Can. J. Math. Vol. **48** (1), 1996 pp. 81–104

ON THE DISTRIBUTION OF SUPERSINGULAR PRIMES

ETIENNE FOUVRY AND M. RAM MURTY

ABSTRACT. Let E be a fixed elliptic curve defined over the rational numbers. We prove that the number of primes $p \leq x$ such that E has supersingular reduction $\bmod p$ is greater than

$$\frac{\log_3 x}{(\log_4 x)^{1+\delta}}$$

for any positive δ and x sufficiently large. Here $\log_k x$ is defined recursively as $\log(\log_{k-1} x)$ and $\log_1 x = \log x$. We also establish several results related to the Lang-Trotter conjecture.

1. **Introduction.** Let E be a fixed elliptic curve over $\mathbb{Q}$. Let j_E be its j-invariant. A supersingular prime for E is a rational prime p such that E has good reduction at p and $\mathrm{End}_{\bar{\mathbb{F}}_p}(E)$ is a maximal order in a quaternion algebra. Let $\pi_0(x)$ be the number of such primes $p \leq x$. If E has complex multiplication, Deuring [De] showed that

$$\pi_0(x) \sim \frac{1}{2}\frac{x}{\log x}$$

as $x \longrightarrow \infty$. If E does not have complex multiplication, then the asymptotic behaviour of $\pi_0(x)$ is at present unknown. Lang and Trotter [L-T] conjecture the existence of a constant $C_E > 0$ such that

$$\pi_0(x) \sim \frac{C_E\sqrt{x}}{\log x}$$

as $x \longrightarrow \infty$. The constant C_E is defined in terms of representations of the Galois group $\mathrm{Gal}\big(\mathbb{Q}(E_{\mathrm{tor}})/\mathbb{Q}\big)$, where $\mathbb{Q}(E_{\mathrm{tor}})$ is the field obtained by adjoining to $\mathbb{Q}$ all the torsion points of E. This constant seems to be rather complicated to compute in a general situation.

Elkies [El1] made the first breakthrough in this direction . By an ingenious argument, he proved

$$\pi_0(x) \longrightarrow \infty$$

as $x \longrightarrow \infty$. Elkies and Murty (see [El2] p. 21) obtained the lower bound

$$\pi_0(x) > \log_2 x$$

for all sufficiently large x, assuming the Riemann Hypothesis for the classical Dirichlet L-functions $L(s,\chi)$. We denote by $\log_k$ the k-fold iterated logarithm function. (Brown [Br1]

Received by the editors May 10, 1994.

AMS subject classification: Primary: 11G05; secondary: 11N36.

https://doi.org/10.4153/CJM-1996-004-7 Published online by Cambridge University Press

obtained the weaker estimate $\pi_0(x) > \log_3 x$ assuming the same unproved hypothesis). They also noted that $\pi_0(x) = O(x^{\frac{3}{4}})$ follows unconditionally using a result of Kaneko [Ka] (see [El3] and also [Mu] for a slightly different approach to the lower bound).

Our goal is to prove unconditionally

THEOREM 1. *For any elliptic curve E and for any positive δ, there exists $x_0(E,\delta)$ such that the inequality*

$$\pi_0(x) \geq \frac{\log_3 x}{(\log_4 x)^{1+\delta}}$$

holds for $x > x_0(E,\delta)$.

THEOREM 2. *For any elliptic curve E, we have the equality*

$$\pi_0(x) = \Omega(\log_2 x)$$

Recall that we write $f(x) = \Omega\big(g(x)\big)$ if there is a constant $c > 0$, such that the inequality $|f(x)| > cg(x)$ holds for infinitely many $x \longrightarrow \infty$.

Both of these theorems will follow from the stronger theorem

THEOREM 3. *For any elliptic curve E and any $\varepsilon > 0$, at least one of the two following statements is true*

(i) $\pi_0(x) = \Omega\big((\log x)^{2-\varepsilon}\big)$

(ii) $\pi_0(x) > \log_2 x$ *for* $x > x_0(E)$.

Instead of considering one fixed curve, one can work with a family of curves and study the behaviour of $\pi_0(x)$ for this family. We thus obtain the average Lang-Trotter Conjecture: let $E_{a,b}$ be the elliptic curve

$$y^2 = x^3 + ax + b$$

with $a, b \in \mathbb{Z}$. Denote by $\pi_0(x,a,b)$ the number of supersingular primes of $E_{a,b}$ less than x.

We will prove the following result

THEOREM 4. *Let $A \geq 1$, $B \geq 1$. Then for every $C > 0$, we have the equality*

$$\sum_{|a|\leq A}\sum_{|b|\leq B} \pi_0(x,a,b) = \frac{2\pi}{3}\cdot AB\int_2^x \frac{dt}{\sqrt{t}\log t} + O\Big((A+B)x^{\frac{3}{2}} + x^{\frac{5}{2}} + AB\sqrt{x}(\log x)^{-C}\Big).$$

It is easy to see that under the conditions

$$A > x^{1+\varepsilon}; \quad B > x^{1+\varepsilon} \tag{1.1}$$

we have

$$\sum_{|a|\leq A}\sum_{|b|\leq B} \pi_0(x,a,b) \sim_\varepsilon \frac{4\pi}{3}\cdot AB\cdot\frac{\sqrt{x}}{\log x} \tag{1.2}$$

https://doi.org/10.4153/CJM-1996-004-7 Published online by Cambridge University Press

Such a result allows to say that the Lang-Trotter Conjecture is true *on average*. Nevertheless, we must check that in the sum considered in Theorem 4, the dominant term does not come from the curves $E_{a,b}$ with complex multiplication, which, by Deuring's Theorem, have many more supersingular primes. It is well known that E has complex multiplication if and only if j_E belongs to a set of thirteen values. So, there are thirteen families of CM-curves $E_{a,b}$, two of them are the families $E_{0,b}$ and $E_{a,0}$ with a and $b \in \mathbb{Z}^*$. The other eleven families are parameterized by $E_{\alpha_i t^2, \beta_i t^3}$, with $t \in \mathbb{Z}^*$ and (α_i, β_i) is in an explicit set of eleven pairs of integers. With these remarks, we deduce that

$$\sum_{|a| \leq A} \sum_{\substack{|b| \leq B \\ E_{a,b} \text{ is CM}}} \pi_0(x, a, b) = O\Big(\frac{x}{\log x} \cdot \max(A, B)\Big)$$

which is negligible compared with the main term.

Let

$$\mathcal{M} = \{(a,b) \in \mathbb{Z}^2; p^2 \mid a \Rightarrow p^3 \nmid b\}.$$

The set $\mathcal{M}$ (set of minimality) has been introduced to ensure that two different elliptic curves with parameters belonging to $\mathcal{M}$, are never isomorphic over $\mathbb{Q}$. We will shortly give the proof of the following theorem, which can be improved in several directions:

THEOREM 5. *Let $\varepsilon > 0$, x, A, B be real numbers satisfying*

$$A, B > x^{1+\varepsilon}; \quad AB > x^{2+\varepsilon} \min(A^{\frac{1}{4}}, B^{\frac{1}{6}}).$$

Then, for $x \longrightarrow \infty$, we have

$$\sum_{|a| \leq A} \sum_{\substack{|b| \leq B \\ (a,b) \in \mathcal{M}}} \pi_0(x, a, b) \sim_\varepsilon \frac{4\pi}{3\zeta(10)} \cdot AB \cdot \frac{\sqrt{x}}{\log x}$$

A natural question is to weaken the condition (1.1) so that the relation (1.2) continues to be true (the shorter the averaging is, the closer we are to the Lang-Trotter Conjecture itself). Using a particular case of the classical Weil's bound, for exponential sums (see Lemma 8 below), we will notably improve the condition (1.1), by proving

THEOREM 6. *Let $\varepsilon > 0$, x, A, B be real numbers satisfying*

$$A, B > x^{\frac{1}{2}+\varepsilon}; \quad AB > x^{\frac{3}{2}+\varepsilon}.$$

Then, for $x \longrightarrow \infty$, we have

$$\sum_{|a| \leq A} \sum_{|b| \leq B} \pi_0(x, a, b) \sim_\varepsilon \frac{4\pi}{3} \cdot AB \cdot \frac{\sqrt{x}}{\log x}.$$

In paragraph 8, we develop other types of averagings, which rather depend on algebraic number theory, and in the last paragraph, we discuss the size of least supersingular prime of an elliptic curve.

