\,08067\,95776\,68614\,06977\,00372\,89157\,54600\,19844\,97929\,83355\,91253\,99909\,55714\,70317\,40567\,85934\,05044\cdots$$

$$\prod_{p\equiv 9[16]}(1-p^{-2})^{-1} = 1.00104\,97991\,21471\,31637\,83963\,95210\,10070\,68052\,00181\,57035\,98663\,81304\,47589\,89310\,55217\,86340\,51978\,44383\,63621\,58656\cdots$$

$$\prod_{p\equiv 15[16]}(1-p^{-2})^{-1} = 1.00185\,24179\,73996\,13159\,93578\,02219\,51678\,26622\,68517\,41444\,99996\,30754\,09303\,19958\,16127\,21985\,97936\,04820\,77136\,34947\cdots$$

Some notes on timing. We tried several large computations to get an idea of the limitations of our script, with the uniform choice $P = 300$ and asking for 100 decimal digits. Since we did not run each computations hundred times to get an average timing, this table has to be taken with a pinch of salt. We present relative timing, knowing that the computation with $q = 3$, $q = 4$ or $q = 4$ took about a tenth of a second.

q	$\varphi(q)$	$\#d_i's$	$\|G^\sharp\|$	r	relative time(ms)	q	$\varphi(q)$	$\#d_i's$	$\|G^\sharp\|$	r	relative time(ms)
3	2	5	2	5	1	52	24	55	12	5	102
4	2	5	2	5	1	53	52	23	6	5	675
5	4	19	3	5	1	55	40	32	12	5	250
7	6	28	4	5	3.2	56	24	28	16	5	15
8	4	5	4	5	2.2	57	36	34	12	5	222
9	6	28	4	5	3.2	59	58	6	4	5	675
11	10	15	4	5	30	60	16	19	12	5	5
12	4	5	4	5	2.5	61	60	84	12	5	1468
13	12	55	6	5	4.4	63	36	28	20	5	23
15	8	19	6	5	2	64	32	30	10	5	96
16	8	19	6	5	1.6	65	48	55	20	5	260
17	16	30	5	5	42	67	66	32	8	5	155
19	18	34	6	5	93	68	32	30	10	5	97
20	8	19	6	5	2	69	44	9	8	5	240
21	12	28	8	5	7	71	70	24	8	5	1850
23	22	9	4	5	100	72	24	28	16	5	15
24	8	5	8	5	5	73	72	72	12	5	1643
25	20	32	6	5	98	75	40	32	12	5	237
27	18	34	6	5	92	76	36	34	12	5	219
28	12	28	8	5	6.5	77	60	54	16	5	855
29	28	31	6	5	175	79	78	32	8	5	2312
31	30	54	8	5	343	80	32	19	20	5	12
32	16	27	8	5	25	81	54	35	8	5	871
33	20	15	8	5	65	83	82	5	4	5	1527
35	24	55	12	5	96	84	24	28	16	5	15
36	12	28	8	5	6.5	85	64	30	18	5	257
37	36	61	9	5	350	87	56	31	12	5	441
39	24	55	12	5	99	88	40	15	16	5	157
40	16	19	12	5	4.6	89	88	31	8	5	2058
41	40	40	8	5	424	91	72	55	30	5	464
43	42	40	8	5	654	92	44	9	8	5	241
44	20	15	8	5	652	93	60	54	16	5	866
45	24	55	12	5	95	95	72	61	18	5	915
47	46	6	4	5	394	96	32	27	16	5	61
48	16	19	12	5	4.8	97	96	70	12	5	3371
49	42	40	8	5	665	99	60	54	16	5	855
51	32	30	10	5	101	100	40	32	12	5	236

This table shows that the value of $\varphi(q)$ is the main determinant of the time needed. The column with the tag "$\#d_i's$" contains the number of tuples $(d_1, \cdots, d_v)$ in the main formula.

