The least common multiple of a quadratic sequence

Javier Cilleruelo

Abstract

For any irreducible quadratic polynomial $f(x)$ in $\mathbb{Z}[x]$ we obtain the estimate $\log$ l.c.m. $(f(1),\dots,f(n)) = n\log n + Bn + o(n)$ where B is a constant depending on f.

1. Introduction

The problem of estimating the least common multiple of the first n positive integers was first investigated by Chebyshev [Che52] when he introduced the function $\Psi(n)=\sum_{p^m\leqslant n}\log p = \log \text{l.c.m.}(1,\dots,n)$ in his study on the distribution of prime numbers. The prime number theorem asserts that $\Psi(n)\sim n$, so the asymptotic estimate $\log \text{l.c.m.}(1,\dots,n)\sim n$ is equivalent to the prime number theorem. The analogous asymptotic estimate for any linear polynomial $f(x)=ax+b$ is also known [Bat02] and it is a consequence of the prime number theorem for arithmetic progressions:

$$\log \text{l.c.m.}(f(1),\dots,f(n)) \sim n\frac{q}{\phi(q)}\sum_{\substack{1\leqslant k\leqslant q\\(k,q)=1}}\frac{1}{k}, \tag{1}$$

where $q=a/(a,b)$.

We address here the problem of estimating $\log \text{l.c.m.}(f(1),\dots,f(n))$ when f is an irreducible quadratic polynomial in $\mathbb{Z}[x]$. When f is a reducible quadratic polynomial the asymptotic estimate is similar to that we obtain for linear polynomials. This case is studied in section §4 with considerably less effort than the irreducible case. We state our main theorem.

Theorem 1. *For any irreducible quadratic polynomial $f(x)=ax^2+bx+c$ in $\mathbb{Z}[x]$ we have*

$$\log \textit{l.c.m.}\ (f(1),\dots,f(n)) = n\log n + Bn + o(n)$$

where $B=B_f$ is defined by the formula

$$B_f = \gamma - 1 - 2\log 2 - \sum_p \frac{(d/p)\log p}{p-1} + \frac{1}{\phi(q)}\sum_{\substack{1\leqslant r\leqslant q\\(r,q)=1}}\log\Big(1+\frac{r}{q}\Big) \tag{2}$$

$$+\log a + \sum_{p\mid 2aD}\log p\Big(\frac{1+(d/p)}{p-1} - \sum_{k\geqslant 1}\frac{s(f,p^k)}{p^k}\Big).$$

In this formula γ is the Euler constant, $D=b^2-4ac=dl^2$, where d is a fundamental discriminant, (d/p) is the Kronecker symbol, $q=a/(a,b)$ and $s(f,p^k)$ is the number of solutions of $f(x)\equiv 0 \pmod{p^k}$ which can be easily calculated using Lemma 2.

For the simplest case, $f(x)=x^2+1$, the constant B_f in Theorem 1 can be written as

$$B_f = \gamma - 1 - \frac{\log 2}{2} - \sum_{p\neq 2}\frac{(-1/p)\log p}{p-1}, \tag{3}$$

2000 Mathematics Subject Classification 2000 Mathematics Subject Classification: 11N37.

Keywords: least common multiple, quadratic sequences, equidistribution of roots of quadratic congruences

This work was supported by Grant MTM 2008-03880 of MYCIT (Spain)

where $(-1/p)$ is the Kronecker symbol (or Legendre symbol since p is odd) defined by $(-1/p)=(-1)^{\frac{p-1}{2}}$ when p is odd.

In section §3 we give an alternative expression for the constant B_f which is more convenient for numerical computations. As an example we will see that the constant B_f in (3) can be written as

$$\begin{aligned} B_f &= \gamma - 1 - \frac{\log 2}{2} + \sum_{k=1}^{\infty}\frac{\zeta'(2^k)}{\zeta(2^k)} + \sum_{k=0}^{\infty}\frac{L'(2^k,\chi_{-4})}{L(2^k,\chi_{-4})} - \sum_{k=1}^{\infty}\frac{\log 2}{2^{2^k}-1} \\ &= -0.0662756342130607063835631770 25... \end{aligned}$$

It would be interesting to extend our estimates to irreducible polynomials of higher degree, but we have found a serious obstruction in our argument. Some heuristic arguments and computations allow us to conjecture that the asymptotic estimate

$$\log \text{l.c.m. } (f(1),\dots,f(n)) \sim (\deg(f)-1)n\log n \tag{4}$$

holds for any irreducible polynomial f in $\mathbb{Z}[x]$ of degree $\deg(f)\geqslant 3$. In subsection 2.4 we explain the obstruction to prove this conjecture. There we also proof that

$$\log \text{l.c.m. } (f(1),\dots,f(n)) \sim n\log n \tag{5}$$

holds for any irreducible quadratic polynomial $f(x)$. Although this estimate is weaker than Theorem 1, the proof is easier.

To obtain the linear term in Theorem 1 we need a more involved argument. An important ingredient in this part of the proof is a deep result about the distribution of the solutions of the quadratic congruences $f(x)\equiv 0 \pmod p$ when p runs over all the primes. It was proved by Duke, Friedlander and Iwaniec [DFI95] (for $D<0$), and by Toth (for $D>0$). Actually we need a more general statement of this result, due to Toth.

Theorem 2 [Tot00]. *For any irreducible quadratic polynomial f in $\mathbb{Z}[x]$, the sequence*

$$\{\nu/p,\ 0\leqslant \nu < p\leqslant x,\ p\in S,\ f(\nu)\equiv 0 \pmod p\}$$

is well distributed in $[0,1)$ as x tends to infinity for any arithmetic progression S containing infinitely many primes p for which the congruence $f(x)\equiv 0 \pmod p$ has solutions.

Acknowledgment. We thank to Arpad Toth for clarifying the statement of Theorem 1.2 in [Tot00], to Guoyou Qian for detecting a mistake in a former version of Lemma 2, to Adolfo Quirós for conversations on some algebraic aspects of the problem, to Enrique González Jiménez for the calculations of some constants and to Fernando Chamizo for some suggestions and a carefully reading of the paper. Finally we thank to the anonymous referee for some valuable suggestions which have improved the quality of the presentation of this paper.

2. Proof of Theorem 1

2.1 Preliminaries

For $f(x)=ax^2+bx+c$ we define $D=b^2-4ac$ and

$$L_n(f)=\text{l.c.m.}(f(1),\dots,f(n)).$$

Since $L_n(f)=L_n(-f)$ we can assume that $a>0$. Also we can assume that b and c are nonnegative integers. If this is not the case, we consider a polynomial $f_k(x)=f(k+x)$ for a k such that $f_k(x)$ has nonnegative coefficients. Then we observe that $\log L_n(f)=\log L_n(f_k)+O_k(\log n)$ and that this error term is negligible for the statement of Theorem 1.

We define the numbers $\beta_p(n)$ by the formula

$$L_n(f)=\prod_p p^{\beta_p(n)} \tag{6}$$

where the product runs over all the primes p. The primes involved in this product are those for which the congruence $f(x) \equiv 0 \pmod p$ has some solution. Except for some special primes (those such that $p \mid 2aD$) the congruence $f(x) \equiv 0 \pmod p$ has 0 or 2 solutions. We will discus this in detail in Lemma 2.

We denote by $\mathcal{P}_f$ the set of non special primes for which the congruence $f(x) \equiv 0 \pmod p$ has exactly two solutions. More concretely

$$\mathcal{P}_f = \{p : \ p \nmid 2aD, \ (D/p) = 1\}$$

where (D/p) is the Kronecker symbol. This symbol is just the Legendre symbol when p is an odd prime.

The quadratic reciprocity law shows that the set $\mathcal{P}_f$ is the set of the primes lying in exactly $\varphi(4D)/2$ of the $\varphi(4D)$ arithmetic progressions modulo $4D$, coprimes with $4D$. As a consequence of the prime number theorem for arithmetic progressions we have

$$\#\{p \leqslant x : \ p \in \mathcal{P}_f\} \sim \frac{x}{2\log x}$$

or equivalently,

$$\sum_{\substack{0 \leqslant \nu < p \leqslant x \\ f(\nu) \equiv 0 \pmod p}} 1 \sim \frac{x}{\log x}.$$

Let $C = 2a + b$. We classify the primes involved in (6) in

- *Special* primes: those such that $p \mid 2aD$.

- $p \in \mathcal{P}_f$: $\begin{cases} \textit{Small} \text{ primes : } p < n^{2/3}. \\ \textit{Medium} \text{ primes: } n^{2/3} \leqslant p < Cn \ : \begin{cases} \textit{bad} \text{ primes: } p^2 \mid f(i) \text{ for some } i \leqslant n. \\ \textit{good} \text{ primes: } p^2 \nmid f(i) \text{ for any } i \leqslant n. \end{cases} \\ \textit{Large} \text{ primes: } Cn \leqslant p \leqslant f(n). \end{cases}$

We will use different strategies to deal with each class.

2.2 Large primes

We consider $P_n(f)$ and the numbers $\alpha_p(n)$ defined by

$$P_n(f) = \prod_{i=1}^{n} f(i) = \prod_p p^{\alpha_p(n)}. \tag{7}$$

Next lemma allow us to analyze the large primes involved in (6).

Lemma 1. *If $p \geqslant 2an + b$ then $\alpha_p(n) = \beta_p(n)$.*

Proof. If $\beta_p(n) = 0$ then $\alpha_p(n) = 0$. If $\alpha_p(n) > \beta_p(n) \geqslant 1$ then there exist $i < j \leqslant n$ such that $p \mid f(i)$ and $p \mid f(j)$. It implies that $p \mid f(j) - f(i) = (j-i)(a(j+i)+b)$. Thus $p \mid (j-i)$ or $p \mid a(j+i)+b$, which is not possible because $p \geqslant 2an + b$. □

Since $C = 2a + b$ we can write

$$\log L_n(f) = \log P_n(f) + \sum_{p < Cn} (\beta_p(n) - \alpha_p(n)) \log p. \tag{8}$$

Indeed we can take C to be any constant greater than $2a+b$. As we will see, the final estimate of $\log L_n(f)$ will not depend on C.