This work was done when the first author was visiting the Centre de Recherches Mathématiques de Montréal. He thanks the C. R. M. for its hospitality and financial support. The second author thanks the University of Orsay for support during which this work was completed.

2. **Lemmas.** We first recall how to detect supersingular primes (see [El1] pp. 561–562). For brevity, we restrict ourselves to odd primes.

Let $D \equiv 0$ or $3 \pmod 4$ and denote by O_D the order

$$O_D = \mathbb{Z}\left[\frac{1}{2}(D+\sqrt{-D})\right]$$

of discriminant $-D$. Given an elliptic curve E over $\mathbb{Q}$, let p be an odd prime of good reduction for E and E_p the reduction of $E \pmod p$. The criterion of Deuring [De] states that p is supersingular if and only if E_p has complex multiplication by some O_D such that p is ramified or inert in $\mathbb{Q}(\sqrt{-D})$. It is well-known that, given D, there exist only finitely many isomorphism classes of elliptic curves over $\bar{\mathbb{Q}}$ with complex multiplication by O_D. Moreover, the j-invariants of these isomorphism classes are conjugate algebraic integers. Let $P_D(X)$ be the modular polynomial associated to O_D. It is a monic and irreducible polynomial of $\mathbb{Z}[X]$, the roots of which are the above j-invariants and it makes sense to consider $P_D(X) \pmod p$.

By Deuring's lifting lemma [De, p. 259], complex multiplication in characteristic p can be lifted to characteristic zero and so the roots of $P_D(X)$ in characteristic p are j-invariants of curves with an endomorphism $\frac{1}{2}(D+\sqrt{-D})$.

That is, E_p has complex multiplication by some $O_{D'}$ for some $D'|D$ with D/D' a perfect square if and only if $P_D(X) \pmod p$ has j_E as a root. If, moreover, $-D$ is a quadratic non-residue mod$p$ or the highest power of p dividing D is odd, then p is a supersingular prime for E. We summarize this in:

LEMMA 1 (DEURING). *Let p an odd prime of good reduction for E. Then p is a supersingular prime for E if and only if there exists some $D \equiv 0$ or $3 \pmod 4$ such that D divides the numerator of $P_D(j_E)$ and $(\frac{-D}{p}) = -1$ or the highest power of p dividing D is odd.*

We continue by recalling the following lemma from Elkies ([El1], Proposition):

LEMMA 2. *Let l be a prime $\equiv 3 \bmod 4$. There are polynomials $R(X)$, $S(X) \in \mathbb{Z}[X]$, such that, modulo l, $P_l(X)$ and $P_{4l}(X)$ factor into $(X-12^3)R(X)^2$ and $(X-12^3)S(X)^2$.*

REMARK. Another proof of Lemma 2 appears in Kaneko [Ka].

It is easily seen that for l prime $\equiv 3 \pmod 4$, $j\left(\frac{1}{2}(1+\sqrt{-l})\right)$ and $j(\sqrt{-l})$ are the only real roots of P_l and P_{4l} respectively, the other falling into complex conjugate pairs. From the Fourier expansion of j, we see

$$j(z) = e^{-2\pi iz} + O(1)$$

as $\mathrm{Im}(z) \longrightarrow \infty$, and hence as $l \longrightarrow \infty$, the real root of P_l (P_{4l} resp.) goes to $-\infty$ (goes to $+\infty$ respectively). Thus, for l sufficiently large, we have $P_l(j_E)P_{4l}(j_E) < 0$. See [Mu] for explicit estimates.

https://doi.org/10.4153/CJM-1996-004-7 Published online by Cambridge University Press

LEMMA 3. *Let $p_1, p_2, \ldots, p_k$ a given set of primes. The number of primes $l \equiv 7 \pmod 8$ such that $(\frac{p_i}{l}) = 1$ for $1 \le i \le k$ and $l \le x$ is*

$$\gg \frac{1}{\log x} \cdot \frac{x}{(p_1 p_2 \cdots p_k)^3}$$

provided $x \ge (p_1 p_2 \cdots p_k)^B$, for some absolute constant $B > 0$.

PROOF. This essentially follows from the proof of a classical theorem of Linnik (see [Bo] p. 56): let $(a, m) = 1$ and denote by $\pi(x; m, a)$ the number of primes $p \le x$ with $p \equiv a \pmod m$. For $x \ge m^{10}$, we have

$$\pi(x; m, a) \gg \frac{1}{\log x} \cdot \frac{x}{m^3}.$$

In our context, the l's we seek lie essentially in some arithmetic progression mod $8p_1 \cdots p_k$, and so the result follows from Linnik's Theorem. Note also that any improvement of the exponents B or 3 in the statement of Lemma 3 has almost no influence on Theorems 1, 2 and 3.

LEMMA 4. *Let l_1 and l_2 be two distinct primes $\equiv 3 \pmod 4$. If p divides the numerator of both $P_{l_1}(j_E)P_{4l_1}(j_E)$ and $P_{l_2}(j_E)P_{4l_2}(j_E)$, then $p \le 4l_1 l_2$.*

A lemma of that type was firstly proved by Gross and Zagier [G-Z], then generalized by Dorman [Do]. Our lemma is an easy consequence of Theorem 2 of Kaneko [Ka]. This theorem has the advantage of giving a result for the prime divisors of the resultant of the polynomials $P_{D_1}(X)$ and $P_{D_2}(X)$, when D_1 and D_2 are distinct discriminants, not necessarily fundamental.

LEMMA 5. *Let h denote the class number of $\mathbb{Q}(\sqrt{-l})$. Then, there exists an absolute constant c_0, such that the inequality*

$$|P_l(j_E)P_{4l}(j_E)| \le 2^{4h} \exp(c_0 C \sqrt{l} \log^2 l)$$

is true with $C = \log(|j_E| + 745)$.

PROOF. From [Mu] Lemma 5, we have the inequality

$$|P_l(j_E)| \le 2^{2h} \exp\Big(C\sqrt{l} \sum \frac{1}{a_i}\Big)$$

where the sum is over the classical set of representatives of h classes of quadratic forms of discriminant $-l$, which means quadratic forms

$$a_i x^2 + b_i xy + c_i y^2$$

satisfying $b_i^2 - 4a_i c_i = -l$, $(a_i, b_i, c_i) = 1$, $-a_i < b_i \le a_i < c_i$ or $0 \le b_i \le a_i = c_i$. Since the congruence $x^2 + l \equiv 0 \pmod{a_i}$, has at most $2^{\omega(a_i)}$ solutions (ω:number of prime divisors), we get the following inequality

$$\sum_{1 \le i \le h} \frac{1}{a_i} \le 2 \sum_{1 \le a \le \sqrt{l}} \frac{2^{\omega(a)}}{a} \le \prod_{p \le \sqrt{l}} \Big(1 + \frac{2}{p-1}\Big) \ll (\log l)^2.$$

https://doi.org/10.4153/CJM-1996-004-7 Published online by Cambridge University Press

To bound $|P_{4l}(j_E)|$, we start from [Mu] Lemma 6 (where the factor 2^h has to be replaced by 2^{3h}) and follow the same technique as above. Hence Lemma 5 follows. Therefore this lemma implies that the numerator of $P_l(j_E)P_{4l}(j_E)$ satisfies

$$\mathrm{Num}\big(P_l(j_E)P_{4l}(j_E)\big) \ll \exp\big(C'(E)\sqrt{l}(\log l)^2\big)$$

with $C'(E)$ depending only on E (an easy consequence of the inequalities $\deg\big(P_l(X)P_{4l}(X)\big) = O(h)$ and $h = O(\sqrt{l}\log l)$).