Here is now a shorter table when asking 1000 decimal digits still with $P = 300$. The time needed is still very decent.

q	$\varphi(q)$	$\#d_i's$	$\lvert G^\sharp\rvert$	r	time(ms)
3	2	8	2	8	3708
4	2	8	2	8	3226
5	4	87	3	8	7067
7	6	249	4	8	29421
8	4	8	4	8	6423
9	6	249	4	8	29267
11	10	96	4	8	56001
12	4	8	4	8	7264
13	12	716	6	8	87480
15	8	87	6	8	14021

When asking for 5000 decimal digits and only $q = 3$, it took about 16 minutes (with $P = 500$) to get an answer, which essentially sets the horizon of the present method.

References

[1] Steven R. Finch. *Mathematical constants*, volume 94 of *Encyclopedia of Mathematics and its Applications*. Cambridge University Press, Cambridge, 2003.

[2] Étienne Fouvry, Claude Levesque, and Michel Waldschmidt. Representation of integers by cyclotomic binary forms. *Acta Arith.*, 184(1):67–86, 2018.

[3] X. Gourdon and P. Sebah. Constants from number theory. *http://numbers.computation.free.fr/Constants/constants.html*, 2010. http://numbers.computation.free.fr/Constants/Miscellaneous/constantsNumTheory.ps.

[4] Kenneth Ireland and Michael Rosen. *A classical introduction to modern number theory*, volume 84 of *Graduate Texts in Mathematics*. Springer-Verlag, New York, second edition, 1990.

[5] M. Lal. Primes of the form $n^4 + 1$. *Math. Comp.*, 21:245–247, 1967.

[6] P. Moree. Approximation of singular series constant and automata. with an appendix by gerhard niklasch. *Manuscripta Matematica*, 101(3):385–399, 2000.

[7] P. Moree and R. Osburn. Two-dimensional lattices with few distances. *Enseign. Math. (2)*, 52(3-4):361–380.

[8] 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(3):438–463, 2004.

[9] Ivan Niven, Herbert S. Zuckerman, and Hugh L. Montgomery. *An introduction to the theory of numbers*. John Wiley & Sons, Inc., New York, fifth edition, 1991.

[10] OEIS Foundation Inc. *The On-Line Encyclopedia of Integer Sequence*, 2019. http://oeis.org/.

[11] Gian-Carlo Rota. On the foundations of combinatorial theory. I. Theory of Möbius functions. *Z. Wahrscheinlichkeitstheorie und Verw. Gebiete*, 2:340–368 (1964), 1964.

[12] Jean-Pierre Serre. *Cours d'arithmétique*, volume 2 of *Collection SUP: "Le Mathématicien"*. Presses Universitaires de France, Paris, 1970.

[13] D. Shanks. On maximal gaps between successive primes. *Math. Comp.*, 18:646–651, 1964.

[14] D. Shanks. The second-order term in the asymptotic expansion of $B(x)$. *Math. Comp.*, 18:75–86, 1964.

[15] Daniel Shanks. On the conjecture of Hardy & Littlewood concerning the number of primes of the form $n^2 + a$. *Math. Comp.*, 14:320–332, 1960.

[16] Daniel Shanks. On numbers of the form $n^4 + 1$. *Math. Comput.*, 15:186–189, 1961.

[17] Daniel Shanks. Lal's constant and generalizations. *Math. Comp.*, 21:705–707, 1967.

[18] E. Witt. Treue Darstellung Liescher Ringe. *J. Reine Angew. Math.*, 177:152–160, 1937.

Aix Marseille Univ, CNRS, Centrale Marseille, I2M, Marseille, France
E-mail address: salma.ettahri@etu.univ-amu.fr

CNRS / Aix Marseille Univ. / Centrale Marseille, I2M, Marseille, France
E-mail address: olivier.ramare@univ-amu.fr

Aix Marseille Univ, CNRS, Centrale Marseille, I2M, Marseille, France
E-mail address: leon.surel@etu.univ-amu.fr