The estimate of $\log P_n(f)$ is easy:

$$\begin{aligned} \log P_n(f) &= \log \prod_{k=1}^{n} f(k) = \log \prod_{k=1}^{n} ak^2\Big(1 + \frac{b}{ka} + \frac{c}{k^2 a}\Big) \\ &= n \log a + \log(n!)^2 + \sum_{k=1}^{n} \log\Big(1 + \frac{b}{ka} + \frac{c}{k^2 a}\Big) \\ &= 2n \log n + n(\log a - 2) + O(\log n) \end{aligned} \tag{9}$$

and we obtain

$$\log L_n(f) = 2n\log n + n(\log a - 2) + \sum_{p<Cn}(\beta_p(n) - \alpha_p(n))\log p + O(\log n). \tag{10}$$

2.3 The number of solutions of $f(x) \equiv 0 \pmod{p^k}$ and the special primes

The number of solutions of the congruence $f(x) \equiv 0 \pmod{p^k}$ will play an important role in the proof of Theorem 1. We write $s(f, p^k)$ to denote this quantity.

The lemma below resumes all the casuistic for $s(f, p^k)$. We observe that except for a finite number of primes, those dividing $2aD$, we have that $s(f; p^k) = 2$ or 0 depending on $(D/p) = 1$ or -1.

Lemma 2. *Let $f(x) = ax^2 + bx + c$ be an irreducible polynomial and $D = b^2 - 4ac$.*

(i) *If $p \nmid 2a$, $D = p^l D_p$ and $(D_p, p) = 1$ then*

$$s(f, p^k) = \begin{cases} p^{\lfloor k/2 \rfloor}, & k \leqslant l \\ 0, & k > l,\ l \text{ odd or } (D_p/p) = -1 \\ 2p^{l/2}, & k > l,\ l \text{ even } \ (D_p/p) = 1. \end{cases}$$

(ii) *If $p \mid a$, $p \neq 2$ then* $s(f, p^k) = \begin{cases} 0, & \text{if } p \mid b \\ 1, & \text{if } p \nmid b. \end{cases}$

(iii) *If b is odd then, for all $k \geqslant 2$,* $s(f, 2^k) = s(f, 2) = \begin{cases} 1 \text{ if } a \text{ is even} \\ 0 \text{ if } a \text{ is odd and } c \text{ is odd} \\ 2 \text{ if } a \text{ is odd and } c \text{ is even.} \end{cases}$

(iv) *If b is even and a is even then $s(f, 2^k) = 0$ for any $k \geqslant 1$.*

(v) *If b is even and a is odd, let $D = 4^l D'$, $D' \not\equiv 0 \pmod 4$.*

(a) *If $k \leqslant 2l - 1$,* $\quad s(f; 2^k) = 2^{\lfloor k/2 \rfloor}$

(b) *If $k = 2l$,* $\quad s(f; 2^k) = \begin{cases} 2^l, & D' \equiv 1 \pmod 4 \\ 0, & D' \not\equiv 1 \pmod 4. \end{cases}$

(c) *If $k \geqslant 2l + 1$,* $\quad s(f; 2^k) = \begin{cases} 2^{l+1}, & D' \equiv 1 \pmod 8 \\ 0, & D' \not\equiv 1 \pmod 8. \end{cases}$

Proof. The proof is a consequence of elementary manipulations and Hensel's lemma. When the modulo is an odd prime p and $p \nmid a$, the congruence $ax^2 + bx + c \equiv 0 \pmod p$ is equivalent to the congruence $y^2 \equiv D \pmod p$. Hensel's lemma (see for example Theorem 123 in [HW08]) provides a method to obtain all the solutions of the congruence $y^2 \equiv D \pmod{p^{k+1}}$ from the solutions of $y^2 \equiv D \pmod{p^k}$. In this way we obtain all the distinct cases contained in part (i) of the lemma. Part (ii) is trivial and parts (iii),(iv) and (v) correspond to the case $p = 2$ which can be analyzed easily. □

Corollary 1. *If $p \nmid 2aD$ then $s(f, p^k) = 1 + (D/p)$.*

Proof. In this case, $l = 0$ and $D_p = D$ in Lemma 2. Thus $s(f, p^k) = 0 = 1 + (D/p)$ if $(D/p) = -1$ and $s(f, p^k) = 2 = 1 + (D/p)$ if $(D/p) = 1$. □

Lemma 3.

$$\alpha_p(n) = n\sum_{k\geqslant 1}\frac{s(f, p^k)}{p^k} + O\left(\frac{\log n}{\log p}\right). \tag{11}$$

where $s(f; p^k)$ denotes the number of solutions of $f(x) \equiv 0 \pmod{p^k}$, $0 \leqslant x < p^k$.

Proof. We observe that the maximum exponent $\alpha_{p,i}$ such that $p^{\alpha_{p,i}} \mid f(i)$ can be written as $\alpha_{p,i} = \sum_{k\geqslant 1,\ p^k \mid f(i)} 1$. Thus

$$\alpha_p(n) = \sum_{i\leqslant n}\alpha_{p,i} = \sum_{i\leqslant n}\sum_{\substack{k\geqslant 1 \\ p^k \mid f(i)}} 1 = \sum_{k\geqslant 1}\sum_{\substack{i\leqslant n \\ p^k \mid f(i)}} 1. \tag{12}$$

The trivial estimate

$$s(f;p^k)\left[\frac{n}{p^k}\right] \leqslant \sum_{i\leqslant n,\ p^k|f(i)} 1 \leqslant s(f;p^k)\left(\left[\frac{n}{p^k}\right]+1\right)$$

gives

$$\sum_{\substack{i\leqslant n\\ p^k|f(i)}} 1 = n\frac{s(f;p^k)}{p^k} + O(s(f;p^k)). \tag{13}$$

Putting (13) in (12) and observing that $k \leqslant \log f(n)/\log p$ and that $s(f,p^k) \ll 1$, we get

$$\alpha_p(n) = n\sum_{k\geqslant 1}\frac{s(f,p^k)}{p^k} + O\Big(\frac{\log n}{\log p}\Big).$$

□

Since $p^{\beta_p(n)} \leqslant f(n)$ we have always the trivial estimate

$$\beta_p(n) \leqslant \log f(n)/\log p \ll \log n/\log p. \tag{14}$$

When we substitute (14) and (11) in (10) for the special primes we obtain

$$\log L_n(f) = 2n\log n + n\left(\log a - 2 - \sum_{p|2aD}\sum_{k\geqslant 1}\frac{s(f,p^k)\log p}{p^k}\right) \tag{15}$$
$$+ \sum_{p<Cn,\ p\nmid 2aD}(\beta_p(n)-\alpha_p(n))\log p + O(\log n).$$

Lemma 3 has an easier formulation for non special primes.

Lemma 4. *For any $p \nmid 2aD$ we have*

$$\alpha_p(n) = n\frac{1+(D/p)}{p-1} + O\Big(\frac{\log n}{\log p}\Big). \tag{16}$$

Proof. It is a consequence of Lemma 3 and Corollary 1. □

2.4 The asymptotic estimate

This subsection is a break in the proof of Theorem 1 to prove, in an easy way, that the weaker estimate

$$\log \mathrm{l.c.m.}(f(1),\dots,f(n)) \sim n\log n \tag{17}$$

holds for any irreducible quadratic polynomial f.

We substitute (14) and (16) in (15) to obtain

$$\log L_n(f) = 2n\log n + \sum_{p<Cn,\ p\nmid 2aD}(\beta_p(n)-\alpha_p(n))\log p + O(n) \tag{18}$$
$$= 2n\log n - n\sum_{p<Cn,\ p\nmid 2aD}\frac{\log p}{p-1} - n\sum_{p<Cn,\ p\nmid 2aD}\frac{(D/p)\log p}{p-1} + O\left(\sum_{p<Cn}\log n\right) + O(n).$$

Now we get (17) using that $\sum_{p\leqslant x}\frac{\log p}{p-1} \sim \log x$ and that the sum $\sum_p \frac{(D/p)\log p}{p-1}$ is a convergent sum.

This is the moment to explain the main obstruction to obtain the analogous estimate for polynomials of degree $\deg(f) \geqslant 3$. For example we consider the polynomial $f(x) = x^3+2$. Using the same approach used in the quadratic case we get

$$\log L_n(f) = 3n\log n + \sum_{p<3n^2}(\beta_p(n)-\alpha_p(n))\log p + O(n). \tag{19}$$

We observe that the primes involved in the sum have the quadratic bound $3n^2$ instead the linear bound we have in the case of quadratic polynomials. The reason is that if $p \mid k^3+2$ and $p \mid j^3+2$ with $j < k \leqslant n$ we only can say that $p \leqslant 3n^2$.

It is easy to check that $\beta_p(n) \ll \log n/\log p$ and $\alpha_p(n) = n\frac{s_p}{p-1}+O(\log n/\log p)$ where s_p is the number of solutions of $x^3+2 \equiv 0 \pmod p$. Then we obtain

$$\log L_n(f) = 3n\log n - n\sum_{p<n}\frac{s_p\log p}{p-1} + O(n) + \sum_{n<p<3n^2}(\beta_p(n)-\alpha_p(n))\log p. \tag{20}$$

The Frobenius density theorem [LS96] implies that $s_p = 1$ in average, so $\sum_{p\leqslant x}\frac{s_p\log p}{p-1} \sim \log x$. Then, in the case $f(x) = x^3+2$ we have

$$\log L_n(f) = 2n\log n(1+o(1)) + \sum_{n<p<3n^2}(\beta_p(n)-\alpha_p(n))\log p. \tag{21}$$

We observe that $\beta_p(n) = \alpha_p(n)$ unless there exist $j < k \leqslant n$ such that $p \mid k^3+2,\ p \mid j^3+2$. In that case we have the trivial bound $|\beta_p(n)-\alpha_p(n)| \ll 1$. Thus, to obtain the asymptotic $\log L_n(f) \sim 2n\log n$ for $f(x) = x^3+2$ we should prove that

$$|\{p:\ n \leqslant p \leqslant 3n^2,\ p \mid k^3+2,\ p \mid j^3+2 \text{ for some } 1 \leqslant j < k \leqslant n\}| = o(n)$$

In general, when $f(x)$ is an irreducible polynomial, the asymptotic estimate $\log \text{l.c.m}(f(1),\dots,f(n)) \sim (\deg(f)-1)n\log n$ would follow from the estimate

$$|\{p:\ n \leqslant p \ll n^{\deg(f)-1},\ p \mid f(k),\ p \mid f(j) \text{ for some } 1 \leqslant j < k \leqslant n\}| = o(n). \tag{22}$$

This is obviously true when $\deg(f) = 2$ but we do not know how to prove it when $\deg(f) \geqslant 3$.

We come back to the proof of Theorem 1.

2.5 Medium primes

These primes can be also classified in bad and good primes. Bad primes are those p such that $p^2 \mid f(i)$ for some $i \leqslant n$. Good primes are those are not bad primes.