The following lemma (see Jutila [Ju] Lemma 8) gives an upper bound on average for a sum of characters at prime arguments. We have

LEMMA 6. *Let*

$$S(D,X) = \sum_{|d|\le D}\Big|\sum_{3\le n\le X}\Lambda(n)\Big(\frac{d}{n}\Big)\Big|$$

where d is a non square integer. Then with $D_0 = \exp\big(c_0(\log X)^{\frac{1}{2}}\big)$, we have, for $3\le D\le D_0$, the inequality

$$S(D,X) \ll X\Big(\exp(-c_1D^{-\varepsilon}\log X) + \exp\big(-c_2(\log X)^{\frac{1}{2}}\big)\Big)$$

where $c_1 = c_1(\varepsilon)$ and c_2 are positive constants. Also,

$$S(D,X) \ll XD^{\varepsilon}$$

for $D_0 < D < X^{\frac{1}{4}}$, and

$$S(D,X) \ll (XD)^{\frac{4}{5}+\varepsilon}$$

for $X^{\frac{1}{4}} \le D \le X^{\frac{49}{50}}$.

In particular, for every $C > 0$, uniformly for $3\le D\le X^{\frac{49}{50}}$, we have

$$S(D,X) \ll XD(\log X)^{-C}.$$

The above estimations of $S(D,X)$ remain valid if the variable of summation n satisfies $n\equiv 3 \pmod 4$ (resp. $n\equiv 1 \pmod 4$).

To prove the last part of this lemma, we can, for instance, detect the odd primes $n\equiv 3 \pmod 4$ by the function $\frac{1}{2}\big(1-(\frac{-1}{n})\big)$, and then apply the first part of the lemma.

LEMMA 7. *Let p be a prime, α and β two integers. Define*

$$\begin{aligned}&M(A,B,\alpha,\beta,p)\\ &\quad= \big|\{(a,b); a\equiv\alpha \pmod p, b\equiv\beta \pmod p, (a,b)\in\mathcal{M}, |a|\le A, |b|\le B\}\big|.\end{aligned}$$

Then, for every positive ε, we have the equality

$$\begin{aligned}M(A,B,\alpha,\beta,p) &= \frac{4AB}{p^2\cdot\zeta(10)}\cdot\big(1+O(p^{-1})\big)\cdot\Big(1+O\big((\log AB)^{-4}\big)\Big)\\ &\quad+O\Big(\frac{A+B}{p}+(AB)^{\varepsilon}+\min(A^{\frac{1}{4}},B^{\frac{1}{6}})\Big).\end{aligned}$$

Note that this lemma is interesting only when A and B are large enough compared with p, for instance

$$A, B > p^{1+\varepsilon}; \quad \frac{AB}{p^{2+\varepsilon}} > \min(A^{\frac{1}{4}}, B^{\frac{1}{6}}).$$

PROOF. We start from the formula

$$M(A,B,\alpha,\beta,p) = \sum_d \mu(d)\Big|\{(a,b); ab \neq 0, a \equiv \alpha \pmod p, b \equiv \beta \pmod p,$$
$$d^4|a, d^6|b, |a| \leq A, |b| \leq B\}\Big|$$
$$+ O\Big(\frac{A+B}{p} + 1\Big).$$

Note that in the above formula, we may suppose that d satisfies

$$d \leq \min(A^{\frac{1}{4}}, B^{\frac{1}{6}})$$

When d has all its prime factor less than $\sqrt{\log AB}$, we use the formula

$$\Big|\{(a,b); a \equiv \alpha \pmod p, b \equiv \beta \pmod p, d^4|a, d^6|b, |a| \leq A, |b| \leq B\}\Big|$$
$$(2.1) \qquad = \Big(\frac{2A}{\varphi(\alpha,p,d^4)} + O(1)\Big) \cdot \Big(\frac{2B}{\varphi(\beta,p,d^6)} + O(1)\Big)$$

where $\varphi(\alpha,p,d^4)$ is equal to pd^4 if $p \not| d$, d^4 if $p|d$ and $\alpha = 0 \pmod p$ and $\varphi(\beta,p,d^6)$ defined similarly. When d has a prime factor greater than $\sqrt{\log AB}$(so d is greater than this bound) we use, for the cardinality studied in (2.1), the trivial bound

$$\leq \Big(\frac{2A}{[p,d^4]} + 1\Big)\Big(\frac{2B}{[p,d^6]} + 1\Big),$$

where $[m,n]$ is the least common multiple of m and n.

In the case $p \not| \alpha\beta$, by a classical computation, we have

$$M(A,B,\alpha,\beta,p) = \frac{4AB}{p^2} \prod_{\substack{q \text{ prime} \neq p \\ q < \sqrt{\log AB}}} \Big(1 - \frac{1}{q^{10}}\Big)$$
$$+ O\Big((AB)^\varepsilon + \Big(\frac{A+B}{p}\Big) + \frac{AB}{p^2}(\log AB)^{-\frac{9}{2}} + \min(A^{\frac{1}{4}}, B^{\frac{1}{6}})\Big)$$

which gives Lemma 7 in that case. In the other cases $(p|\alpha\beta)$, the computation leads, in the above formula, to a slightly different product over q which is nevertheless also of the form $\zeta(10)^{-1} \cdot \big(1 + O(p^{-1})\big) \cdot \Big(1 + O\big((\log AB)^{-4}\big)\Big)$. This completes the proof of the lemma.

The following lemma is a particular case of [Sc] Corollary 2F:

LEMMA 8. *Let u and v be integers such that at least one of them is not divisible by the prime p. Then, we have the inequality*

$$\Big|\sum_{n=0}^{p-1} e\Big(\frac{un^4 + vn^6}{p}\Big)\Big| \leq 5\sqrt{p}$$

https://doi.org/10.4153/CJM-1996-004-7 Published online by Cambridge University Press

3. **Proof of Theorem 3.** Let $p_1, \dots, p_k$ be the first k supersingular primes for E. By Lemma 3, we can find

$$\gg_E \frac{1}{\log x} \cdot \frac{x}{(p_1 \cdots p_k)^3}$$

primes $l \equiv 7 \pmod 8$ such that $l \leq x$, $(\frac{p_i}{l}) = 1$ for $1 \leq i \leq k$, and $(\frac{q_i}{l}) = 1$ for $1 \leq i \leq t$(where the q_i's are the primes where E has bad reduction) provided $x \geq (p_1 \cdots p_k)^B$ and B a sufficiently large constant, depending only on E. Note that these congruence conditions are compatible when 2 is one of the p_i's or q_i's. For such l, we have by Lemma 2 and by the fact that 2 divides $\deg\big(P_l(X)P_{4l}(X)\big)$, the equality

$$\left(\frac{\mathrm{Num}\big(P_l(j_E)P_{4l}(j_E)\big)}{l}\right) = 1.$$

On the other hand, by the remark following Lemma 2, $\mathrm{Num}\big(P_l(j_E)P_{4l}(j_E)\big)$ is a negative rational integer $= -N_l$ (say). Then, we have

$$\left(\frac{N_l}{l}\right) = -1.$$

By the choice of l in the lemma, not all the primes dividing N_l can be among $2, p_1, \dots, p_k$, $q_1, \dots, q_t$. Hence, by Lemma 1, there is a prime $p_{k+1}(l)$ which is a new (odd) supersingular prime for E.

Thus, to each l, we can associate a supersingular prime $p_{k+1}(l)$. If all these are distinct, then we have

$$\pi_0(T) \gg_E \frac{1}{\log x} \frac{x}{(p_1 \cdots p_k)^3}$$

where

$$T = \max_{l \leq x} N_l.$$

By the remark following Lemma 5, we have

$$T \ll \exp\big(C'(E)\sqrt{x}(\log x)^2\big)$$

Choosing $x = (p_1 \cdots p_k)^A$, for a sufficiently large A depending on E, we find the lower bound

$$\pi_0(y) \gg (\log y)^{2-\varepsilon} \tag{3.1}$$

for $y = \exp\Big(A(p_1 \cdots p_k)^{\frac{A}{2}}\big(\log(p_1 \cdots p_k)\big)^2\Big)$.

If for infinitely many k, the $p_{k+1}(l)$, constructed as above, are all distinct, then (3.1) is established for infinitely many $y \longrightarrow \infty$, hence the first part of Theorem 3.

