

ON THE ERROR TERM OF THE LOGARITHM OF THE LCM OF A QUADRATIC SEQUENCE

JUANJO RUÉ, PAULIUS ŠARKA, AND ANA ZUMALACÁRREGUI

ABSTRACT. We study the logarithm of the least common multiple of the sequence of integers given by $1^2 + 1, 2^2 + 1, \dots, n^2 + 1$. Using a result of Homma [4] on the distribution of roots of quadratic polynomials modulo primes we calculate the error term for the asymptotics obtained by Cilleruelo [2].

1. INTRODUCTION

The first important attempt to prove the Prime Number Theorem was made by Chebyshev. In 1853 [2] he introduced the function $\psi(n) = \sum_{p^m \leq n} \log p$ and proved that the Prime Number Theorem was equivalent to the asymptotic estimate $\psi(n) \sim n$. He also proved that if $\psi(n)/n$ had a limit as n tends to infinity then that limit is 1. The proof of this result was only completed (independently) two years after Chebyshev's death by Hadamard and de la Vallée Poussin.

Observe that Chebyshev's function is precisely $\psi(n) = \log \text{lcm}(1, 2, \dots, n)$, so it seems natural to consider the following question: for a given polynomial $f(x) \in \mathbb{Z}[x]$, what can be said about the $\log \text{lcm}(f(1), f(2), \dots, f(n))$? As Hadamard and de la Vallée Poussin proved, for $f(x) = x$ this quantity asymptotically behaves as n . Some progress has been made in the direction of generalising this result to a broader class of polynomials. In [1] the authors use the Prime Number Theorem for arithmetic progressions to get the asymptotic estimate for any linear polynomial $f(x) = ax + b$:

$$\log \text{lcm}(f(1), f(2), \dots, f(n)) \sim n \frac{q}{\varphi(q)} \sum_{\substack{k=1 \\ (k,q)=1}}^q \frac{1}{k},$$

where $q = a/\text{gcd}(a, b)$. Recently, Cilleruelo [2] extended this result to the quadratic case, obtaining that for an irreducible polynomial $f(x) = ax^2 + bx + c \in \mathbb{Z}[x]$ the following asymptotic estimate holds:

$$(1) \quad \log \text{lcm}(f(1), f(2), \dots, f(n)) = n \log n + B_f n + o(n),$$

where the constant B_f is explicit. The author also proves that for reducible polynomials of degree two, the asymptotic is linear in n . For polynomials of higher degree nothing is known, except for products of linear polynomials, which are studied in [5].

An important ingredient in Cilleruelo's argument is a result of Toth [9], a generalisation of a deep theorem of Duke, Friedlander and Iwaniec [3] about the distribution of solutions of quadratic congruences $f(x) \equiv 0 \pmod{p}$, when p runs over all primes. Recent improvements of the latter result in the negative discriminant case [4] allowed us prove Theorem 1.1, sharpening the error term in a special case of expression (1).

We focus our study on the particular polynomial $f(x) = x^2 + 1$, which simplifies the calculation, and shows how the method developed in [2] works in a clear manner. The same ideas could be extended to general irreducible quadratic polynomials of negative discriminant, however, a generalisation of [4] (in the same direction as Toth's) would be necessary.

For this particular polynomial the expression for B is given by

$$(2) \quad \gamma - 1 - \frac{\log 2}{2} - \sum_{p \neq 2} \frac{\left(\frac{-1}{p}\right) \log p}{p-1} \approx -0.0662756342,$$

where γ is the Euler constant, $\left(\frac{-1}{p}\right)$ is the Legendre symbol and the sum is taken over all odd prime numbers (B can be computed with high numerical precision by using its expression in terms of L-series and zeta-series, see [2] for details). More precisely, we obtain the following estimate:

Theorem 1.1. *For any $\theta < 4/9$ we have*

$$\log \operatorname{lcm}(1^2 + 1, 2^2 + 1, \dots, n^2 + 1) = n \log n + Bn + O\left(\frac{n}{(\log n)^\theta}\right),$$

where the constant B is given by Expression (2).

The infinite sum in (2) appears in other mathematical contexts: as it is pointed in [7] this sum is closely related to multiplicative sets whose elements are non-hypotenuse numbers (i.e. integers which could not be written as the hypotenuse of a right triangle with integer sides).

Plan of the paper: in Section 2 we recall the basic necessary results and fix the notation used in the rest of the paper. We explain the strategy for the proof of Theorem 1.1 in Section 3, which is based on a detailed study of medium primes (Section 4). Then, using these partial results, in Section 5 we provide the complete proof of Theorem 1.1.