As we have seen in the previous section, for any prime $p \in \mathcal{P}_f$ the congruence $f(x) \equiv 0 \pmod p$ has exactly two solutions, say $0 \leqslant \nu_{p,1}, \nu_{p,2} < p$.

If p is a good prime, we have that $\alpha_p(n)$ is just the number of integers $i \leqslant n$ such that $p \mid f(i)$. All these integers have this form

$$\nu_{p,1}+kp, \quad 0 \leqslant k \leqslant \left[\frac{n-\nu_{p,1}}{p}\right] \tag{23}$$

$$\nu_{p,2}+kp, \quad 0 \leqslant k \leqslant \left[\frac{n-\nu_{p,2}}{p}\right]. \tag{24}$$

Also it is clear that if p is a good prime then $\beta_p(n) \leqslant 1$. These observations motivate the following definition:

Definition 1. *For any $p \in \mathcal{P}_f$ we define*

$$\alpha_p^*(n) = \left[\frac{n-\nu_{p,1}}{p}\right] + \left[\frac{n-\nu_{p,2}}{p}\right] + 2 \tag{25}$$

$$\beta_p^*(n) = \begin{cases} 1, & \textit{if } \beta_p(n) \geqslant 1 \\ 0, & \textit{otherwise.} \end{cases} \tag{26}$$

Lemma 5. *For any $p \in \mathcal{P}_f$ we have*

i) $\alpha_p(n) - \alpha_p^*(n) = \frac{2n}{p(p-1)} + O(\log n/\log p)$

ii) *$\alpha_p(n) = \alpha_p^*(n)$ and $\beta_p(n) = \beta_p^*(n)$ if $p^2 \nmid f(i)$ for any $i \leqslant n$.*

Proof. i) Lemma 4 implies that $\alpha_p(n)=\frac{2n}{p-1}+O(\log n/\log p)$ when $p\in\mathcal{P}_f$. On the other hand we have that $\alpha_p^*(n)=\frac{2n}{p}+O(1)$. Thus, $\alpha_p(n)-\alpha_p^*(n)=\frac{2n}{p(p-1)}+O(\log n/\log p)$.

ii) The first assertion has been explained at the beginning of the subsection. For the second, if $p\nmid f(i)$ for any $i\leqslant n$ then $\beta_p(n)=\beta_p^*(n)=0$. And if $p\mid f(i)$ for some $i\leqslant n$ we have that $\beta_p^*(n)=\beta_p(n)=1$ since $p^2\nmid f(i)$. □

By substituting (16) and (14) in (15) for small primes we obtain

$$\begin{aligned}\log L_n(f)=2n\log n+n&\left(\log a-2-\sum_{p\mid 2aD}\sum_{k\geqslant 1}\frac{s(f,p^k)\log p}{p^k}\right)\\&-\sum_{\substack{p<n^{2/3}\\ p\nmid 2aD}}\frac{(1+(D/p))\log p}{p-1}+\sum_{\substack{n^{2/3}\leqslant p<Cn\\ p\in\mathcal{P}_f}}(\beta_p(n)-\alpha_p(n))\log p+O(n^{2/3}).\end{aligned}\tag{27}$$

Now we split the last sum in (27) in

$$\begin{aligned}\sum_{\substack{n^{2/3}\leqslant p<Cn\\ p\in\mathcal{P}_f}}(\beta_p(n)-\alpha_p(n))\log p&=\sum_{\substack{n^{2/3}\leqslant p<Cn\\ p\in\mathcal{P}_f}}(\beta_p(n)-\beta_p^*(n)-\alpha_p(n)+\alpha_p^*(n))\log p\\&+\sum_{\substack{p<Cn\\ p\in\mathcal{P}_f}}\beta_p^*(n)\log p-\sum_{\substack{n^{2/3}\leqslant p<Cn\\ p\in\mathcal{P}_f}}\alpha_p^*(n)\log p+O(n^{2/3})\\&=S_1(n)+S_2(n)-S_3(n)+O(n^{2/3}).\end{aligned}\tag{28}$$

To estimate $S_1(n)$ we observe that Lemma 5 ii) implies that $\beta_p(n)-\beta_p^*(n)-\alpha_p(n)+\alpha_p^*(n)=0$ for any good prime p. On the other hand, Lemma 5 i) and (14) implies that $|\beta_p(n)-\beta_p^*(n)-\alpha_p(n)+\alpha_p^*(n)|\ll\log n/\log p$. Thus,

$$|S_1(n)|\ll\log n\ |\{p:\ n^{2/3}<p<Cn,\ p\text{ bad}\}|.\tag{29}$$

Lemma 6. *The number of bad primes $p\nmid D,\ Q\leqslant p<2Q$ is $\ll n^2/Q^2$.*

Proof. Let P_r the set of all primes p such that $f(i)=ai^2+bi+c=rp^2$ for some $i\leqslant n$. For $p\in P_r$ we have $(2ai+b)^2-4arp^2=D$ and then, $|\frac{2ai+b}{p}-2\sqrt{ra}|\ll\frac{1}{p^2}\ll\frac{1}{Q^2}$. We observe that all the fractions $\frac{2ai+b}{p},\ 1\leqslant i\leqslant n,\ Q\leqslant p<2Q$ are pairwise different. Otherwise $(2ai+b)p'=(2ai'+b)p$ and then $p\mid 2ai+b$. But it would imply that $p\mid(2ai+b)^2-4arp^2=D$, which is not possible. On the other hand, $\left|\frac{2ai+b}{p}-\frac{2ai'+b}{p'}\right|\geqslant\frac{1}{pp'}\gg\frac{1}{Q^2}$. Thus, the number of primes $p\in P_r$ lying in $[Q,2Q]$ is $\ll 1$. We finish the proof by observing that $r\leqslant f(n)/Q^2\ll n^2/Q^2$. □

Now, if we split the interval $[n^{2/3},Cn]$ in dyadic intervals and apply lemma above to each interval we obtain $|S_1(n)|\ll n^{2/3}\log n$.

To estimate $S_3(n)=\sum_{n^{2/3}<p<Cn,\ p\in\mathcal{P}_f}\alpha_p^*(n)$ we start by writing

$$\begin{aligned}\alpha_p^*(n)&=\left[\frac{n-\nu_{p,1}}{p}\right]+\left[\frac{n-\nu_{p,2}}{p}\right]+2\\&=\frac{2n}{p}+\Big(\frac{1}{2}-\frac{\nu_{p,1}}{p}\Big)+\Big(\frac{1}{2}-\frac{\nu_{p,2}}{p}\Big)+\frac{1}{2}-\left\{\frac{n-\nu_{p,1}}{p}\right\}+\frac{1}{2}-\left\{\frac{n-\nu_{p,2}}{p}\right\}.\end{aligned}$$

Thus

$$
\begin{aligned}
S_3(n) &= n \sum_{n^{2/3}<p<Cn} \frac{(1+(D/p))\log p}{p} &(30)\\
&+ \sum_{\substack{n^{2/3}<p<Cn\\ 0\leqslant\nu<p\\ f(\nu)\equiv 0 \pmod p}} \Big(\frac{1}{2}-\frac{\nu}{p}\Big)\log p + \sum_{\substack{n^{2/3}<p<Cn\\ 0\leqslant\nu<p\\ f(\nu)\equiv 0 \pmod p}} \Big(\frac{1}{2}-\Big\{\frac{n-\nu}{p}\Big\}\Big)\log p &(31)\\
&= n \sum_{n^{2/3}<p<Cn} \frac{(1+(D/p))\log p}{p-1} + O(n^{2/3}) &(32)\\
&+ \sum_{\substack{0\leqslant\nu<p<Cn\\ f(\nu)\equiv 0 \pmod p}} \Big(\frac{1}{2}-\frac{\nu}{p}\Big)\log p + \sum_{\substack{0\leqslant\nu<p<Cn\\ f(\nu)\equiv 0 \pmod p}} \Big(\frac{1}{2}-\Big\{\frac{n-\nu}{p}\Big\}\Big)\log p &(33)
\end{aligned}
$$

Substituting this in (28) and then in (27) we obtain

$$
\begin{aligned}
\log L_n(f) = 2n\log n + n\left(\log a - 2 - \sum_{p\mid 2aD}\sum_{k\geqslant 1}\frac{s(f,p^k)\log p}{p^k}\right) \qquad (34)\\
- \sum_{\substack{p<Cn\\ p\nmid 2aD}} \frac{(1+(D/p))\log p}{p-1} + S_2(n) - T_1(n) - T_2(n) + O(n^{2/3}\log n)
\end{aligned}
$$

where

$$
\begin{aligned}
S_2(n) &= \sum_{\substack{p<Cn\\ p\in\mathcal{P}_f}} \beta_p^*(n)\log p &(35)\\
T_1(n) &= \sum_{\substack{0\leqslant\nu<p<Cn\\ f(\nu)\equiv 0 \pmod p}} \Big(\frac{1}{2}-\frac{\nu}{p}\Big)\log p &(36)\\
T_2(n) &= \sum_{\substack{0\leqslant\nu<p<Cn\\ f(\nu)\equiv 0 \pmod p}} \Big(\frac{1}{2}-\Big\{\frac{n-\nu}{p}\Big\}\Big)\log p. &(37)
\end{aligned}
$$

Sums $T_1(n)$ and $T_2(n)$ will be $o(n)$ as a consequence of Theorem 2. But this is not completely obvious and we will provide a detailed proof in the next subsection.

First we will obtain in the next lemma a simplified expression for (34).

Lemma 7.

$$\log L_n(f) = n\log n + cn + S_2(n) - T_1(n) - T_2(n) + O(n^{2/3}\log n), \qquad (38)$$

where

$$c = \log a - \log C - 2 + \gamma - \sum_{p\nmid 2aD}\frac{(d/p)\log p}{p-1} + \sum_{p\mid 2aD}\log p\Big(\frac{1}{p-1} - \sum_{k\geqslant 1}\frac{s(f,p^k)}{p^k}\Big)$$

and $S_2(n)$, $T_1(n)$ *and* $T_2(n)$ *are as in* (35), (36) *and* (37).