Suppose now that it is not the case. Then, for all k sufficiently large, there are l_1 and l_2, such that $\mathrm{Num}\big(P_{l_1}(j_E)P_{4l_1}(j_E)\big)$ and $\mathrm{Num}\big(P_{l_2}(j_E)P_{4l_2}(j_E)\big)$ have, at least, a common prime factor called p_{k+1}. By Lemma 4, this new supersingular prime satisfies

$$p_{k+1} \leq 4 l_1 l_2$$

https://doi.org/10.4153/CJM-1996-004-7 Published online by Cambridge University Press

and by Lemma 3, we find

$$p_{k+1} \leq 4(p_1 \cdots p_k)^{2A}.$$

This recursive inequality yields

$$\pi_0(x) \gg \log_2 x$$

for all sufficiently large x. This completes the proof of Theorem 3. Theorem 2 is an immediate corollary.

4. **Proof of Theorem 1.** Actually, the proof of Theorem 3 investigates two opposite situations: in the first case a construction of a lot of new supersingular primes, but apparently very far from the old ones, and in the second case, the construction of only one supersingular prime but rather close to the old ones. In some sense, Theorem 1 covers both these cases.

Let $\delta > 0$, then Theorem 2 implies that there exists an arbitrarily large real number x_0, such that

$$\pi_0(x_0) \geq \frac{\log_2 x_0}{(\log_3 x_0)^{1+\delta}}$$

so, maybe by forgetting some supersingular primes less than x_0, we assert that there exist $p_1, \ldots, p_k$, supersingular primes less than x_0, with

$$\frac{\log_2 x_0}{(\log_3 x_0)^{1+\delta}} \leq k < \frac{\log_2 x_0}{(\log_3 x_0)^{1+\delta}} + 1.$$

We follow now the proof of Theorem 3, and define $x_1 = y$ in the first case, or $x_1 = 4(p_1 \cdots p_k)^{2A}$ in the second one. In both cases, it is easy to see, using the inequality

$$\log(p_1 \cdots p_k) < \left(\frac{\log_2 x_0}{(\log_3 x_0)^{1+\delta}} + 1\right) \log x_0$$

that x_1 satisfies the inequality

$$\log x_1 < (\log x_0)(\log_2 x_0).$$

In the first case, we have trivially

$$\pi_0(x_1) \geq \frac{\log_2 x_1}{(\log_3 x_1)^{1+\delta}} \tag{4.1}$$

and, in the second one, by construction of p_{k+1}, we know that

$$\pi_0(x_1) \geq \pi_0(x_0) + 1 \geq \frac{\log_2 x_0}{(\log_3 x_0)^{1+\delta}} + 1,$$

but, in that case, since

$$x_1 \leq \exp\left(3A \cdot \log x_0 \cdot \left(\frac{\log_2 x_0}{(\log_3 x_0)^{1+\delta}} + 1\right)\right),$$

https://doi.org/10.4153/CJM-1996-004-7 Published online by Cambridge University Press

we have

$$\frac{\log_2 x_1}{(\log_3 x_1)^{1+\delta}} \le \frac{\log_2 x_0}{(\log_3 x_0)^{1+\delta}} + O\big((\log_3 x_0)^{-\delta}\big) \le \frac{\log_2 x_0}{(\log_3 x_0)^{1+\delta}} + 1 \le \pi_0(x_1).$$

So, in both cases, (4.1) is valid. By replacing x_0 by x_1 and so on, we construct an infinite sequence $(x_n)_{n\ge 0}$ tending to infinity, such that:

$$\pi_0(x_n) \ge \frac{\log_2 x_n}{(\log_3 x_n)^{1+\delta}}, \tag{4.2}$$

and

$$\log_2 x_n \le (\log x_{n-1})(\log_2 x_{n-1}). \tag{4.3}$$

Now, if x is any large real number, it satisfies, for some n, the inequality

$$x_n \le x < x_{n+1}$$

from which we deduce, by (4.2),

$$\pi_0(x) \ge \pi_0(x_n) \ge \frac{\log_2 x_n}{(\log_3 x_n)^{1+\delta}}.$$

we have also, by (4.3),

$$\frac{\log_3 x}{(\log_4 x)^{1+2\delta}} \le \frac{\log_3 x_{n+1}}{(\log_4 x_{n+1})^{1+2\delta}} \le \frac{\log_2 x_n}{(\log_3 x_n)^{1+2\delta}}\big(1+o(1)\big) \le \frac{\log_2 x_n}{(\log_3 x_n)^{1+\delta}} \le \pi_0(x).$$

Hence the end of the proof of Theorem 1 with δ replaced by 2δ.

5. **Lang-Trotter conjecture on average.** It is well known that the total number of equivalence classes of elliptic curves over $\mathbb{F}_p$ with $p+1$ points is equal to the total number of classes of ideals of O_{4p}. The latter quantity is the Kronecker class number $H(-4p)$ (see, for instance[Bi], pp. 58–59). Now an elliptic curve over $\mathbb{F}_p$ can be written as (for $p \ne 2,3$), $E_{a,b}$ with $a, b \in \mathbb{F}_p$. The curves isomorphic to $E_{a,b}$ are the curves E_{au^4,bu^6}, with $u \in \mathbb{F}_p^*$. So, the number of curves isomorphic to the elliptic curve (over $\mathbb{F}_p$) $E_{a,b}$ is

$\frac{p-1}{6}$ for $a = 0, b \not\equiv 0 \pmod p$ and $p \equiv 1 \pmod 6$
$\frac{p-1}{4}$ for $b = 0, a \not\equiv 0 \pmod p$ and $p \equiv 1 \pmod 4$
$\frac{p-1}{2}$ in the remaining cases.

Since there are $O(1)$ isomorphism classes over $\mathbb{F}_p$ containing a curve of the form $E_{0,b}$ or $E_{a,0}$, we deduce that the number of elliptic curves $E_{a,b}$ with $0 \le a, b < p$ having $p+1$ points over $\mathbb{F}_p$ is equal to

$$\frac{p}{2}\cdot H(-4p) + O(p)$$

https://doi.org/10.4153/CJM-1996-004-7 Published online by Cambridge University Press

It remains to study the curves $E_{a,b}$ with $|a| \leq A$ and $|b| \leq B$, to write, under the assumptions of Theorem 4,

(5.1)
$$\sum_{|a|\leq A}\sum_{|b|\leq B} \pi_0(x;a,b) = \frac{1}{2}\sum_{p\leq x}\Big(\frac{2A}{p}+O(1)\Big)\cdot\Big(\frac{2B}{p}+O(1)\Big)\cdot p \cdot \Big(H(-4p)+O(1)\Big)+O(AB)$$
$$= 2AB\sum_{p\leq x}\frac{H(-4p)}{p}+O\Big((A+B)\frac{x^{\frac{3}{2}}}{\log x}+AB\log\log x+\frac{x^{\frac{5}{2}}}{\log x}\Big)$$

where the error $O(AB)$ comes from the primes 2 and 3 which are supersingular for some $E_{a,b}$ and from the p which are supersingular for curves with non-minimal equation $E_{a'p^4,b'p^6}$.

The equality
$$H(-4p) = h(-4p) + h(-p)$$

and the Dirichlet class number formula
$$h(-d) = \frac{w\sqrt{d}}{2\pi}L(1,\chi_{-d})$$

for $d \equiv 0$ or $3 \pmod 4$, $w = 6, 4$, or 2 when $d = 3, 4$ or $d \geq 7$, and χ_{-d} the Kronecker symbol $(\frac{-d}{\cdot})$ transform the study of (5.1) into a sum of Dirichlet series at the point $s = 1$. The right hand-side of (5.1) becomes

$$(5.2)\quad \frac{2AB}{\pi}\Big(\sum_{\substack{p\leq x\\ p\equiv 3 \pmod 4}}\frac{L(1,\chi_{-p})}{\sqrt{p}}+2\sum_{p\leq x}\frac{L(1,\chi_{-4p})}{\sqrt{p}}\Big)+O\Big((A+B)x^{\frac{3}{2}}+AB\log x+x^{\frac{5}{2}}\Big).$$

By partial summation and Polya-Vinogradov inequality, we have, for any parameter $U > 1$, the equality

$$(5.3)\qquad L(1,\chi_{-p}) = \sum_{n\leq U}\frac{\chi_{-p}(n)}{n}+O\Big(\frac{\sqrt{p}\log p}{U}\Big)$$

and the same equality for $-4p$.