2. BACKGROUND AND NOTATION

Throughout the paper p will denote a prime number and the Landau symbols O and o , as well as the Vinogradov symbols \ll, \gg will be employed with their usual meaning. We will also use the following notation:

$$\begin{aligned}\pi(n) &= |\{p : p \leq n\}|, \\ \pi_1(n) &= |\{p : p \equiv 1 \pmod{4}, p \leq n\}|, \\ \pi_1([a, b]) &= |\{p : p \equiv 1 \pmod{4}, a < p \leq b\}|.\end{aligned}$$

The Prime Number Theorem states that the following estimate holds:

$$(3) \quad \psi(n) = \log \operatorname{lcm}(1, 2, \dots, n) = n + E(n), \quad E(n) = O\left(\frac{n}{(\log n)^\kappa}\right),$$

where κ can be chosen as large as necessary. We also use the following estimate, which follows from the Prime Number Theorem for arithmetic progressions:

$$(4) \quad \pi_1(n) = \frac{n}{2 \log n} + O\left(\frac{n}{(\log n)^2}\right).$$

The result needed in order to refine the error term of (1) is the main theorem in [4], which deals with the distribution of fractional parts ν/p , where p is a prime less than or equal to n and ν is a root in $\mathbb{Z}/p\mathbb{Z}$ of a quadratic polynomial $f(x)$ with negative discriminant. For this f , we define the discrepancy $D_f(n)$ associated to the set of fractions $\{\nu/p : f(\nu) \equiv 0 \pmod{p}, p \leq n\}$ as

$$D_f(n) = \sup_{[u, v] \in [0, 1]} \left| [u, v] - \frac{1}{\pi(n)} \sum_{p \leq n} \sum_{\substack{u < \nu/p \leq v \\ f(\nu) \equiv 0 \pmod{p}}} 1 \right|,$$

where $[u, v] := v - u$. Under these assumptions, the main theorem of Homma [4] can be stated as follows:

Theorem 2.1. *Let f be any irreducible quadratic polynomial with integer coefficients and negative discriminant. Then for any $\delta < 8/9$ we have*

$$D_f(n) = O\left(\frac{1}{(\log n)^\delta}\right).$$

As a consequence of this result, we have the following lemma:

Lemma 2.1. *Let $g : [0, 1] \rightarrow \mathbb{R}$ be any function of bounded variation, and $n < N$ two positive real numbers. Then for any $\delta < 8/9$*

$$\sum_{\substack{n < p < N \\ 0 \leq \nu < p \\ \nu^2 \equiv -1 \pmod{p}}} g\left(\frac{\nu}{p}\right) = 2\pi_1([n, N]) \int_0^1 g(t) dt + O\left(\frac{N}{(\log N)^{1+\delta}}\right).$$

Proof. We know by the Koksma–Hlawka identity (see Theorem 2.11 in [8]) that for any sequence $A = \{a_1, a_2, \dots, a_n\}$, $A \subset [0, 1]$, with discrepancy $D(n)$ and for any $g : [0, 1] \rightarrow \mathbb{R}$ with bounded variation, we have

$$\frac{1}{n} \sum_{i=1}^n g(a_i) = \int_0^1 g(t) dt + O(D(n)),$$

so

$$\sum_{i=n}^N g(a_i) = \sum_{i=1}^N g(a_i) - \sum_{i=1}^n g(a_i) = (N - n) \int_0^1 g(t) dt + O(ND(N)) + O(nD(n)).$$

In our case, using Theorem 2.1, we get

$$\sum_{\substack{n < p < N \\ 0 \leq \nu < p \\ \nu^2 \equiv -1 \pmod{p}}} g\left(\frac{\nu}{p}\right) = 2\pi_1([n, N]) \int_0^1 g(t) dt + O\left(\frac{\pi_1(N)}{(\log N)^\delta}\right).$$

Using the rough estimate $\pi_1(N) = O\left(\frac{N}{\log N}\right)$ we get the required error term. \square

3. THE STRATEGY

The content of this section can be found in [2]. We include it here for completeness and to prepare the reader for the forthcoming arguments.

Denote by $P_n = \prod_{i=1}^n (i^2 + 1)$ and $L_n = \text{lcm}(1^2 + 1, 2^2 + 1, \dots, n^2 + 1)$, and write $\alpha_p(n) = \text{ord}_p(P_n)$ and $\beta_p(n) = \text{ord}_p(L_n)$. The argument for estimating L_n stems from the following equality:

$$\log L_n = \log P_n + \sum_p (\beta_p(n) - \alpha_p(n)) \log p.$$

Clearly it is not difficult to estimate $\log P_n$. Indeed, using Stirling's approximation formula, we get

$$\log \prod_{i=1}^n (i^2 + 1) = \log \prod_{i=1}^n i^2 + \log \prod_{i=1}^n \left(1 + \frac{1}{i^2}\right) = 2 \log n! + O(1) = 2n \log n - 2n + O(\log n),$$

and so in the remainder of the paper we will be concerned with the estimation of $\sum_p (\beta_p(n) - \alpha_p(n)) \log p$. We start here by making three simple observations:

Lemma 3.1.