Proof. Let $D = l^2 d$ where d is a fundamental discriminant. First we observe that $(D/p) = (l/p)^2(d/p)$ and that if $p \nmid D$ then $(D/p) = (d/p)$. As a consequence of the prime number theorem on arithmetic progressions we know that the sum $\sum_p \frac{(d/p)\log p}{p-1}$ is convergent. On the other hand, the well known estimate

$\sum_{p\leqslant x}\frac{\log p}{p-1}=\log x-\gamma+o(1)$ where γ is the Euler constant, implies that

$$\sum_{\substack{p<Cn\\ p\nmid 2aD}}\frac{(1+(D/p))\log p}{p-1}=\log n+\log C-\gamma-\sum_{p\mid 2aD}\frac{\log p}{p-1} \tag{39}$$
$$+\sum_{p\nmid 2aD}\frac{(d/p)\log p}{p-1}+o(1).$$

Finally we substitute (39) in (34). □

2.6 Equidistribution of the roots $\pmod p$ of a quadratic polynomial

Now we develop a method to prove that $T_1(n)$, $T_2(n)$ and other similar sums which will appear in the estimate of $S_2(n)$ are all $o(n)$. These sums are all of the form

$$\sum_{\substack{0\leqslant\nu<p\leqslant x,\ p\in S\\ f(\nu)\equiv 0\pmod p}} a(\nu,p,x)\log p \tag{40}$$

for some function $a(\nu,p,x)\ll 1$. By partial summation we also get easily that

$$\sum_{\substack{0\leqslant\nu<p\leqslant x,\ p\in S\\ f(\nu)\equiv 0\pmod p}} a(\nu,p,x)\log p=\log x\sum_{\substack{0\leqslant\nu<p\leqslant x,\ p\in S\\ f(\nu)\equiv 0\pmod p}} a(\nu,p,x)-\int_1^x\frac{1}{t}\sum_{\substack{0\leqslant\nu<p\leqslant t,\ p\in S\\ f(\nu)\equiv 0\pmod p}} a(\nu,p,x) \tag{41}$$
$$=\log x\sum_{\substack{0\leqslant\nu<p\leqslant x,\ p\in S\\ f(\nu)\equiv 0\pmod p}} a(\nu,p,x)+o(x/\log x). \tag{42}$$

Hence, to prove that the sums (40) are $o(x)$ we must show that

$$\sum_{\substack{0\leqslant\nu<p\leqslant x,\ p\in S\\ f(\nu)\equiv 0\pmod p}} a(\nu,p,x)=o(x/\log x).$$

Theorem 2 implies, in particular, that for any arithmetic progression S and for any piecewise continuos function g in $[0,1]$ such that $\int_0^1 g=0$ we have that

$$\sum_{\substack{0\leqslant\nu<p\leqslant x,\ p\in S\\ f(\nu)\equiv 0\pmod p}} g(\nu/p)=o(x/\log x). \tag{43}$$

Lemma 8. *Let f be an irreducible polynomial in $\mathbb{Z}[x]$. We have that the sums $T_1(n)$ and $T_2(n)$ defined in* (36) *and* (37) *are both $o(n)$.*

Proof. To prove that $T_1(n)=o(n)$ we apply (43) to the function $g(x)=x-1/2$.

To prove that $T_2(n)=o(n)$, the strategy is splitting the range of the primes in small intervals such that n/p are almost constant in each interval. We take H a large, but fixed number and we divide the interval $[1,Cn]$ in H intervals $L_h=(\frac{h-1}{H}Cn,\frac{h}{H}Cn],\ h=1,\dots,H$. Now we write

$$\sum_{\substack{0\leqslant\nu<p<n\\ f(\nu)\equiv 0\pmod p}}\left(\left\{\frac{n-\nu}{p}\right\}-\frac{1}{2}\right)=\Sigma_{31}+\Sigma_{32}+\Sigma_{33}+O(n/(H^{1/3}\log n)) \tag{44}$$

where

$$\Sigma_{31} = \sum_{H^{2/3}\leqslant h\leqslant H}\ \sum_{\substack{0\leqslant\nu<p\in L_h\\ f(\nu)\equiv 0 \pmod p}} \left(\left\{\frac{H}{h}-\frac{\nu}{p}\right\}-\frac{1}{2}\right)$$

$$\Sigma_{32} = \sum_{H^{2/3}\leqslant h\leqslant H}\ \sum_{\substack{0\leqslant\nu<p\in L_h\\ f(\nu)\equiv 0 \pmod p\\ \frac{\nu}{p}\notin[\frac{H}{h},\frac{H}{h-1}]}} \left(\left\{\frac{n}{p}-\frac{\nu}{p}\right\}-\left\{\frac{H}{h}-\frac{\nu}{p}\right\}\right)$$

$$\Sigma_{33} = \sum_{H^{2/3}\leqslant h\leqslant H}\ \sum_{\substack{0\leqslant\nu<p\in L_h\\ f(\nu)\equiv 0 \pmod p\\ \frac{\nu}{p}\in[\frac{H}{h},\frac{H}{h-1}]}} \left(\left\{\frac{n}{p}-\frac{\nu}{p}\right\}-\left\{\frac{H}{h}-\frac{\nu}{p}\right\}\right).$$

To estimate Σ_{31} we apply (43) with the function $\left\{\frac{H}{h}-x\right\}-\frac{1}{2}$ in each L_h and we obtain

$$\Sigma_{31} = o(Hn/\log n) = o(n\log n) \tag{45}$$

since H is a constant.

To bound Σ_{32} we observe that if $p\in L_h$ and $\frac{\nu}{p}\notin[\frac{H}{h},\frac{H}{h-1}]$, then

$$0\leqslant\left\{\frac{n}{p}-\frac{\nu}{p}\right\}-\left\{\frac{H}{h}-\frac{\nu}{p}\right\}=\frac{n}{p}-\frac{H}{h}\leqslant\frac{H}{h(h-1)}.$$

Thus

$$|\Sigma_{32}| \ll \sum_{H^{2/3}\leqslant h<H}\ \sum_{p\in L_h}\frac{H}{h^2} \ll \sum_{H^{2/3}\leqslant h<H}\ \sum_{p\in L_h}\frac{1}{H^{1/3}} \ll \frac{\pi(n)}{H^{1/3}} \ll \frac{n}{H^{1/3}\log n}. \tag{46}$$

To bound Σ_{33} first we observe that

$$\begin{aligned}\Sigma_{33} &\ll \sum_{H^{2/3}\leqslant h<H}\ \sum_{\substack{0\leqslant\nu<p\in L_h\\ f(\nu)\equiv 0 \pmod p\\ \frac{\nu}{p}\in[\frac{H}{h},\frac{H}{h-1}]}} 1\\ &= \sum_{H^{2/3}\leqslant h<H}\ \sum_{\substack{0\leqslant\nu<p\in L_h\\ f(\nu)\equiv 0 \pmod p}} \left(\chi_{[H/h,H/(h-1)]}(\nu/p)-\frac{H}{h(h-1)}\right)\\ &+ \sum_{H^{2/3}\leqslant h<H}\ \sum_{\substack{0\leqslant\nu<p\in L_h\\ f(\nu)\equiv 0 \pmod p}} \frac{H}{h(h-1)},\end{aligned}$$

where, here and later, $\chi_{[a,b]}(x)$ denotes the characteristic function of the interval $[a,b]$.

Theorem 2 implies that

$$\sum_{\substack{0\leqslant\nu<p\in L_h\\ f(\nu)\equiv 0 \pmod p}} \left(\chi_{[H/h,H/(h-1)]}(\nu/p)-\frac{H}{h(h-1)}\right) = o(n/\log n).$$

Thus,

$$\begin{aligned}\Sigma_{33} &\ll \sum_{H^{2/3}\leqslant h<H} o(\frac{n}{\log n}) + \sum_{H^{2/3}\leqslant h<H}\ \sum_{\substack{0\leqslant\nu<p\in L_h\\ f(\nu)\equiv 0 \pmod p}}\frac{1}{H^{1/3}}\\ &\ll o(n/\log n)+\frac{\pi(n)}{H^{1/3}} \ll o(n/\log n)+O(n/(H^{1/3}\log n)).\end{aligned} \tag{47}$$

Estimates (45), (46) and (47) imply $\Sigma_3 \ll o(n/\log n)+n/(H^{1/3}\log n)$. Since H can be chosen arbitrarily large, we have that $\Sigma_3 = o(n/\log n)$ which finishes the proof. □

To present Lemma 10 we need some previous considerations.

For primes $p \in \mathcal{P}_f$ the congruence $f(x) \equiv 0 \pmod p$ has exactly two solutions, say $0 \leqslant \nu_{p,1},\ \nu_{p,2} < p$.

In some parts of the proof of Theorem 1 we will need to estimate some quantities depending on $\min(\nu_{p,1}, \nu_{p,2})$. For this reason it is convenient to know how they are related.

If $f(x) = ax^2 + bx + c$ and $p \in \mathcal{P}_f$ then $\nu_{p,1} + \nu_{p,2} \equiv -b/a \pmod p$. The next lemma will give more information when the prime p belongs to some particular arithmetic progression.

Lemma 9. *Let $q = a/(a,b),\ l = b/(a,b)$. For any $r,\ (r,q) = 1$ and for any prime $p \equiv lr^{-1} \pmod q$ and $p \in \mathcal{P}_f$ we have*

$$\frac{\nu_{p,1}}{p} + \frac{\nu_{p,2}}{p} \equiv \frac{r}{q} - \frac{l}{pq} \pmod 1. \tag{48}$$

Proof. To avoid confusions we denote by $\overline{q}_p$ and $\overline{p}_q$ the inverses of $q \pmod p$ and $p \pmod q$ respectively. From the obvious congruence $q\overline{q}_p + p\overline{p}_q \equiv 1 \pmod{pq}$ we deduce that $\frac{\overline{q}_p}{p} + \frac{\overline{p}_q}{q} - \frac{1}{pq} \in \mathbb{Z}$. Since $p \equiv l\overline{r}_q \pmod q$ we obtain $\frac{\overline{q}_p}{p} \equiv \frac{1}{pq} - \frac{r\bar{l}_q}{q} \pmod 1$. Thus

$$\frac{\nu_{p,1}}{p} + \frac{\nu_{p,2}}{p} \equiv \frac{-l\overline{q}_p}{p} \equiv -l\left(\frac{1}{pq} - \frac{r\bar{l}_q}{q}\right) \equiv \frac{r}{q} - \frac{l}{pq} \pmod 1.$$

□

Since the two roots are symmetric respect to $\frac{r}{2q} - \frac{l}{2pq}$, necessarily one of then lies in $\left[\frac{r}{2q} - \frac{l}{2pq}, \frac{1}{2} + \frac{r}{2q} - \frac{l}{2pq}\right) \pmod 1$ and the other in the complementary set.