We choose
$$U = x^{\frac{3}{4}}.$$

To obtain cancelations on the summation over p, we introduce the Legendre symbol, so we recall the formula

If $p \equiv 3 \pmod 4$ then $\chi_{-p}(n) = (\frac{n}{p})$ and if $p \geq 3$ then

$$(5.4)\qquad \chi_{-4p}(n) = \Big(\frac{2}{n}\Big)^2(-1)^{\frac{p-1}{2}\cdot\frac{n-1}{2}}\Big(\frac{n}{p}\Big)$$

the right hand side of this formula being understood to be 0 when n is even.

https://doi.org/10.4153/CJM-1996-004-7 Published online by Cambridge University Press

We will mainly concentrate on the sum

$$S^{(1)}(U,X)=\sum_{n\leq U}\frac{1}{n}\sum_{\substack{p\leq x\\ p\equiv 3\ (\mathrm{mod}\ 4)}}\frac{(\frac{n}{p})}{\sqrt{p}}.$$

If n is a perfect square, the inner sum is equal to

$$\frac{1}{2}\int_2^x\frac{dt}{\sqrt{t}\log t}+O\big(\sqrt{x}\exp(-\sqrt{\log x})\big)$$

by the prime number theorem and partial summation. This gives rise to the following main term for $S^{(1)}(U,X)$:

$$\frac{\pi^2}{12}\cdot\int_2^x\frac{dt}{\sqrt{t}\log t}+O\Big(\sqrt{x}\big(U^{-\frac{1}{2}}+\exp(-\sqrt{\log x})\big)\Big) \tag{5.5}$$

We now estimate the sum when n is not a perfect square. If $x_1=x\exp(-c\sqrt{\log x})$, for an appropriate constant c, we begin by noting, that we trivially have

$$\sum_{n\leq U}{}'\frac{1}{n}\sum_{p\leq x_1}{}^{*}\frac{(\frac{n}{p})}{\sqrt{p}}\ll\sqrt{x}(\log U)\exp\Big(-\frac{c}{2}\sqrt{\log x}\Big) \tag{5.6}$$

where the prime on the summation indicates (henceforth) that n is not a square and the star that $p\equiv 3\pmod 4$.

It therefore remains to estimate

$$\sum_{n\leq U}{}'\frac{1}{n}\sum_{x_1<p\leq x}{}^{*}\frac{(\frac{n}{p})}{\sqrt{p}}.$$

Using dyadic decomposition, (that is, decomposing the sum into intervals of the form $(V,2V)$), we see that the above sum is

$$\ll(\log x)|S^{(1)}(V)| \tag{5.7}$$

for some V satisfying $3\leq V\leq U$ and

$$S^{(1)}(V)=\sum_{V\leq n<2V}{}'\frac{1}{n}\sum_{x_1<p\leq x}{}^{*}\frac{(\frac{n}{p})}{\sqrt{p}}.$$

By partial integration, we get

$$VS^{(1)}(V)\ll\frac{1}{\sqrt{x}\log x}\cdot\sum_{V\leq n<2V}{}'\Big|\sum_{x_1<p\leq x}{}^{*}\log p\Big(\frac{n}{p}\Big)\Big|+\int_{x_1}^{x}\psi(t)\sum_{V\leq n<2V}{}'\Big|\sum_{x_1<p\leq t}{}^{*}\log p\Big(\frac{n}{p}\Big)\Big|\,dt$$

where $\psi(t)$ is the derivative of the function $\frac{1}{\sqrt{t}\log t}$. A direct application of Lemma 6 gives the bound

$$S^{(1)}(V)\ll\frac{\sqrt{x}}{(\log x)^C} \tag{5.8}$$

https://doi.org/10.4153/CJM-1996-004-7 Published online by Cambridge University Press

for every positive C and every $V \leq U$.

It remains to apply the same technique for the sum in (5.2) containing $L(1,\chi_{-4p})$, using now the formula (5.4). The main term coming from this sum is

$$(5.9)\quad 2 \sum_{\substack{n\leq U\\ n \text{ is an odd square}}} \frac{1}{n}\sum_{p\leq x}\frac{1}{\sqrt{p}} = \frac{\pi^2}{4}\cdot\int_2^x \frac{dt}{\sqrt{t}\log t} + O\Big(\sqrt{x}\big(U^{-\frac{1}{2}} + \exp(-\sqrt{\log x})\big)\Big).$$

Gathering the formulas (5.1), (5.2), (5.3), (5.5), (5,6), (5.7), (5.8) and (5.9), we complete the proof of Theorem 4.

6. **Sketch of the proof of Theorem 5.** Let p a prime less than x, and let A, B and x satisfying the assumptions of Theorem 5. Then the quantity $M(A,B,\alpha,\beta,p)$ studied in Lemma 7, satisfies

$$(6.1)\qquad M(A,B,\alpha,\beta,p) = \frac{4AB}{p^2\zeta(10)}\Big(1 + O(p^{-1}) + O\big((\log x)^{-4}\big)\Big),$$

now, following the beginning of the proof of Theorem 4, we have the equality

$$\sum_{|a|\leq A}\ \sum_{\substack{|b|\leq B\\ (a,b)\in\mathcal{M}}} \pi_0(x,a,b) = \sum_{p\leq x}\sum_{\alpha}\sum_{\beta} M(A,B,\alpha,\beta,p)$$

where the inner sum is made over $0 \leq \alpha,\beta < p$, $E_{\alpha,\beta}$ is an elliptic curve $\pmod p$ with exactly $p+1$ points.

By (6.1), this last quantity is equal to

$$\frac{2AB}{\zeta(10)}\sum_{p\leq x}\frac{H(-4p)}{p}\Big(1 + O(p^{-1}) + O\big((\log x)^{-4}\big)\Big) + O(AB\log x).$$

The proof now follows the evaluation of (5.1).

7. **Use of exponential sums. Proof of Theorem 6.** Let p be fixed. In each of the $H(-4p)$ equivalence classes of elliptic curves over $\mathbb{F}_p$, with $p+1$ elements, we choose a curve

$$E_{\alpha,\beta} : y^2 = x^3 + \alpha x + \beta$$

with $0 \leq \alpha,\beta < p$. There are $H(-4p) - O(1)$ of these classes with $E_{\alpha,\beta}$ such that $\alpha\beta \neq 0$.

To prove Theorem 6, we may suppose that A and B are integers plus $\frac{1}{2}$. We dissect the interval $[-A,A]$ into subintervals of length p, the first one being $[-A,-A+p]$, the last one, if not complete is denoted by $\mathcal{A}$. The same procedure is applied to $[-B,B]$, the last interval is called $\mathcal{B}$. With these notations and the notation $[x]$ for the integer part of x, we can write under the assumption $\alpha\beta \neq 0$, the equality

https://doi.org/10.4153/CJM-1996-004-7 Published online by Cambridge University Press

$$\begin{aligned}
&\left|\{(a,b);\,|a|\le A,|b|\le B, E_{a,b} \pmod p \text{ is isomorphic to } E_{\alpha,\beta}\}\right| \\
&\qquad= \left[\frac{2A}{p}\right]\cdot\left[\frac{2B}{p}\right]\cdot\frac{p-1}{2}+\frac{1}{2}\cdot\left[\frac{2A}{p}\right]\left|\{u\in\mathbb{F}_p^*, \beta u^6\in\mathcal{B} \pmod p\}\right| \\
&\qquad\quad+\frac{1}{2}\cdot\left[\frac{2B}{p}\right]\left|\{u\in\mathbb{F}_p^*, \alpha u^4\in\mathcal{A} \pmod p\}\right| \qquad\qquad (7.1)\\
&\qquad\quad+\frac{1}{2}\left|\{u\in\mathbb{F}_p^*, \alpha u^4\in\mathcal{A} \pmod p), \beta u^6\in\mathcal{B} \pmod p\}\right| \\
&\qquad\quad+O\big(\min(A/p^4, B/p^6)\big)
\end{aligned}$$

where the error term comes from the curves $E_{\alpha u^4p^{4k},\beta u^6p^{6k}}$, $(k\ge 1)$. We write the characteristic function of $\mathcal{A} \pmod p$)as

$$\frac{1}{p}\sum_{h=0}^{p-1}\sum_{a\in\mathcal{A}} e\left(\frac{h(t-a)}{p}\right)$$

and the last term in (7.1) becomes

$$\frac{1}{2p^2}\sum_{h=0}^{p-1}\sum_{a\in\mathcal{A}}\sum_{l=0}^{p-1}\sum_{b\in\mathcal{B}}\sum_{u=1}^{p-1} e\left(\frac{h(\alpha u^4-a)+l(\beta u^6-b)}{p}\right).$$