- i) $\beta_2(n) - \alpha_2(n) = -n/2 + O(1)$,
- ii) $\beta_p(n) - \alpha_p(n) = 0$, when $p > 2n$.
- iii) $\beta_p(n) - \alpha_p(n) = 0$, when $p \equiv 3 \pmod{4}$.

Proof.

- i) $i^2 + 1$ is never divisible by 4 and is divisible by 2 for every odd i .
- ii) Note that $\alpha_p(n) \neq \beta_p(n)$ only if there exist $i < j \leq n$ such that $p|i^2 + 1$ and $p|j^2 + 1$. But this implies $p|(i - j)(i + j)$, and so $p \leq 2n$.
- iii) $i^2 + 1$ is never divisible by $p \equiv 3 \pmod{4}$ as -1 is not a quadratic residue modulo such prime. \square

Since we have dealt with the prime 2, from now on we will only consider odd primes. Lemma 3.1 also states that it is sufficient to study the order of prime numbers which are smaller than $2n$ and are equivalent to 1 modulo 4. We split these primes in two groups: ones that are smaller than $n^{2/3}$ and others that are between $n^{2/3}$ and $2n$, *small* and *medium* primes respectively.

The computation for small primes is easy and is carried out in the lemma below, after obtaining simple estimates for $\alpha_p(n)$ and $\beta_p(n)$. Analysis of medium primes, which is left for the next section, is more subtle and will lead to improvement of the error term.

Lemma 3.2. *For primes $p \equiv 1 \pmod{4}$ the following estimates hold:*

- i) $\beta_p(n) \ll \frac{\log n}{\log p}$,
- ii) $\alpha_p(n) = \frac{2n}{p-1} + O\left(\frac{\log n}{\log p}\right)$.

Proof.

- i) It is clear that $\beta_p(n)$ satisfies $p^{\beta_p(n)} \leq n^2 + 1$, so

$$\beta_p(n) \leq \frac{\log(n^2 + 1)}{\log p} \ll \frac{\log n}{\log p}.$$

- ii) In order to estimate $\alpha_p(n)$ note that for primes $p \equiv 1 \pmod{4}$ the equation $i^2 \equiv -1 \pmod{p^a}$ has two solutions ν_1 and ν_2 in the interval $[1, p^a]$ and every other solution is of the form $\nu_1 + kp^a$ or $\nu_2 + kp^a$, $k \in \mathbb{Z}$. The number of times p^a divides $i^2 + 1$, $i = 1, \dots, n$ is given by

$$(5) \quad 2 + \left\lfloor \frac{n - \nu_1}{p^a} \right\rfloor + \left\lfloor \frac{n - \nu_2}{p^a} \right\rfloor,$$

which equals to 0 for $p^a > n^2 + 1$ and $2n/p^a + O(1)$ for $p^a \leq n^2 + 1$. Therefore we get

$$\begin{aligned} \alpha_p(n) &= 2 \sum_{j=1}^{\left\lfloor \frac{\log(n^2+1)}{\log p} \right\rfloor} \frac{n}{p^j} + O\left(\frac{\log n}{\log p}\right) \\ &= 2n \sum_{j=1}^{\infty} \frac{1}{p^j} - 2n \sum_{j=\left\lfloor \frac{\log(n^2+1)}{\log p} \right\rfloor+1}^{\infty} \frac{1}{p^j} + O\left(\frac{\log n}{\log p}\right) \\ &= \frac{2n}{p-1} + O\left(\frac{\log n}{\log p}\right), \end{aligned}$$

and the claim follows. \square

Lemma 3.3. *The following estimate holds:*

$$\sum_{2 < p < n^{2/3}} (\alpha_p(n) - \beta_p(n)) \log p = \sum_{2 < p < n^{2/3}} \frac{\left(1 + \left(\frac{-1}{p}\right)\right) n \log p}{p-1} + O(n^{2/3}).$$

Proof. Using the estimates from Lemma 3.2 we get

$$\sum_{2 < p < n^{2/3}} \beta_p(n) \log p \ll \sum_{2 < p < n^{2/3}} \log n \ll n^{2/3},$$

and also

$$\begin{aligned} \sum_{2 < p < n^{2/3}} \alpha_p(n) \log p &= \sum_{\substack{p < n^{2/3} \\ p \equiv 1 \pmod{4}}} \left(\frac{2n \log p}{p-1} + O(\log n) \right) \\ &= \sum_{2 < p < n^{2/3}} \frac{\left(1 + \left(\frac{-1}{p}\right)\right) n \log p}{p-1} + O(n^{2/3}), \end{aligned}$$

and hence the claim follows. \square

4. MEDIUM PRIMES

In order to deal with the remaining primes, we note, that if a prime $p \equiv 1 \pmod{4}$ satisfies $n^{2/3} \leq p \leq 2n$ then it divides $i^2 + 1$ for some $i \leq n$. However, since such a prime is sufficiently large compared to $n^2 + 1$, the case that p^2 divides some $i^2 + 1$, $i \leq n$ is unlikely.