Definition 2. *For $(r,q) = 1,\ 1 \leqslant r \leqslant q,\ p \equiv lr^{-1} \pmod q$ and $p \in \mathcal{P}_f$ we define $\nu_{p,1}$ the root of $f(x) \equiv \pmod p$ such that*

$$\frac{\nu_{p,1}}{p} \in T_{rp} = \left[\frac{r}{2q} - \frac{l}{2pq}, \frac{1}{2} + \frac{r}{2q} - \frac{l}{2pq}\right) \pmod 1,$$

and we define $\nu_{p,2}$ the root of $f(x) \equiv 0 \pmod p$ such that $\frac{\nu_{p,2}}{p} \in [0,1) \setminus T_{rp}$.

Lemma 10. *Assume the notation above. Let $\alpha_1, \alpha_2, \beta_1, \beta_2, c_1, c_2$ be constants and $g_1(x), g_2(x)$ two linear functions satisfying that*

$$J_n(p) = \left[g_1\left(\frac{n}{p}\right) + \frac{c_1}{p}, g_2\left(\frac{n}{p}\right) + \frac{c_2}{p}\right] \subset T_{rp}$$

for any prime $p \in K_n = [\alpha_1 n + \beta_1, \alpha_2 n + \beta_2]$. We have

$$\sum_{\substack{p \in K_n \cap \mathcal{P}_f \\ p \equiv lr^{-1} \pmod q}} \left(\chi_{J_n(p)}\left(\frac{\nu_{p,1}}{p}\right) - 2|J_n(p)|\right) \log p = o(n) \tag{49}$$

where χ_I is the characteristic function of the set I.

Proof. Since $J_n(p) \subset T_{rp}$ then $\nu_2/p \notin J_n(p)$ and we can write

$$\sum_{\substack{p \in K_n \cap \mathcal{P}_f \\ p \equiv lr^{-1} \pmod q}} \chi_{J_n(p)}\left(\frac{\nu_{p,1}}{p}\right) \log p = \sum_{\substack{1 \leqslant \nu \leqslant p \in K_n, \\ f(\nu) \equiv 0 \pmod p \\ p \equiv lr^{-1} \pmod q}} \chi_{J_n(p)}\left(\frac{\nu}{p}\right) \log p$$

and

$$\sum_{\substack{p \in K_n \cap \mathcal{P}_f \\ p \equiv lr^{-1} \pmod q}} 2|J_n(p)| \log p = \sum_{\substack{1 \leqslant \nu \leqslant p \in K_n, \\ f(\nu) \equiv 0 \pmod p \\ p \equiv lr^{-1} \pmod q}} |J_n(p)| \log p.$$

Thus,

$$\sum_{\substack{p \in K_n \cap \mathcal{P}_f \\ p \equiv lr^{-1} \pmod q}} \left(\chi_{J_n(p)}\left(\frac{\nu_{p,1}}{p}\right) - 2|J_n(p)|\right) \log p = \sum_{\substack{1 \leqslant \nu \leqslant p \in K_n, \\ f(\nu) \equiv 0 \pmod p \\ p \equiv lr^{-1} \pmod q}} \left(\chi_{J_n(p)}\left(\frac{\nu}{p}\right) - |J_n(p)|\right) \log p.$$

The proof will be accomplished by showing that

$$\sum_{\substack{1\leqslant \nu\leqslant p\in K_n,\\ f(\nu)\equiv 0 \pmod p\\ p\equiv lr^{-1} \pmod q}} \left(\chi_{J_n(p)}\Big(\frac{\nu}{p}\Big)-|J_n(p)|\right)=o(n/\log n). \tag{50}$$

We split K_n in intervals $L_h=(\frac{h-1}{H}n,\frac{h}{H}n]$ of length n/H and two extra intervals $I,\ F$ (the initial and the final intervals) of length $\leqslant n/H$. Here h runs over a suitable set of consecutive integers $\mathcal{H}$ of cardinality $\ll (\alpha_2-\alpha_1)H$.

Let I_h denote the interval $[g_1(H/h)+c_1H/(nh), g_2(H/h)+c_2H/(nh)]$.

We write

$$\sum_{\substack{1\leqslant \nu\leqslant p\in K_n,\\ f(\nu)\equiv 0 \pmod p\\ p\equiv lr^{-1} \pmod q}} \left(\chi_{J_n(p)}\Big(\frac{\nu}{p}\Big)-|J_n(p)|\right)=\Sigma_1+\Sigma_2+\Sigma_3+\Sigma_4 \tag{51}$$

where

$$\begin{aligned}
\Sigma_1 &= \sum_{h\in\mathcal{H}}\ \sum_{\substack{0\leqslant\nu<p\in L_h\\ f(\nu)\equiv 0 \pmod p\\ p\equiv lr^{-1} \pmod q}} \left(\chi_{I_h}\Big(\frac{\nu}{p}\Big)-|I_h|\right)\\
\Sigma_2 &= \sum_{h\in\mathcal{H}}\ \sum_{\substack{0\leqslant\nu<p\in L_h\\ f(\nu)\equiv 0 \pmod p\\ p\equiv lr^{-1} \pmod q}} (|I_h|-|J_n(p)|)\\
\Sigma_3 &= \sum_{h\in\mathcal{H}}\ \sum_{\substack{0\leqslant\nu<p\in L_h\\ f(\nu)\equiv 0 \pmod p\\ p\equiv lr^{-1} \pmod q}} \left(\chi_{J_n(p)}\Big(\frac{\nu}{p}\Big)-\chi_{I_h}\Big(\frac{\nu}{p}\Big)\right)\\
\Sigma_4 &= \sum_{\substack{0\leqslant\nu<p\in I\cup F\\ f(\nu)\equiv 0 \pmod p\\ p\equiv lr^{-1} \pmod q}} \left(\chi_{I_h}\Big(\frac{\nu}{p}\Big)-|J_n(p)|\right).
\end{aligned}$$

The inner sum in Σ_1 can be estimated as we did in Lemma 8, (with the function $g(x)=\chi_I(x)-|I|$ instead of $g(x)=x-1/2$), and we get again that $\Sigma_1=o(n/\log n)$.

To estimate Σ_2 and Σ_3 we observe that if $p\in L_h$ then $J_n(p)$ and I_h are almost equal. Actually, comparing the end points of both intervals and because g is a linear function, we have that and $\chi_{J_n(p)}(x)=\chi_{I_h}(x)$ except for an interval (or union of two intervals) E_h of measure

$$|E_h|\ll \min(1,H/h^2).$$

In particular, the estimate $||J_n(p)|-|I_h||\ll\min(1,H/h^2)$ holds.

Thus, we have

$$\begin{aligned}
\Sigma_2 &\ll \sum_{h\in\mathcal{H}}\sum_{p\in L_n}\min(1,H/h^2)\ll \sum_{h\leqslant H^{2/3}}\sum_{p\in L_h}1+\sum_{H^{2/3}<h\in\mathcal{H}}\sum_{p\in L_h}\frac{1}{H^{1/3}}\\
&\ll \pi(n/H^{1/3})+\frac{1}{H^{1/3}}\pi(\alpha_1 n+\alpha_2)\ll n/(H^{1/3}\log n).
\end{aligned}$$

To bound Σ_3 first we observe that

$$\begin{aligned}\Sigma_3 &\ll \sum_{h\in\mathcal{H}} \sum_{\substack{0\leqslant\nu<p\in L_h\\ f(\nu)\equiv 0 \pmod p\\ p\equiv lr^{-1} \pmod q}} \chi_{E_h}(\nu/p)\\ &= \sum_{h\in\mathcal{H}} \sum_{\substack{0\leqslant\nu<p\in L_h\\ f(\nu)\equiv 0 \pmod p\\ p\equiv lr^{-1} \pmod q}} (\chi_{E_h}(\nu/p)-|E_h|) + \sum_{h\in\mathcal{H}} \sum_{\substack{0\leqslant\nu<p\in L_h\\ f(\nu)\equiv 0 \pmod p\\ p\equiv lr^{-1} \pmod q}} |E_h|.\end{aligned}$$

Theorem 2 implies that

$$\sum_{\substack{0\leqslant\nu<p\in L_h\\ f(\nu)\equiv 0 \pmod p\\ p\equiv lr^{-1} \pmod q}} (\chi_{E_h}(\nu/p)-|E_h|) = o(n/\log n).$$

On the other hand,

$$\begin{aligned}\sum_{h\in\mathcal{H}} \sum_{\substack{0\leqslant\nu<p\in L_h\\ f(\nu)\equiv 0 \pmod p\\ p\equiv lr^{-1} \pmod q}} |E_h| &\ll \sum_{h\leqslant H^{2/3}} \sum_{p\in L_h} 1 + \sum_{H^{2/3}<h\in\mathcal{H}} \sum_{p\in L_h} \frac{H}{h^2}\\ &\ll \pi(n/H^{1/3}) + \frac{1}{H^{1/3}}\pi(\alpha_1 n+\alpha_2)\\ &\ll \frac{n}{H^{1/3}\log n}.\end{aligned}$$

Thus, $\Sigma_3 \ll o(n/\log n) + n/(H^{1/3}\log n)$.

Finally we estimate Σ_4. We observe that

$$|\Sigma_4| \leqslant \sum_{p\in I} 1 + \sum_{p\in F} 1 \ll n/(H\log n)$$

as a consequence of the prime number theorem. Then

$$\Sigma_1+\Sigma_2+\Sigma_3+\Sigma_4 = O(n/(H^{1/3}\log n)) + O(n/(H\log n)) + o(n/\log n)$$

finishing the proof because we can take H arbitrarily large. □

2.7 Estimate of $S_2(n)$ and end of the proof

Lemma 11.

$$S_2(n) = n\Big(1+\log C - \log 4 + \frac{1}{\phi(q)}\sum_{(r,q)=1}\log(1+\frac{r}{q})\Big) + o(n) \tag{52}$$

Proof. Following the notation of Lemma 9 we split

$$S_2(n) = \sum_{\substack{(r,q)=1\\ 1\leqslant r\leqslant q}} S_{2r}(n) + \sum_{p\leqslant l}\beta_p^*(n)\log p = \sum_{\substack{(r,q)=1\\ 1\leqslant r\leqslant q}} S_{2r}(n) + O(1)$$

where

$$S_{2r}(n) = \sum_{\substack{l<p\leqslant Cn\\ p\equiv lr^{-1} \pmod q}} \beta_p^*(n)\log p. \tag{53}$$

Since $p\equiv lr^{-1} \pmod q$, Lemma 9 implies that $\frac{\nu_{p,1}}{p}+\frac{\nu_{p,2}}{p} \equiv \frac{r}{q}-\frac{l}{pq} \pmod 1$. We observe also that, since $p>l$ we have that $0<\frac{r}{q}-\frac{l}{pq}\leqslant 1$.