Since $\mathcal{A}$ and $\mathcal{B}$ are intervals, we deduce that this term is equal to

$$\begin{aligned}
&\frac{|\mathcal{A}|\,|\mathcal{B}|}{2}\cdot\frac{p-1}{p^2}+O\left(\frac{|\mathcal{A}|}{p^2}\sum_{l=1}^{p-1}\left\|\frac{l}{p}\right\|^{-1}\left|\sum_{u=1}^{p-1}e\left(\frac{l\beta u^6}{p}\right)\right|\right) \\
&\qquad\qquad+O\left(\frac{|\mathcal{B}|}{p^2}\sum_{h=1}^{p-1}\left\|\frac{h}{p}\right\|^{-1}\left|\sum_{u=1}^{p-1}e\left(\frac{h\alpha u^4}{p}\right)\right|\right) \\
&\qquad\qquad+O\left(\frac{1}{p^2}\sum_{l=1}^{p-1}\sum_{h=1}^{p-1}\left\|\frac{l}{p}\right\|^{-1}\left\|\frac{h}{p}\right\|^{-1}\left|\sum_{u=1}^{p-1}e\left(\frac{h\alpha u^4+l\beta u^6}{p}\right)\right|\right)
\end{aligned}$$

where $\|x\|$ is the distance between x and the nearest integer.

An application of Lemma 7 says that this quantity is equal to

$$\frac{|\mathcal{A}|\,|\mathcal{B}|}{2}\cdot\frac{p-1}{p^2}+O\left(\frac{|\mathcal{A}|\log p}{\sqrt{p}}+\frac{|\mathcal{B}|\log p}{\sqrt{p}}+\sqrt{p}\log^2 p\right),$$

and applying a similar technique to the second and the third term of (7.1), we get

$$\begin{aligned}
&\left|\{(a,b);\,|a|\le A,|b|\le B, E_{a,b} \pmod p \text{ is isomorphic to } E_{\alpha,\beta}\}\right| \\
&\qquad=\frac{p-1}{2}\Big(\left[\frac{2A}{p}\right]\cdot\left[\frac{2B}{p}\right]+\left[\frac{2A}{p}\right]\cdot\frac{|\mathcal{B}|}{p}+\left[\frac{2B}{p}\right]\cdot\frac{|\mathcal{A}|}{p}+\frac{|\mathcal{A}|\,|\mathcal{B}|}{p^2}) \\
&\qquad\quad+O\left((\sqrt{p}\log^2 p)\left(1+\frac{A}{p}+\frac{B}{p}\right)\right).
\end{aligned}$$

https://doi.org/10.4153/CJM-1996-004-7 Published online by Cambridge University Press

Using the equality $[\frac{2A}{p}] + \frac{\mathcal{A}}{p} = \frac{2A}{p}$, we get

$$= \frac{p-1}{2} \cdot \frac{4AB}{p^2} + O\Big((\sqrt{p} \log^2 p) \Big(1 + \frac{A}{p} + \frac{B}{p} \Big) \Big).$$

Now, summing over the $H(-4p) - O(1)$ classes of isomorphism with $\alpha\beta \not\equiv 0 \pmod p$, we arrive at the formula

$$\sum_{|a| \leq A} \sum_{|b| \leq B} \pi_0(x, a, b) = 2AB \sum_{p \leq x} \frac{H(-4p)}{p} + O\big(x^2 \log^3 x + AB \log x + (A + B) x \log^3 x \big)$$

where the error term $O(AB \log x)$ comes from the curves $E_{a,b}$ with $p | ab$.

The proof follows the proof of Theorem 4.

8. **Other types of averagings.** In Theorems 4, 5, and 6, we considered a very large family of curves in two parameters a and b. The aim of this paragraph is to present examples of studies of the function $\pi_0(x, a, b)$ over a thinner family of elliptic curves which is parameterized in one variable only. Some of these results will depend on GRH (*i.e.* the hypothesis that the zeta-function of any number field has no zero with a real part greater than $\frac{1}{2}$) but all of them are based on the fact that the study of the number of zeroes of $P_D(X) \pmod p$, denoted by $\nu(D, p)$, on average, via Chebotarev Theorem, requires the introduction of H_D, the Hilbert class field of the field $\mathbb{Q}(\sqrt{-D})$.

We will prove

THEOREM 7. *Let a_0 and b_0 be two non-zero integers . If we suppose that* GRH *is satisfied for all the ζ_{H_D}, then there exist three constants c_1^+, c_2^+ and $c_2^- > 0$, such that we have*

$$\sum_{|b| \leq B} \pi_0(x, a_0, b) \leq c_1^+ B \frac{\sqrt{x}}{\log x} \tag{8.1}$$

uniformly for $B \geq x \geq x_0(a_0)$

$$c_2^- A \frac{\sqrt{x}}{\log x} \leq \sum_{|a| \leq A} \pi_0(x, a, b_0) \leq c_2^+ A \frac{\sqrt{x}}{\log x} \tag{8.2}$$

uniformly for $A \geq x \geq x_0(b_0)$.

In the case where no particular hypothesis is assumed, there exists a $\theta > 0$, such that the following lower bound holds

$$\sum_{|a| \leq A} \pi_0(x, a, b_0) \geq c_1^- A (\log x)^\theta \tag{8.3}$$

uniformly for $A \geq x \geq x_0(b_0)$.

Note that (8.1) and (8.2) give for $\pi_0(x, a, b)$ average upper and lower bounds which are compatible with the Lang-Trotter Conjecture and that (8.3) produces a much better bound than Theorem 1 but always on average (compare also with Theorem 3(i)).

Since $P_D(X)$ is an irreducible polynomial, Nagell's Theorem asserts that on average over p, $\nu(D, p)$ behaves like 1. But we will work with an unbounded number of polynomials $P_D(X)$, so we require a rather large uniformity over D. By classical techniques from analytic and algebraic number theory, we will prove

https://doi.org/10.4153/CJM-1996-004-7 Published online by Cambridge University Press

LEMMA 9. *Under* GRH, *uniformly for $x \geq 2$ and $D \equiv 0, 3 \pmod 4$, we have the equalities*

$$\sum_{p\leq x} \nu(D,p) = \operatorname{li} x + O(x^{\frac{1}{2}} D^{\frac{1}{2}} \log Dx),$$

$$\sum_{p\leq x, (\frac{-D}{p})=-1} \nu(D,p) = \frac{1}{2} \operatorname{li} x + O(x^{\frac{1}{2}} D^{\frac{1}{2}} \log Dx)$$

and

$$\sum_{\substack{p\leq x, (\frac{-D}{p})=-1 \\ p\equiv 2 \pmod 3}} \nu(D,p) = \frac{1}{4} \operatorname{li} x + O(x^{\frac{1}{2}} D^{\frac{1}{2}} \log Dx) \quad (\text{for } D \neq -3m^2).$$

All these equalities remain true if $\nu(D,p)$ is replaced by $\nu^*(D,p)$, the number of distinct roots of $P_D(X) \pmod p$.

Note that the above equalities give an asymptotic formula for $D \leq x^{1-\varepsilon}$ which is quite satisfactory, since we will use Lemma 9 for $D \ll \sqrt{x}$.

The proof of this lemma requires two lemmas:

LEMMA A. *Let $f(X) \in \mathbb{Z}[X]$ be an irreducible polynomial of degree n. Let $n(f,p)$ be the number of solutions of $f(x) \equiv 0 \pmod p$. Assuming* GRH, *we have*

$$\sum_{p\leq x} n(f,p) = \operatorname{li} x + O\Big(x^{\frac{1}{2}} n\big(\delta(f) + \log x\big)\Big)$$

where

$$\delta(f) = \sum_{p\mid D(f)} \log p + \log n$$

and $D(f)$ is the discriminant of f.