Having this in mind, we separate contribution of higher degrees from the contribution of degree 1. Define for $p \equiv 1 \pmod{4}$:

$$\begin{aligned}\alpha_p^*(n) &= |\{i : p|i^2 + 1, i \leq n\}|, \\ \beta_p^*(n) &= 1,\end{aligned}$$

and, for $p \equiv 3 \pmod{4}$, $\alpha_p^*(n) = \beta_p^*(n) = 0$. Then

$$(6) \quad \sum_{n^{2/3} \leq p \leq 2n} (\beta_p(n) - \alpha_p(n)) \log p = \sum_{n^{2/3} \leq p \leq 2n} (\beta_p(n) - \beta_p^*(n) - \alpha_p(n) + \alpha_p^*(n)) \log p + \sum_{n^{2/3} \leq p \leq 2n} \beta_p^*(n) \log p - \sum_{n^{2/3} \leq p \leq 2n} \alpha_p^*(n) \log p.$$

We now estimate each sum in the previous equation. We start estimating the first one:

Lemma 4.1. *The following estimate holds:*

$$\sum_{n^{2/3} \leq p \leq 2n} (\beta_p(n) - \beta_p^*(n) - \alpha_p(n) + \alpha_p^*(n)) \log p \ll n^{2/3} \log n.$$

To prove this lemma we need some preliminary results. As it was intended, $(\beta_p(n) - \beta_p^*(n) - \alpha_p(n) + \alpha_p^*(n)) \log p$ is nonzero only when $p^2|i^2 + 1$ for some $i \leq n$. We claim, that number of such primes is small:

Lemma 4.2. *The following estimate holds:*

$$|\{p : p^2|i^2 + 1, n^{2/3} \leq p \leq 2n, i \leq n\}| \ll n^{2/3}.$$

Proof. Let us split the interval $[n^{2/3}, 2n]$ into dyadic intervals, consider one of them, say $[Q, 2Q]$, and define

$$P_k = \{p : i^2 + 1 = kp^2 \text{ for some } i \leq n\}.$$

We estimate the size of the set $P_k \cap [Q, 2Q]$, which is nonempty only when $k \leq (n^2 + 1)/Q^2$. For every $p \in P_k \cap [Q, 2Q]$ we have $i^2 - kp^2 = (i + \sqrt{kp})(i - \sqrt{kp}) = -1$, thus

$$\left| \frac{i}{p} - \sqrt{k} \right| = \frac{1}{p^2} \left(\frac{i}{p} + \sqrt{k} \right)^{-1} \leq \frac{1}{p^2} \leq \frac{1}{Q^2}.$$

On the other hand, all fractions i/p , $p \in P_k$, are pairwise different, since $ip' = i'p$ implies $p = p'$ (otherwise $p|i$, and so $p|i^2 - kp^2 = -1$, a contradiction), therefore

$$\left| \frac{i}{p} - \frac{i'}{p'} \right| \geq \frac{1}{pp'} \gg \frac{1}{Q^2}.$$

Combining both inequalities we get $|P_k \cap [Q, 2Q]| \ll 1$ for every $k \leq (n^2 + 1)/Q^2$. Recalling that $P_k \cap [Q, 2Q]$ is empty for other values of k we have

$$|\{p : p^2|i^2 + 1, Q \leq p \leq 2Q, i \leq n\}| = |\cup_k (P_k \cap [Q, 2Q])| \ll \frac{n^2}{Q^2}.$$

Summing over all dyadic intervals the result follows. \square

Now we use this estimate to prove Lemma 4.1.