Now we will check that

$$\beta_p^*(n) = \begin{cases} 1, & \text{if} \quad \frac{n}{p} \geqslant \frac{1}{2} + \frac{r}{2q} - \frac{l}{2pq} \\ \chi_{[\frac{r}{2q}-\frac{l}{2pq},\frac{n}{p}]}(\nu_{p,1}/p), & \text{if} \quad \frac{r}{q} - \frac{l}{pq} < \frac{n}{p} < \frac{1}{2} + \frac{r}{2q} - \frac{l}{2pq} \\ \chi_{[\frac{r}{2q}-\frac{l}{2pq},\frac{r}{q}-\frac{l}{pq}]}(\nu_{p,1}/p), & \text{if} \quad \frac{r}{2q} - \frac{l}{2pq} \leqslant \frac{n}{p} \leqslant \frac{r}{q} - \frac{l}{pq} \\ \chi_{[\frac{r}{q}-\frac{l}{pq}-\frac{n}{p},\frac{r}{q}-\frac{l}{pq}]}(\nu_{p,1}/p) & \text{if} \quad \frac{n}{p} < \frac{r}{2q} - \frac{l}{2pq} \end{cases}$$

We observe that $\beta_p^*(n) = 1$ if and only if $\frac{\nu_{p,1}}{p} \leqslant \frac{n}{p}$ or $\frac{\nu_{p,2}}{p} \leqslant \frac{n}{p}$. We remind that

$$\frac{r}{2q} - \frac{l}{2pq} \leqslant \frac{\nu_{p,1}}{p} < \frac{1}{2} + \frac{r}{2q} - \frac{l}{2pq} \tag{54}$$

Also we observe that Lemma 9 implies that

$$\frac{\nu_{p,2}}{p} = \begin{cases} \frac{r}{q} - \frac{l}{pq} - \frac{\nu_{p,1}}{p} & \text{if } \frac{\nu_{p,1}}{p} \leqslant \frac{r}{q} - \frac{l}{pq} \\ \frac{r}{q} - \frac{l}{pq} - \frac{\nu_{p,1}}{p} + 1 & \text{if } \frac{\nu_{p,1}}{p} > \frac{r}{q} - \frac{l}{pq}. \end{cases} \tag{55}$$

- Assume $\frac{n}{p} \geqslant \frac{1}{2} + \frac{r}{2q} - \frac{l}{2pq}$. Then $\nu_{p,1} < p\left(\frac{1}{2} + \frac{r}{2q} - \frac{l}{2pq}\right) < n$, so $\beta_p^*(n) = 1$

- Assume $\frac{r}{q} - \frac{l}{pq} < \frac{n}{p} < \frac{1}{2} + \frac{r}{2q} - \frac{l}{2pq}$.

  * If $\chi_{[\frac{r}{2q}-\frac{l}{2pq},\frac{n}{p}]}(\nu_{p,1}/p) = 1$ then $\nu_{p,1} \leqslant n$, so $\beta_p^*(n) = 1$.
  * If $\chi_{[\frac{r}{2q}-\frac{l}{2pq},\frac{n}{p}]}(\nu_{p,1}/p) = 0$ then $\frac{\nu_{p,1}}{p} > \frac{n}{p} > \frac{r}{q} - \frac{l}{pq}$. Relations (54) and (55) imply that $\frac{\nu_{p,2}}{p} = 1 + \frac{r}{q} - \frac{l}{pq} - \frac{\nu_{p,1}}{p} > \frac{1}{2} + \frac{r}{2q} - \frac{l}{2pq} > \frac{n}{p}$. Since $\nu_{p,1} > n$ and $\nu_{p,2} > n$ we get $\beta_p^*(n) = 0$.

- Assume $\frac{r}{2q} - \frac{l}{2pq} \leqslant \frac{n}{p} \leqslant \frac{r}{q} - \frac{l}{pq}$.

  * If $\chi_{[\frac{r}{2q}-\frac{l}{2pq},\frac{r}{q}-\frac{l}{pq}]}(\nu_{p,1}/p) = 1$ then (55) imply that $0 < \frac{\nu_{p,2}}{p} \leqslant \frac{r}{2q} - \frac{l}{2pq}$, which implies that $\nu_{p,2} \leqslant n$, so $\beta_p^*(n) = 1$.
  * If $\chi_{[\frac{r}{2q}-\frac{l}{2pq},\frac{r}{q}-\frac{l}{pq}]}(\nu_{p,1}/p) = 0$ then $\frac{\nu_{p,1}}{p} > \frac{r}{q} - \frac{l}{pq} \geqslant \frac{n}{p}$ and relation (55) imply that $\frac{\nu_{p,2}}{p} = \frac{r}{q} - \frac{l}{pq} - \frac{\nu_{p,1}}{p} + 1 > \frac{r}{q} - \frac{l}{pq} \geqslant \frac{n}{p}$. Since $\nu_{p,1} > n$ and $\nu_{p,2} > n$ we get $\beta_p^*(n) = 0$.

- Assume $\frac{n}{p} < \frac{r}{2q} - \frac{l}{2pq}$.

  * If $\chi_{[\frac{r}{q}-\frac{l}{pq}-\frac{n}{p},\frac{r}{q}-\frac{l}{pq}]}(\nu_{p,1}/p) = 1$ then $\frac{\nu_{p,1}}{p} \leqslant \frac{r}{q} - \frac{l}{pq}$ and relation (55) implies that $\frac{\nu_{p,2}}{p} = \frac{r}{q} - \frac{l}{pq} - \frac{\nu_{p,1}}{p} \leqslant \frac{r}{q} - \frac{l}{pq} - (\frac{r}{q} - \frac{l}{pq} - \frac{n}{p}) = \frac{n}{p}$, so $\beta_p^*(n) = 1$
  * If $\chi_{[\frac{r}{q}-\frac{l}{pq}-\frac{n}{p},\frac{r}{q}-\frac{l}{pq}]}(\nu_{p,1}/p) = 0$ we distinguish two cases:

    · If $\frac{r}{2q} - \frac{l}{2q} \leqslant \frac{\nu_{p,1}}{p} < \frac{r}{q} - \frac{l}{pq} - \frac{n}{p}$ then $\frac{\nu_{1,p}}{p} \geqslant \frac{r}{2q} - \frac{l}{2q} > \frac{n}{p}$, and also we have that $\frac{\nu_{p,2}}{p} = \frac{r}{q} - \frac{l}{pq} - \frac{\nu_{p,1}}{p} > \frac{r}{q} - \frac{l}{pq} - \left(\frac{r}{q} - \frac{l}{pq} - \frac{n}{p}\right) = \frac{n}{p}$. Thus $\beta_p^*(n) = 0$

    · If $\frac{r}{q} - \frac{l}{pq} < \frac{\nu_{p,1}}{p} < \frac{1}{2} + \frac{r}{2q} - \frac{l}{2pq}$ then $\frac{\nu_{p,1}}{p} > \frac{1}{2}\left(\frac{r}{q} - \frac{l}{pq}\right) > \frac{n}{p}$. On the other hand, $\frac{\nu_{p,2}}{p} = \frac{r}{q} - \frac{l}{pq} - \frac{\nu_{p,1}}{p} + 1 > \frac{r}{q} - \frac{l}{pq} - \left(\frac{1}{2} + \frac{r}{2q} - \frac{l}{2pq}\right) + 1 = \frac{1}{2} + \frac{r}{2q} - \frac{l}{2pq} > \frac{n}{p}$. Thus, again we have that $\beta_p^*(n) = 0$.

Now we split $S_{2r}(n)=\sum_{i=1}^{4} S_{2ri}(n)$ according the ranges of the primes involved in the lemma above.

$$\begin{aligned}
S_{2r1}(n) &= \sum_{\substack{l<p\leqslant \frac{n+l/(2q)}{1/2+r/(2q)}\\ p\equiv lr^{-1}\pmod q\\ p\in\mathcal{P}_f}} \log p\\
S_{2r2}(n) &= \sum_{\substack{\frac{n+l/(2q)}{1/2+r/(2q)}<p<\frac{n+l/q}{r/q}\\ p\equiv lr^{-1}\pmod q\\ p\in\mathcal{P}_f}} \chi_{[\frac{r}{2q}-\frac{l}{2pq},\frac{n}{p}]}(\nu_{p,1}/p)\log p\\
S_{2r3}(n) &= \sum_{\substack{\frac{q}{r}(n+\frac{l}{q})\leqslant p\leqslant \frac{2q}{r}(n+\frac{l}{q})\\ p\equiv lr^{-1}\pmod q\\ p\in\mathcal{P}_f}} \chi_{[\frac{r}{2q}-\frac{l}{2pq},\frac{r}{q}-\frac{l}{pq}]}(\nu_{p,1}/p)\log p\\
S_{2r4}(n) &= \sum_{\substack{\frac{2q}{r}(n+\frac{l}{2q})<p<Cn\\ p\equiv lr^{-1}\pmod q\\ p\in\mathcal{P}_f}} \chi_{[\frac{r}{q}-\frac{l}{pq}-\frac{n}{p},\frac{r}{q}-\frac{l}{pq}]}(\nu_{p,1}/p)\log p.
\end{aligned}$$

Since $(q,D)=1$ and the primes are odd numbers, the primes $p\equiv lr^{-1}\pmod q$, $p\in\mathcal{P}_f$ lie in a set of $\phi(4qD)/(2\phi(q))$ arithmetic progressions modulo $4qD$. The prime number theorem for arithmetic progressions implies that

$$\sum_{\substack{p\leqslant x\\ p\equiv lr^{-1}\pmod q,\ p\in P_f}} \log p \sim \frac{x}{2\phi(q)} \tag{56}$$

and

$$\sum_{\substack{ax<p\leqslant bx\\ p\equiv lr^{-1}\pmod q,\ p\in P_f}} \frac{\log p}{p} = \frac{\log(b/a)}{2\phi(q)}+o(1) \tag{57}$$

We will use these estimates and lema 10 to estimate $S_{2ri}(n),\ i=1,2,3,4$.