PROOF. Let $K = \mathbb{Q}(\theta)$ with $f(\theta) = 0$. If d_K is the discriminant of K, then the standard methods of analytic number theory yield that the number of prime ideals of degree 1 in K is

$$\pi_K(x) = \operatorname{li} x + O(x^{\frac{1}{2}} \log d_K x^n).$$

(see *e.g.* [Ho] pp. 55–56, [Dave] , [He]).

The result stated in Lemma A follows from two observations. First, $n(f,p)$ is the number of prime ideals of degree 1 in K, lying over p, provided $p \nmid D(f)$. Thus

$$\sum_{p\leq x} n(f,p) = \pi_K(x) + O\Big(n \sum_{p\mid D(f)} 1\Big)$$

(see [He] p. 229 for instance). Second, by a result of Hensel (see [Se] Proposition 6, for instance), we write

$$\log d_K \leq n \sum_{p\mid D(f)} \log p + n \log n$$

which completes the proof.

LEMMA B. *If K is a number field, $f(X) \in O[X]$ is irreducible over K, of degree n and $n(f,\mathfrak{P})$ denotes the number of solutions of $f(X) \equiv 0 \pmod{\mathfrak{P}}$, then assuming* GRH, *we have*

$$\sum_{N\mathfrak{P}\leq x} n(f,\mathfrak{P}) = \operatorname{li} x + O\Big(x^{\frac{1}{2}}[K:\mathbb{Q}]n\big(\delta(f)+\log x\big)\Big)$$

where

$$\delta(f) = \sum_{\mathfrak{P}\mid D(f)} \log N\mathfrak{P} + \log n.$$

In that expression $N\mathfrak{P}$ is the absolute norm of the prime ideal $\mathfrak{P}$ and the implied constant is absolute.

PROOF. The number of prime ideals of K of relative degree from K to $\mathbb{Q}$ greater or equal to 2 and of absolute norm less than x is

$$O([K:\mathbb{Q}]x^{\frac{1}{2}}).$$

The number of prime ideals of $K(\theta)$ lying over a given prime is at most n. Thus the result follows from Lemma A.

PROOF OF LEMMA 9. The first part is immediate from Lemma A, since only prime divisors of D divide $\delta(P_D)$.

If we take $K = \mathbb{Q}(\sqrt{-D})$ in Lemma B, we obtain

$$\sum_{N\mathfrak{P}\leq x} n(P_D,\mathfrak{P}) = \operatorname{li} x + O\big(x^{\frac{1}{2}}D^{\frac{1}{2}}\log Dx\big).$$

Thus

$$(*) \qquad \sum_{p\leq x,(\frac{-D}{p})=1} \nu(D,p) = \frac{1}{2}\operatorname{li} x + O(x^{\frac{1}{2}}D^{\frac{1}{2}}\log Dx).$$

Subtracting from the first assertion gives the result.

Finally, if $K = \mathbb{Q}(\sqrt{-3})$, we note that $P_D(X)$ is still irreducible over $\mathbb{Q}(\sqrt{-3},\sqrt{-D})$ (this is because ramification implies that the fields are disjoint when $D \neq -3m^2$). Hence working over $\mathbb{Q}(\sqrt{-3},\sqrt{-D})$, we find

$$(**) \qquad \sum_{\substack{p\leq x,(\frac{-D}{p})=1\\ p\equiv 1 \pmod 3}} \nu(D,p) = \frac{1}{4}\operatorname{li} x + O(x^{\frac{1}{2}}D^{\frac{1}{2}}\log Dx).$$

Subtracting $(**)$ from $(*)$ yields

$$(***). \qquad \sum_{\substack{p\leq x,(\frac{-D}{p})=1\\ p\equiv 2 \pmod 3}} \nu(D,p) = \frac{1}{4}\operatorname{li} x + O(x^{\frac{1}{2}}D^{\frac{1}{2}}\log Dx)$$

https://doi.org/10.4153/CJM-1996-004-7 Published online by Cambridge University Press

Now consider

$$\sum_{\substack{p\leq x \\ p\equiv 1 \pmod 3}} \nu(D,p).$$

This can be interpreted as follows:

Consider $K=\mathbb{Q}(\sqrt{-3})$ and look at the number of solutions over this field of $P_D(X)\equiv 0 \pmod{\mathfrak{P}}$. By Lemma B, this is

$$2\sum_{\substack{p\leq x \\ p\equiv 1 \pmod 3}} \nu(D,p)=\operatorname{li}x+O(x^{\frac{1}{2}}D^{\frac{1}{2}}\log Dx).$$

Thus, we have, after subtracting from the first part of Lemma 9, the equality

$$\sum_{\substack{p\leq x \\ p\equiv 2 \pmod 3}} \nu(D,p)=\frac{1}{2}\operatorname{li}x+O(x^{\frac{1}{2}}D^{\frac{1}{2}}\log Dx).$$

To complete the proof, it remains to subtract from $(***)$ the above expression.

The following result of Kaneko gives a bound for the least D such that Deuring criterion is satisfied (Lemma 1). We have

LEMMA 10 ([KA], THEOREM 1). *Let E an elliptic curve over $\mathbb{Q}$ and p an odd supersingular prime for E. Then there exists a $D\leq \frac{4}{\sqrt{3}}\sqrt{p}$ such $p\mid \operatorname{Num}\big(P_D(j_E)\big)$, $(\frac{-D}{p})=-1$ or the highest power of p dividing D is odd.*

A. PROOF OF (8.1). To control the size of the supersingular primes we are counting, it is sufficient to prove for $X\leq x$ the upper bound

$$\mathcal{B}(X,B)=\sum_{|b|\leq B}\left(\pi_0(X,a_0,b)-\pi_0\Big(\frac{X}{2},a_0,b\Big)\right)=O\Big(B\frac{\sqrt{X}}{\log X}\Big) \tag{8.4}$$

Since for X large enough, any $D\ll\sqrt{X}$ has no prime divisor greater than $\frac{X}{2}$, Lemma 10 implies that $\mathcal{B}(X,B)$ satisfies the inequality

$$\begin{aligned}\mathcal{B}(X,B)&\leq \sum_{D\ll\sqrt{X}}\sum_{|b|\leq B}\sum_{\substack{\frac{X}{2}<p\leq X \\ p\mid P_D(j_{E_{a_0,b}})}} 1\\ &\ll \sum_{D\ll\sqrt{X}}\sum_{\frac{X}{2}<p\leq X}\Big(\sum_{\substack{\alpha \pmod p \\ P_D(\alpha)\equiv 0 \pmod p}}\sum_{b \pmod p} 1\Big)\frac{B}{p}\end{aligned}\tag{8.5}$$

where the variable of summation satisfies the equation

$$1728\frac{4a_0^3}{4a_0^3+27b^2}\equiv\alpha \pmod p.$$

This quadratic equation in b has at most $O(1)$ solutions (more precisely, at most 2, if $p\nmid 3a_0$). Hence, by (8.5), we find the relation

$$\mathcal{B}(X,B)\ll B\sum_{D\ll\sqrt{X}}\sum_{\frac{X}{2}<p\leq X}\frac{\nu(D,p)}{p}.$$

https://doi.org/10.4153/CJM-1996-004-7 Published online by Cambridge University Press

Lemma 9 is applied under the form

$$\sum_{\frac{X}{2}<p\leq X} \nu(D,p) = O\Big(\frac{X}{\log X}\Big)$$

which gives (8.4) and this proves (8.1).