Proof of Lemma 4.1. We use estimates from Lemma 3.2 and the estimate for $\alpha_p^*(n)$, which follows from Expression (5):

$$\begin{aligned}\beta_p(n) &\ll \frac{\log n}{\log p}, \\ \alpha_p(n) &= \frac{2n}{p-1} + O\left(\frac{\log n}{\log p}\right), \\ \alpha_p^*(n) &= \frac{2n}{p} + O(1).\end{aligned}$$

For any prime $n^{2/3} < p < 2n$, such that $p^2 | i^2 + 1$ for some $i \leq n$, we get

$$|\beta_p(n) - \beta_p^*(n) - \alpha_p(n) + \alpha_p^*(n)| = \frac{2n}{p(p-1)} + O\left(\frac{\log n}{\log p}\right) \ll \frac{\log n}{\log p}.$$

It follows from Lemma 4.2 that the number of such primes is $\ll n^{2/3}$, thus

$$\sum_{n^{2/3} \leq p \leq 2n} (\beta_p(n) - \beta_p^*(n) - \alpha_p(n) + \alpha_p^*(n)) \log p \ll n^{2/3} \log n.$$

□

We continue estimating the second sum in Equation (6):

Lemma 4.3. *The following estimate holds:*

$$\sum_{n^{2/3} \leq p \leq 2n} \beta_p^*(n) \log p = n + O\left(\frac{n}{\log n}\right).$$

Proof. Summing by parts and using estimate (4) for $\pi_1(x)$ we get:

$$\begin{aligned}\sum_{n^{2/3} \leq p \leq 2n} \beta_p^*(n) \log p &= \sum_{\substack{n^{2/3} \leq p \leq 2n \\ p \equiv 1 \pmod{4}}} \log p \\ &= \sum_{\substack{p \leq 2n \\ p \equiv 1 \pmod{4}}} \log p + O(n^{2/3}) \\ &= \log(2n) \pi_1(2n) - \int_2^{2n} \frac{\pi_1(t)}{t} dt + O(n^{2/3}) \\ &= n + O\left(\frac{n}{\log n}\right).\end{aligned}$$

□

Finally, we deal with the contribution of the coefficients α_p^* . In this point we need to take care of the error term in a more detailed way:

Lemma 4.4. *For any $\delta < 8/9$ the following estimate holds:*

$$\sum_{n^{2/3} \leq p \leq 2n} \alpha_p^*(n) \log p = n \sum_{n^{2/3} \leq p \leq 2n} \frac{\left(1 + \left(\frac{-1}{p}\right)\right) \log p}{p-1} + O\left(\frac{n}{(\log n)^{\delta/2}}\right).$$

Proof. Using (5) and noting that $\nu_1 + \nu_2 = p$, where $1 \leq \nu_1, \nu_2 \leq p$ are solutions of $i^2 \equiv -1 \pmod{p}$, we get

$$\begin{aligned}\alpha_p^*(n) &= 2 + \left\lfloor \frac{n - \nu_1}{p} \right\rfloor + \left\lfloor \frac{n - \nu_2}{p} \right\rfloor \\ &= 2 + \frac{2n}{p} - \frac{\nu_1 + \nu_2}{p} - \left\{ \frac{n - \nu_1}{p} \right\} - \left\{ \frac{n - \nu_2}{p} \right\} \\ &= \frac{2n}{p} + \frac{1}{2} - \left\{ \frac{n - \nu_1}{p} \right\} + \frac{1}{2} - \left\{ \frac{n - \nu_2}{p} \right\},\end{aligned}$$

so the sum over all primes in the interval $[n^{2/3}, 2n]$ is equal to

$$\sum_{n^{2/3} \leq p \leq 2n} \alpha_p^*(n) \log p = n \sum_{n^{2/3} \leq p \leq 2n} \frac{\left(1 + \left(\frac{-1}{p}\right)\right) \log p}{p} + \sum_{\substack{n^{2/3} \leq p \leq 2n \\ \nu^2 \equiv -1 \pmod{p} \\ 0 \leq \nu < p}} \log p \left(\frac{1}{2} - \left\{ \frac{n - \nu}{p} \right\} \right).$$

We rewrite

$$n \sum_{n^{2/3} \leq p \leq 2n} \frac{\left(1 + \left(\frac{-1}{p}\right)\right) \log p}{p} = n \sum_{n^{2/3} \leq p \leq 2n} \frac{\left(1 + \left(\frac{-1}{p}\right)\right) \log p}{p - 1} + O(n^{1/3} \log n)$$

and

$$\sum_{n^{2/3} \leq p \leq 2n} \sum_{\substack{\nu^2 \equiv -1 \pmod{p} \\ 0 \leq \nu < p}} \log p \left(\frac{1}{2} - \left\{ \frac{n - \nu}{p} \right\} \right) = \log n \sum_{p \leq 2n} \sum_{\substack{0 < \nu < p \\ \nu^2 \equiv -1 \pmod{p}}} \left(\frac{1}{2} - \left\{ \frac{n - \nu}{p} \right\} \right) + O\left(\frac{n}{\log n}\right).$$