By (56) we have

$$S_{2r1}(n)=\frac{n}{\phi(q)}\frac{q}{q+r}+o(n). \tag{58}$$

To estimate S_{2r2} we write

$$\begin{aligned}
S_{2r2}(n) &= \sum_{\substack{\frac{n+l/(2q)}{1/2+r/(2q)}<p<\frac{n+l/q}{r/q}\\ p\equiv lr^{-1}\pmod q}} \chi_{[\frac{r}{2q}-\frac{l}{2pq},\frac{n}{p}]}(\nu_{p,1}/p)\log p\\
&= \sum_{\substack{\frac{n+l/(2q)}{1/2+r/(2q)}<p<\frac{n+l/q}{r/q}\\ p\equiv lr^{-1}\pmod q}} \Big(\frac{2n}{p}-\frac{r}{q}+\frac{l}{pq}\Big)\log p\\
&+ \sum_{\substack{\frac{n+l/(2q)}{1/2+r/(2q)}<p<\frac{n+l/q}{r/q}\\ p\equiv lr^{-1}\pmod q}} \Big(\chi_{[\frac{r}{2q}-\frac{l}{2pq},\frac{n}{p}]}(\nu_{p,1}/p)-2\Big(\frac{n}{p}-\frac{r}{2q}+\frac{l}{2pq}\Big)\Big)\log p
\end{aligned}$$

Lemma 10 implies that the last sum is $o(n)$. Thus,

$$\begin{aligned}
S_{2r2} &= \sum_{\substack{\frac{n+l/(2q)}{1/2+r/(2q)}<p<\frac{n+l/q}{r/q} \\ p\equiv lr^{-1} \pmod q \\ p\in\mathcal{P}_f}} \Big(\frac{2n}{p}-\frac{r}{q}\Big)\log p + o(n) \\
&= 2n \sum_{\substack{\frac{n+l/(2q)}{1/2+r/(2q)}<p<\frac{n+l/q}{r/q} \\ p\equiv lr^{-1} \pmod q \\ p\in\mathcal{P}_f}} \frac{\log p}{p} - \frac{r}{q} \sum_{\substack{\frac{n+l/(2q)}{1/2+r/(2q)}<p<\frac{n+l/q}{r/q} \\ p\equiv lr^{-1} \pmod q \\ p\in\mathcal{P}_f}} \log p + o(n) \\
&= \frac{n}{\phi(q)}\log\Big(\frac{1}{2}+\frac{q}{2r}\Big) - \frac{n}{\phi(q)}\Big(\frac{1}{2}-\frac{r}{q+r}\Big) + o(n)
\end{aligned}$$

by (56) and (57).

To estimate $S_{2r3}(n)$ we write

$$\begin{aligned}
S_{2r3}(n) &= \sum_{\substack{\frac{q}{r}(n+\frac{l}{q})\leqslant p\leqslant\frac{2q}{r}(n+\frac{l}{q}) \\ p\equiv lr^{-1} \pmod q \\ p\in\mathcal{P}_f}} \Big(\frac{r}{q}-\frac{l}{pq}\Big)\log p \\
&+ \sum_{\substack{\frac{q}{r}(n+\frac{l}{q})\leqslant p\leqslant\frac{2q}{r}(n+\frac{l}{q}) \\ p\equiv lr^{-1} \pmod q \\ p\in\mathcal{P}_f}} \Big(\chi_{[\frac{r}{2q}-\frac{l}{2pq},\frac{r}{q}-\frac{l}{pq}]}(\nu_{p,1}/p) - \Big(\frac{r}{q}-\frac{l}{pq}\Big)\Big)\log p \\
&= \frac{n}{2\phi(q)} + o(n)
\end{aligned}$$

by (56) and lema 10.

To estimate $S_{2r4}(n)$ we write

$$\begin{aligned}
S_{2r4}(n) &= \sum_{\substack{\frac{2q}{r}(n+\frac{l}{2q})<p<Cn \\ p\equiv lr^{-1} \pmod q \\ p\in\mathcal{P}_f}} \Big(\frac{2n}{p}+\frac{2l}{pq}\Big)\log p \\
&= \sum_{\substack{\frac{2q}{r}(n+\frac{l}{2q})<p<Cn \\ p\equiv lr^{-1} \pmod q \\ p\in\mathcal{P}_f}} \Big(\chi_{[\frac{r}{q}-\frac{l}{pq}-\frac{n}{p},\frac{r}{q}-\frac{l}{pq}]}(\nu_{p,1}/p) - \Big(\frac{2n}{p}+\frac{2l}{pq}\Big)\Big)\log p \\
&= \frac{n}{\phi(q)}\Big(\log C - \log(2q/r)\Big) + o(n)
\end{aligned}$$

by (57) and Lemma 10.

Thus

$$\begin{aligned}
S_{2r}(n) &= S_{2r1}(n) + S_{2r2}(n) + S_{2r3}(n) + S_{2r4}(n) + O(1) \\
&= \frac{n}{\phi(q)}\frac{q}{q+r} + o(n) \\
&+ \frac{n}{\phi(q)}\log\Big(\frac{1}{2}+\frac{q}{2r}\Big) - \frac{n}{\phi(q)}\Big(\frac{1}{2}-\frac{r}{q+r}\Big) + o(n) \\
&+ \frac{n}{2\phi(q)} + o(n) \\
&+ \frac{n}{\phi(q)}\Big(\log C - \log(2q/r)\Big) + o(n) \\
&= \frac{n}{\phi(q)}\Big(1 + \log C - \log 4 + \log(1+r/q)\Big) + o(n).
\end{aligned}$$

Now sum in all $r \leqslant q$, $(r,q)=1$ to finish the estimate of $S_2(n)$. □

Finally we substitute (52) in (38) to conclude the proof of Theorem 1.

3. Computation of the constant B_f

The sum $\sum_p \frac{(d/p)\log p}{p-1}$, appearing in the formula of the constant B_f converges very slowly. The next lemma gives an alternative expression for this sum, more convenient in order to obtain a fast computation.

Lemma 12.

$$\sum_p \frac{(d/p)\log p}{p-1} = \sum_{k=1}^{\infty} \frac{\zeta'(2^k)}{\zeta(2^k)} - \sum_{k=0}^{\infty} \frac{L'(2^k,\chi_d)}{L(2^k,\chi_d)} + \sum_{p|d} s_p. \tag{59}$$

where $s_p = \sum_{k=1}^{\infty} \frac{\log p}{p^{2^k}-1}$.

Proof. For $s>1$ we consider the function $G_d(s) = \prod_p \Big(1-\frac{1}{p^s}\Big)^{(d/p)}$. Taking the derivative of the logarithm of $G_d(s)$ we obtain that

$$\frac{G_d'(s)}{G_d(s)} = \sum_p \frac{(d/p)\log p}{p^s-1}. \tag{60}$$

Since $L(s,\chi_d) = \prod_p \Big(1 - \frac{(d/p)}{p}^s\Big)^{-1}$ we have

$$\begin{aligned} G_d(s)L(s,\chi_d) &= \prod_p \Big(1-\frac{1}{p^s}\Big)^{(d/p)}\Big(1-\frac{(d/p)}{p^s}\Big)^{-1} && (61)\\ &= \prod_{(d/p)=-1} \Big(1-\frac{1}{p^{2s}}\Big)^{-1} && (62)\\ &= \prod_p \Big(1-\frac{1}{p^{2s}}\Big)^{\frac{(d/p)-1}{2}} \prod_{p|d}\Big(1-\frac{1}{p^{2s}}\Big)^{1/2} && (63)\\ &= G_d^{1/2}(2s)\zeta^{1/2}(2s)T^{1/2}(2s) && (64) \end{aligned}$$

where $T(s) = \prod_{p|d}\Big(1-\frac{1}{p^s}\Big)$.

The derivative of the logarithm gives

$$\frac{G_d'(s)}{G_d(s)} - \frac{G_d'(2s)}{G_d(2s)} = \frac{\zeta'(2s)}{\zeta(2s)} + \frac{T_d'(2s)}{T_d(2s)} - \frac{L'(s,\chi_d)}{L(s,\chi_d)}.$$

Thus

$$\begin{aligned} \frac{G_d'(s)}{G_d(s)} - \frac{G_d'(2^m s)}{G_d(2^m s)} &= \sum_{k=0}^{m-1}\left(\frac{G_d'(2^k s)}{G_d(2^k s)} - \frac{G_d'(2^{k+1}s)}{G_d(2^{k+1}s)}\right) && (65)\\ &= \sum_{k=1}^{m} \frac{\zeta'(2^k s)}{\zeta(2^k s)} + \sum_{k=1}^{m}\frac{T_d'(2^k s)}{T_d(2^k s)} - \sum_{k=0}^{m-1}\frac{L'(2^k s,\chi_d)}{L(2^k s,\chi_d)}. && (66) \end{aligned}$$

By (60) we have that for $s \geqslant 2$,

$$\begin{aligned}|\frac{\zeta'(s)}{\zeta(s)}| &\leqslant \sum_{n\geqslant 2}\frac{\Lambda(n)}{n^s-1} \leqslant \frac{\log 2}{2^s-1}+\sum_{n\geqslant 3}\frac{\log n}{n^s-1}\\ &\leqslant \frac{4}{3}\frac{\log 2}{2^s}+\frac{9}{8}\sum_{n\geqslant 3}\frac{\log n}{n^s} \leqslant \frac{4}{3}\frac{\log 2}{2^s}+\frac{9}{8}\int_2^\infty \frac{\log x}{x^s}dx\\ &= \frac{4}{3}\frac{\log 2}{2^s}+\frac{9}{8}\Big(\frac{\log 2}{2^{s-1}(s-1)}+\frac{1}{2^{s-1}(s-1)^2}\Big)\\ &\leqslant \frac{1}{2^s(s-1)}\Big(\frac{20\log 2+8}{9}\Big) \leqslant \frac{5}{2}\cdot\frac{2^{-s}}{s-1}.\end{aligned}$$

Thus, $|\frac{\zeta'(2^k)}{\zeta(2^k)}| \leqslant \frac{5}{2}\cdot\frac{2^{-2^k}}{2^k-1}$. The same estimate holds for $|\frac{G_d'(2^k)}{G_d(2^k)}|$, $|\frac{T_d'(2^k)}{T_d(2^k)}|$ and $|\frac{L'(2^k,\chi_d)}{L(2^k,\chi_d)}|$. When $m \to \infty$ and then $s \to 1$ we get

$$\sum_p \frac{(d/p)\log p}{p-1} = \sum_{k=1}^\infty \frac{\zeta'(2^k)}{\zeta(2^k)} - \sum_{k=0}^\infty \frac{L'(2^k,\chi_d)}{L(2^k,\chi_d)} + \sum_{k=1}^\infty \frac{T_d'(2^k)}{T_d(2^k)}. \tag{67}$$

Finally we observe that $\frac{T_d'(2^k)}{T_d(2^k)} = \sum_{p|d}\frac{\log p}{p^{2^k}-1}$, so $\sum_{k=1}^\infty \frac{T_d'(2^k)}{T_d(2^k)} = \sum_{p|d} s_p$. □

The advantage of the lemma above is that the series involved converge very fast. For example,

$$\sum_{k=0}^\infty \frac{L'(2^k,\chi_d)}{L(2^k,\chi_d)} = \sum_{k=0}^6 \frac{L'(2^k,\chi_d)}{L(2^k,\chi_d)} + Error$$

with $|Error| \leqslant 10^{-40}$.