Notice that for any sequence a_p satisfying $a_p \ll 1$ we have by a summing by parts argument that

$$\sum_{p < x} a_p \log p = \log x \sum_{p < x} a_p - \int_1^x \frac{1}{t} \sum_{p < t} a_p dt = \log x \sum_{p < x} a_p + O\left(\frac{x}{\log x}\right).$$

In order to get the claimed bound, it remains to show that

$$\sum_{p \leq 2n} \sum_{\substack{0 < \nu < p \\ \nu^2 \equiv -1 \pmod{p}}} \left(\frac{1}{2} - \left\{ \frac{n - \nu}{p} \right\} \right) = O\left(\frac{n}{(\log n)^{1+\delta/2}}\right).$$

To do that, we divide the summation interval into $1 + H$ parts $[1, 2n] = [1, A] \cup L_1 \cup \dots \cup L_H$, where

$$L_i = \left(\frac{2nAH}{2n(H-i+1) + A(i-1)}, \frac{2nAH}{2n(H-i) + Ai} \right].$$

We choose $A = \lfloor n/(\log n)^{\delta/2} \rfloor$ and $H = \lfloor (\log n)^\delta \rfloor$ in order to minimize the error term, but we continue using these notations for the sake of conciseness.

Observe that in every of these parts, except the first one, n/p is almost constant, which enables to use the fact that ν/p is well distributed. More precisely, if $p \in L_i$ then

$$\frac{n}{p} \in [\lambda_i, \lambda_{i-1}] := \left[\frac{2n(H-i) + Ai}{2AH}, \frac{2n(H-i+1) + A(i-1)}{2AH} \right),$$

and the length of such interval is small: $|\lambda_i, \lambda_{i-1}| = \frac{2n-A}{2AH}$. We would then like to replace $\frac{n}{p}$ by λ_i whenever $\frac{n}{p} \in [\lambda_i, \lambda_{i-1}]$ using

$$(7) \quad \left\{ \frac{n - \nu}{p} \right\} = \left\{ \lambda_i - \frac{\nu}{p} \right\} + \left\{ \frac{n}{p} - \lambda_i \right\},$$

but this equality does not hold if $\lambda_i < \frac{\nu}{p} + k < \frac{n}{p}$ for some integer k , in particular $\frac{\nu}{p} + k \in [\lambda_i, \lambda_{i-1}]$. Therefore we must differentiate this two cases: if $\lambda_i \leq \frac{\nu}{p} + k \leq \lambda_{i-1}$ for some k we rewrite it as $\frac{\nu}{p} \in [\lambda_i, \lambda_{i-1}]_1$ and $\frac{\nu}{p} \notin [\lambda_i, \lambda_{i-1}]_1$ otherwise.

We now split the previous sum into three parts:

$$\sum_{p \leq 2n} \sum_{\substack{0 < \nu < p \\ \nu^2 \equiv -1 \pmod{p}}} \left(\frac{1}{2} - \left\{ \frac{n - \nu}{p} \right\} \right) = \Sigma_1 + \Sigma_2 + \Sigma_3 + O(\pi_1(A)),$$

where Σ_1 , Σ_2 and Σ_3 are defined as

$$\begin{aligned} \Sigma_1 &= \sum_{i=1}^H \sum_{p \in L_i} \sum_{\substack{0 \leq \nu < p \\ \nu^2 \equiv -1 \pmod{p}}} \left(\frac{1}{2} - \left\{ \lambda_i - \frac{\nu}{p} \right\} \right), \\ \Sigma_2 &= \sum_{i=1}^H \sum_{p \in L_i} \sum_{\substack{0 \leq \nu < p \\ \nu^2 \equiv -1 \pmod{p} \\ \frac{\nu}{p} \notin [\lambda_i, \lambda_{i-1}]_1}} \left(\left\{ \lambda_i - \frac{\nu}{p} \right\} - \left\{ \frac{n - \nu}{p} - \frac{\nu}{p} \right\} \right), \\ \Sigma_3 &= \sum_{i=1}^H \sum_{p \in L_i} \sum_{\substack{0 \leq \nu < p \\ \nu^2 \equiv -1 \pmod{p} \\ \frac{\nu}{p} \in [\lambda_i, \lambda_{i-1}]_1}} \left(\left\{ \lambda_i - \frac{\nu}{p} \right\} - \left\{ \frac{n - \nu}{p} - \frac{\nu}{p} \right\} \right). \end{aligned}$$

Recall that $A = n/(\log n)^{\delta/2} + O(1)$ and $H = (\log n)^\delta + O(1)$, so $\pi_1(A) = O(n/(\log n)^{1+\delta/2})$. We now estimate each of the sums $\Sigma_1, \Sigma_2, \Sigma_3$ separately, making use of Lemma 2.1. For the first one note that

$$\int_0^1 \left(\frac{1}{2} - \{ \lambda_i - t \} \right) dt = 0,$$

so we get, using Lemma 2.1,

$$\begin{aligned} \Sigma_1 &= \sum_{i=1}^H \sum_{p \in L_i} \sum_{\substack{0 \leq \nu < p \\ \nu^2 \equiv -1 \pmod{p}}} \left(\frac{1}{2} - \left\{ \lambda_i - \frac{\nu}{p} \right\} \right) \\ (8) \quad &= \sum_{i=1}^H O \left(\frac{2nAH}{2n(H-i) + Ai} \middle/ \left(\log \frac{2nAH}{2n(H-i) + Ai} \right)^{1+\delta} \right) \\ &= O \left(\frac{2nAH}{(\log n)^{1+\delta}} \int_0^H \frac{di}{2n(H-i) + Ai} \right) \\ &= O \left(\frac{2nAH}{(\log n)^{1+\delta}} \frac{\log 2n/A}{2n - A} \right) = O \left(\frac{n \log \log n}{(\log n)^{1+\delta/2}} \right). \end{aligned}$$

For the second sum we use Equation (7):

$$\begin{aligned} \Sigma_2 &= \sum_{i=1}^H \sum_{p \in L_i} \sum_{\substack{0 \leq \nu < p \\ \nu^2 \equiv -1 \pmod{p} \\ \frac{\nu}{p} \notin [\lambda_i, \lambda_{i-1}]_1}} \left\{ \frac{n}{p} - \lambda_i \right\} \\ (9) \quad &\leq \sum_{i=1}^H \sum_{p \in L_i} \sum_{\substack{0 \leq \nu < p \\ \nu^2 \equiv -1 \pmod{p}}} |[\lambda_i, \lambda_{i-1}]| \\ &\leq \frac{2n - A}{2AH} 2\pi_1(2n) = O \left(\frac{n}{(\log n)^{1+\delta/2}} \right). \end{aligned}$$

Finally, for the third sum we use the notation $\mathbb{I}_{[\lambda_i, \lambda_{i-1}]_1}$ for the indicator function of the interval $[\lambda_i, \lambda_{i-1}]$ modulo 1, which satisfies

$$\int_0^1 \mathbb{I}_{[\lambda_i, \lambda_{i-1}]_1}(t) dt = |[\lambda_i, \lambda_{i-1}]|,$$

so using Lemma 2.1 we get

$$\begin{aligned} \Sigma_3 &\ll \sum_{i=1}^H \sum_{\substack{0 \leq \nu < p \in L_i \\ \nu^2 \equiv -1 \pmod{p} \\ \frac{\nu}{p} \in [\lambda_i, \lambda_{i-1}]_1}} 1 = \sum_{i=1}^H \sum_{\substack{0 \leq \nu < p \in L_i \\ \nu^2 \equiv -1 \pmod{p}}} \mathbb{I}_{[\lambda_i, \lambda_{i-1}]_1} \left(\frac{\nu}{p} \right) \\ &= \sum_{i=1}^H 2\pi_i(L_i) |\lambda_i, \lambda_{i-1}| + O \left(\frac{2nAH}{2n(H-i) + Ai} / \left(\log \frac{2nAH}{2n(H-i) + Ai} \right)^{1+\delta} \right) \\ &= O \left(\frac{n \log \log n}{(\log n)^{1+\delta/2}} \right), \end{aligned}$$

estimating similarly as in the derivation of (8) and (9).

Finally, we note that any function f satisfying $f(n) = O \left(\frac{n \log \log n}{(\log n)^{1+\delta/2}} \right)$ for every $\delta < 8/9$ also satisfies $f(n) = O \left(\frac{n}{(\log n)^{1+\delta/2}} \right)$ for every $\delta < 8/9$, hence this concludes the proof. \square

5. PROOF OF THEOREM 1.1

Combining Lemmas 3.3, 4.1, 4.3 and 4.4, and taking $\theta = \delta/2$, we get that

$$(10) \quad \log L_n = 2n \log n - n \left(1 + \frac{\log 2}{2} + \sum_{2 < p \leq 2n} \frac{(1 + (\frac{-1}{p})) \log p}{p-1} \right) + O \left(\frac{n}{(\log n)^\theta} \right),$$

for any constant $\theta < 4/9$. Note that,

$$\sum_{2 < p \leq 2n} \frac{(1 + (\frac{-1}{p})) \log p}{p-1} = \sum_{2 < p \leq 2n} \frac{\log p}{p-1} + \sum_{2 < p \leq 2n} \frac{(\frac{-1}{p}) \log p}{p-1}.$$

For the first sum, observe that Merten's Theorem implies

$$(11) \quad \sum_{2 < p \leq 2n} \frac{\log p}{p-1} = \sum_{p^j \leq 2n} \frac{\log p}{p^j} - \log 2 + \sum_{\substack{p^j > 2n \\ 2 < p \leq 2n}} \frac{\log p}{p^j} = \log n - \gamma + o(1),$$

and the error term can be bounded by $O(1/\log n)$ using Prime Number Theorem in the form (3) and summation by parts. Note that this bound can be sharpened to $O(\exp(-c\sqrt{\log n}))$ for certain constant c , see [6] (Exercise 4, page 182).