Hence we can write $B_f = C_0 + C_d + C(f)$ where C_0 is an universal constant, C_d depends only on d, and $C(f)$ depends on f. More precisely,

$$\begin{aligned}C_0 &= \gamma - 1 - 2\log 2 - \sum_{k=1}^\infty \frac{\zeta'(2^k)}{\zeta(2^k)} = -1.17254716741901485085875215283640\ldots\\ C_d &= \sum_{k=0}^\infty \frac{L'(2^k,\chi_d)}{L(2^k,\chi_d)} - \sum_{p|d} s_p\\ C(f) &= \frac{1}{\phi(q)}\sum_{\substack{1\leqslant r\leqslant q\\(r,q)=1}}\log\Big(1+\frac{r}{q}\Big) + \log a + \sum_{p|2aD}\log p\Big(\frac{1+(d/p)}{p-1} - \sum_{k\geqslant 1}\frac{s(f,p^k)}{p^k}\Big).\end{aligned}$$

The values of s_p and $\sum_{k\geqslant 0} L'(2^k,\chi_d)/L(2^k,\chi_d)$, can be calculated with MAGMA with high precision. We include some of the values of C_d and $C(f)$:

$$\begin{aligned}C_{-4} &= +\,0.346538435736895987549 - s_2 &&= +\,0.066550762366036180349\ldots\\ C_{-8} &= -\,0.076694093066485311184 - s_2 &&= -\,0.356681766437345118384\ldots\\ C_{-3} &= +\,0.586272400297149523649 - s_3 &&= +\,0.435045713698422447292\ldots\\ C_{-7} &= -\,0.070022837990444988815 - s_7 &&= -\,0.111373766208260107471\ldots\\ C_{-15} &= -\,0.486320692903261758405 - s_3 - s_5 &&= -\,0.707190640126000030028\ldots\end{aligned}$$

$$\begin{aligned}
C(x^2+1) &= (3\log 2)/2 &&= 1.03972077083991796412 5\dots\\
C(x^2+2) &= (3\log 2)/2 &&= 1.03972077083991796412 5\dots\\
C(x^2+x+1) &= \log 2+(\log 3)/6 &&= 0.87624922867129692464 9\dots\\
C(x^2+x+2) &= \log 2+(\log 7)/(42) &&= 0.73947837458507181668 1\dots\\
C(2x^2+1) &= 3\log 2 &&= 2.07944154167983592825 1\dots\\
C(2x^2+x+1) &= 2\log 2+\log 3+(\log 7)/(42) &&= 1.83809066325318150807 6\dots\\
C(2x^2+x+2) &= \log 2+(7\log 3)6+(\log 5)/(20) &&= 2.05533341296111163477 5\dots\\
C(2x^2+2x+1) &= 3\log 2 &&= 2.07944154167983592825 1\dots
\end{aligned}$$

Table below contains the constant $B = B_f$ for all irreducible quadratic polynomial $f(x) = ax^2+bx+c$ with $0 \leqslant a, b, c \leqslant 2$. When f_1, f_2 are irreducible quadratic polynomials such that $f_1(x) = f_2(x + k)$ for some k, we only include one of them since $L_n(f_1) = L_n(f_2) + O(\log n)$.

$f(x)$	d	q	B_f
x^2+1	-4	1	$-0.0662756342130607063 8\dots$
x^2+2	-8	1	$-0.4895081630164420051 1\dots$
x^2+x+1	-3	1	$+0.1387477749507045210 8\dots$
x^2+x+2	-7	1	$-0.5444425590422031416 4\dots$
$2x^2+1$	-8	1	$+0.5502126078234759590 0\dots$
$2x^2+x+1$	-7	2	$+0.5541697296259065497 4\dots$
$2x^2+x+2$	-15	2	$+0.1755956054160967538 8\dots$
$2x^2+2x+1$	-4	1	$+0.9734451366268572577 4\dots$

Table below shows the error term $E_f(n) = \log L_n(f) - n\log n - B_f n$ for the polynomials above and some values of n.

$f(x)$	$E_f(10^2)$	$E_f(10^3)$	$E_f(10^4)$	$E_f(10^5)$	$E_f(10^6)$	$E_f(10^7)$
x^2+1	-18	$+6$	-111	$+34$	-2634	-1557
x^2+2	-36	-11	-263	-761	-1462	-8457
x^2+x+1	-6	-9	$+17$	-654	-2528	-1685
x^2+x+2	$+9$	-20	-218	-2120	$+687$	-686
$2x^2+1$	-15	-1	-301	-251	$+1084$	-14821
$2x^2+x+1$	-1	$+6$	$+18$	-1289	$+235$	-2553
$2x^2+x+2$	-34	$+4$	-295	$+27$	$+1169$	$+1958$
$2x^2+2x+1$	-9	-89	$+9$	-232	-2876	-10624

4. Quadratic reducible polynomials

To complete the problem of estimating the least common multiple of quadratic polynomials we will study here the case of reducible quadratic polynomials. Being this case much easier than the irreducible case, we will give a complete description for the sake of the completeness.

If $f(x) = ax^2 + bx + c$ with $g = (a, b, c) > 1$, it is easy to check that $\log L_n(f) = \log L_n(f') + O(1)$ where $f'(x) = a'x^2 + b'x + c'$ with $a' = a/g,\ b' = b/g,\ c' = c/g$.

If $f(x) = (ax + b)^2$ with $(a, b) = 1$ then, since $(m^2, n^2) = (m, n)^2$, we have that $L_n((ax + b)^2) = L_n^2(ax + b)$ and we can apply (1) to get

$$\log \text{l.c.m.}\{(a+b)^2,\dots,(an+b)^2\} \sim 2n\frac{a}{\phi(a)}\sum_{\substack{1\leqslant k\leqslant a\\ (k,a)=1}}\frac{1}{k}. \tag{68}$$

Now we consider the more general case $f(x)=(ax+b)(cx+d),\ (a,b)=(c,d)=1$.

Theorem 3. *Let $f(x)=(ax+b)(cx+d)$ with $(a,b)=(c,d)=1$ and $ad\neq bd$. Let $q=ac/(a,c)$. We have*

$$\log l.c.m.(f(1),\dots,f(n))\sim\frac{n}{\varphi(q)}\sum_{1\leqslant r\leqslant q,\ (r,q)=1}\max\Big(\frac{a}{(br)_a},\frac{c}{(dr)_c}\Big). \tag{69}$$

Proof. Suppose $p^2\mid L_n(f)$. It implies that $p^2\mid(ai+b)(ci+d)$ for some i. If $p\mid ai+b$ and $p\mid ci+d$ then $p\mid(ad-bc)i$. If $p\nmid(ad-bc)$ then $p\mid i$ and consequently $p\mid b$ and $p\mid d$. Thus, if $p\nmid(ad-bc)bd$ and $p^2\mid(ai+b)(ci+d)$ then $p^2\mid(ai+b)$ or $p^2\mid(ci+d)$. In these cases $p\leqslant M_n=\max(\sqrt{an+b},\sqrt{cn+d},|(ad-bd)bd|)$.

Thus we write

$$L_n(f)=\prod_{p\leqslant M_n}p^{\beta_p(n)}\prod_{p>M_n}p^{\epsilon_p(n)}=\prod_{p\leqslant M_n}p^{\beta_p(n)-\epsilon_p(n)}\prod_{p}p^{\epsilon_p(n)}, \tag{70}$$

where $\epsilon_p(n)=1$ if $p\mid f(i)$ for some $i\leqslant n$ and $\epsilon_p(n)=0$ otherwise. Since $p^{\beta_p(n)}\leqslant f(n)$ we have that $\beta_p(n)\ll\log n/\log p$ and then

$$\sum_{p\leqslant M_n}(\beta_p(n)-\epsilon_p(n))\log p\ll(\log n)\pi(M_n)\ll\sqrt{n}. \tag{71}$$

Thus,

$$\log L_n(f)=\sum_{\substack{p\mid f(i)\\ \text{for some } i\leqslant n}}\log p+O(\sqrt{n}). \tag{72}$$

Let $q=ac/(a,c)$. Suppose that $p\equiv r^{-1}\pmod q,\ (r,q)=1$. Let $k=(br)_a$ the least positive integer such that $k\equiv br\pmod a$. Then $p\mid(ai+b)$ for some $i\leqslant n$ if and only if $kp\leqslant an+b$. Similarly, let $j=(dr)_c$ be the least positive integer such that $j\equiv dr\pmod c$. Again, $p\mid(ci+d)$ for some $\leqslant i\leqslant n$ if $jp\leqslant cn+d$. Thus, the primes $p\equiv r^{-1}\pmod{ac}$ counted in the sum above are those such that $p\leqslant\max(\frac{an+b}{k},\frac{cn+d}{j})$. The prime number theorem for arithmetic progressions implies that there are $\sim\frac{n}{\varphi(q)}\max(\frac{a}{k},\frac{c}{j})$ of such primes.

We finish the proof summing up in all $1\leqslant r\leqslant q,\ (r,q)=1$. □

References

Bat02 P. Bateman, *A limit involving Least Common Multiples*: 10797, American Mathematical Monthly **109** (2002), no. 4, 393-394.

Che52 P.L. Chebyshev, *Memoire sur les nombres premiers.* J. Math. pures et appl. **17** (1852), 366-390.

DFI95 W. Duke, J. Friedlander and H. Iwaniec, *Equidistribution of roots of a quadratic congruence to prime moduli*, Ann. of Math. **141** (1995), no. 2, 423–441.

HW08 G.H. Hardy and E.M. Wright, *An Introduction to the Theory of Numbers (Sixth edition)*, Oxford: Oxford University Press, (2008).

LS96 H. Lenstra and P. Stevenhagen, *Chebotarëv and his density theorem*, The Mathematical Inteligencer **18**(1996), no. 2, 26–37.

Tot00 A. Toth, *Root of quadratic congruences*, Internat. Math. Res. Notices **14** (2000), 719–739.

Javier Cilleruelo franciscojavier.cilleruelo@uam.es
Instituto de Ciencias Matemáticas (CSIC-UAM-UC3M-UCM) and Departamento de Matemáticas , Universidad Autónoma de Madrid , 28049 Madrid, Spain