For the second sum, we recall that the complete oscillating sum is convergent, and it follows from Prime Number Theorem in arithmetic progressions that

$$\sum_{2 < p \leq 2n} \frac{(\frac{-1}{p}) \log p}{p-1} = \sum_{p \neq 2} \frac{(\frac{-1}{p}) \log p}{p-1} + O \left(\frac{1}{\log n} \right).$$

Thus we have that, for every $\theta < 4/9$,

$$\log L_n = n \log n - n \left(1 - \gamma + \frac{\log 2}{2} + \sum_{p \neq 2} \frac{(\frac{-1}{p}) \log p}{p-1} \right) + O \left(\frac{n}{(\log n)^\theta} \right),$$

which completes the proof.

Acknowledgments: This work was done during second author's visit at Universidad Autónoma de Madrid in the winter of 2011. He would like to thank the people of Mathematics Department and especially Javier Cilleruelo for their warm hospitality. The authors are also grateful for his advice and helpful suggestions in the preparation of this paper.

Pieter Moree is greatly thanked for noticing the connection between the constant (2) and the non-hypotenuse numbers, for pointing out reference [6] in relation with expression (11) and also for useful comments.

The first author is supported by a JAE-DOC grant from the JAE program in CSIC, Spain. The last author is supported by a FPU grant from Ministerio de Educación, Ciencia y Deporte, Spain. Both authors were jointly financed by the MTM2011-22851 grant (Spain) and the ICMAT Severo Ochoa Project SEV-2011-0087 (Spain).

REFERENCES

- [1] P. Bateman, J. Kalb, and A. Stenger. A limit involving least common multiples. *American Mathematical Monthly*, 109:393–394, 2002.
- [2] J. Cilleruelo. The least common multiple of a quadratic sequence. *Compositio Mathematica*, 147(4):1129–1150, 2011.
- [3] W. Duke, J. Friedlander, and H. Iwaniec. Equidistribution of roots of a quadratic congruence to prime moduli. *Annals of Mathematics*, 141(2):423–441, 1995.
- [4] K. Homma. On the discrepancy of uniformly distributed roots of quadratic congruences. *Journal of Number Theory*, 128(3):500–508, 2008.
- [5] S. Hong, G. Quian, and Q. Tan. The least common multiple of sequence of product of linear polynomials. *Acta Mathematica Hungarica (to appear)*.
- [6] H. L. Montgomery and R. C. Vaughan. *Multiplicative number theory. I. Classical theory*, volume 97 of *Cambridge Studies in Advanced Mathematics*. Cambridge University Press, Cambridge, 2007.
- [7] P. Moree. Counting numbers in multiplicative sets: Landau versus Ramanujan. *preprint, available on-line at arXiv:1110.0708v1*, 2011.
- [8] H. Niederreiter. *Random number generation and quasi-Monte Carlo methods*, volume 63 of *CBMS-NSF Regional Conference Series in Applied Mathematics*. Society for Industrial and Applied Mathematics (SIAM), 1992.
- [9] Á. Tóth. Roots of quadratic congruences. *Internat. Math. Res. Notices*, (14):719–739, 2000.

J. RUÉ: INSTITUTO DE CIENCIAS MATEMÁTICAS (CSIC-UAM-UC3M-UCM), 28049 MADRID, SPAIN
E-mail address: `juanjo.rue@icmat.es`

P. ŠARKA: INSTITUTE OF MATHEMATICS AND INFORMATICS, AKADEMIJOS 4, VILNIUS LT-08663, LITHUANIA AND DEPARTMENT OF MATHEMATICS AND INFORMATICS, VILNIUS UNIVERSITY, NAUGARDUKO 24, VILNIUS LT-03225, LITHUANIA
E-mail address: `paulius.sarka@gmail.com`

A. ZUMALACÁRREGUI: INSTITUTO DE CIENCIAS MATEMÁTICAS (CSIC-UAM-UC3M-UCM) AND DEPARTAMENTO DE MATEMÁTICAS, UNIVERSIDAD AUTÓNOMA DE MADRID, 28049 MADRID, SPAIN
E-mail address: `ana.zumalacarregui@uam.es`