B. Proof of (8.2). The proof of the upper bound works like in the case of (8.1), except we meet the cubic equation

$$1728\frac{4a^3}{4a^3+27b_0^2} \equiv \beta \pmod p.$$

which has at most three roots if p is large enough. For the lower bound we use the inequality

$$\begin{aligned} \mathcal{A}(x,A) &= \sum_{|a|\leq A}\Big(\pi_0(x,a,b_0) - \pi_0\Big(\frac{x}{2},a,b_0\Big)\Big) \\ &\geq \sum_{\frac{X}{2}<D\leq X}\ \sum_{\substack{\frac{x}{2}<p\leq x;(\frac{-D}{p})=-1 \\ p\nmid P_D(1728)}}\Big(\sum_{\substack{\beta \pmod p \\ P_D(\beta)=0 \pmod p}}\ \sum_{a \pmod p} 1\Big)\frac{A}{p} \end{aligned} \tag{8.6}$$

with $X=\frac{\sqrt{x}}{10}$, where the variable of summation a satisfies

$$1728\frac{4a^3}{4a^3+27b_0^2} \equiv \beta \pmod p; \quad 4a^3+27b_0^2 \not\equiv 0 \pmod p. \tag{8.7}$$

The value of X has been chosen to ensure that Lemma 1 produces different supersingular primes by Lemma 4. The relations (8.7) are equivalent to the unique equation

$$4(1728-\beta)a^3 - 27\beta b_0^2 \equiv 0 \pmod p) \tag{8.8}$$

for p large enough. If we impose the conditions $p\equiv 2 \pmod 3$ and $\beta \not\equiv 1728 \pmod p$, (8.8) has at least one root; we deduce the lower bound

$$\mathcal{A}(x,A) \geq A \sum_{\frac{X}{2}<D\leq X}\ \sum_{\substack{\frac{x}{2}<p\leq x;(\frac{-D}{p})=-1 \\ p\equiv 2 \pmod 3}} \frac{\nu^*(D,p)}{p} - E \tag{8.9}$$

In that expression E is the error term coming from the contribution of terms with $p|P_D(1728)$. For D large enough and for an absolute C, we have the inequalities

$$1 \leq |P_D(1728)| = O\big(\exp(C\sqrt{D}\log^2 D)\big)$$

(the proof is the same as for the inequality for $P_l(j_E)$ mentioned in Lemma 5) and

$$\nu^*(D,p) \leq h(-D)$$

https://doi.org/10.4153/CJM-1996-004-7 Published online by Cambridge University Press

from which we deduce

$$E \ll Ax^{-1} \sum_{D\le X} h(-D)\sqrt{D}\log^2 D \ll Ax^{\varepsilon}. \tag{8.10}$$

It is easy to deduce from (8.6), (8.9), (8.10) and Lemma 9 the lower bound of (8.2).

C. WITHOUT GRH. To obtain (8.3), we proceed by using the unconditional version of the Prime Ideal Theorem. By standard analytic number theory, we obtain the relation

$$\pi_K(x) = \operatorname{li} x + O(\operatorname{li} x^{\beta}) + O\left(x \exp\left(-\sqrt{\frac{\log x}{\log d_K}}\right)\right)$$

with the notation as in the proof of Lemma A. Using Stark's bound for the exceptional Siegel's zero β ([St] Theorem 1′, [MMS] p. 279):

$$\beta < \max\left(1 - \frac{1}{4\log d_K}, 1 - \frac{c_1}{d_K^{\frac{1}{n_K}}}\right)$$

we obtain a uniform result for the sum

$$\sum_{\substack{p\le x, (\frac{-D}{p})=-1\\ p\equiv 2 \pmod 3}} \nu(D,p)$$

only for $D < (\log x)^{\theta}$, for some $\theta > 0$.

REMARK. With more care, we can remove the influence of the Siegel zeroes, thus improving the value of θ.

9. On the least supersingular prime.

The aim of this paragraph is to deal with the following question:

Let $E_{a,b}$ be a given elliptic curve. What is the size of $p_1(a,b)$, which is the least supersingular prime of $E_{a,b}$? Actually, using techniques of the large sieve, we will only prove that $p_1(a,b)$ is very small *for almost all elliptic curves*. In some sense, this result has to be compared with the result concerning the size of the least non quadratic residue (mod p) (see, for instance [Bo], p. 7). We will prove the following

THEOREM 8. *Let $2 \le y \le \sqrt{x}$. Then we have the inequality*

$$\left|\{(a,b); |a| \le x, |b| \le x, p_1(a,b) > y\}\right| \ll_{\kappa} x^2 y^{-\frac{1}{2}} \log^{\kappa} y \tag{9.1}$$

for every $\kappa > 1 - \frac{\pi}{6}$.

This theorem asserts that in this set of $\simeq x^2$ elliptic curves, almost all of them have their least supersingular prime rather small, less than y (say), for instance with $y = \sqrt{x}$, the number of exceptions is $O(x^{\frac{7}{4}}\sqrt{\log x})$. We are concerned by bounds y, which are much smaller than the bound which would emerge by closely following the proof presented in paragraph 3 (with $k = 0$). Note also that the proof of (9.1) is quite straightforward for $\kappa \ge 1$.

The starting point of our proof is a generalisation in several dimensions of the large sieve; we have:

https://doi.org/10.4153/CJM-1996-004-7 Published online by Cambridge University Press

LEMMA 11. *For each prime p, let $\Omega(p)$ be a subset of cardinality $\omega(p)$ of the group $\mathbb{Z}^n/p\mathbb{Z}^n$ of n-dimensional vectors modulo p.*

Let $X > 1$ and $E(X)$ be the number of $\mathbf{x} = (x_1, \ldots, x_n)$ with $\max|x_i| \leq X$, for which $\mathbf{x}$ $\pmod p) \notin \Omega(p)$, for each prime p.

Then, for $X \geq P^2$, we have the inequality

$$E(X) \ll X^n \Big/ \Bigl(\sum_{q \leq P} \mu^2(q) \prod_{p|q} \frac{\omega(p)}{p^n - \omega(p)} \Bigr).$$

Such a result is Lemma A of [Ga] and follows from an n-dimensional analogue of the large sieve inequality (see for instance [Hu] Theorem 1 or [Hl]).

To go from Lemma 11 to Theorem 8, we choose $n = 2; P = y$ and $X = x$. For each p, we define

$$\Omega(p) = \{(\alpha, \beta) \pmod p; E_{\alpha,\beta} \pmod p \text{ is an elliptic curve with } p+1 \text{ points}\}$$

so we have

$$\omega(p) = \frac{p}{2} H(-4p) + O(p)$$

and we note the implication,

$$(a, b) \pmod p \in \Omega(p) \Rightarrow p \text{ is a supersingular prime for } E_{a,b}.$$

(We could get an equivalence above with some care about the minimality of the equation, that is, by considering $(ap^{-4k}, bp^{-6k}) \bmod p$ where k is the largest possible integer.) So, we have by Lemma 11 the relation

$$\bigl|\{(a,b); |a| \leq x, |b| \leq x, p_1(a,b) > y\}\bigr| \ll x^2 / \mathcal{H}(y)$$

with

$$\mathcal{H}(y) = \sum_{q \leq y} \mu^2(q) \prod_{p|q} \frac{\omega(p)}{p^2 - \omega(p)},$$

and $\omega(2) = \omega(3) = 0$. In paragraph 5, we proved the relation

$$\sum_{p \leq y} \frac{H(-4p)}{2p} = \Bigl(\frac{\pi}{3} + o(1)\Bigr) \frac{\sqrt{y}}{\log y} \quad (y \to \infty), \tag{9.2}$$

and, if we use the trivial inequality

$$\mathcal{H}(y) \geq \sum_{p \leq y} \frac{\omega(p)}{p^2 - \omega(p)}$$

we obtain Theorem 8 for any $\kappa = 1$. The improvement comes from taking into account the contribution in $\mathcal{H}(y)$, of integers q which are not prime. We define the multiplicative function $g(n)$ by the formula

$$g(n) = \mu^2(n) \prod_{p|n} \frac{\omega(p)}{p^2 - \omega(p)} \cdot \sqrt{n},$$

https://doi.org/10.4153/CJM-1996-004-7 Published online by Cambridge University Press

then, by partial summation of (9.2), we see that g satisfies

$$\sum_{p\le y} g(p)\log p = \big(a+o(1)\big)y \quad (y\longrightarrow\infty), \tag{9.3}$$

with $a = \frac{\pi}{6}$. The problem is now to find a lower bound for the summatory function $G(x) = \sum_{n\le x} g(n)$. The problem of the upper bound is more popular in the literature, and we were unable to find a published result, which fits to our requirement.

The proof of the following lemma was communicated by G. Tenenbaum:

LEMMA 12. *Let g a multiplicative function satisfying (9.3) (for a strictly positive a) and the relation*

$$g(p)\ge 0 \quad \textit{for every } p \textit{ and } \sum \frac{g^2(p)}{p^2} < \infty. \tag{9.4}$$

Then we have the equality

$$G(x) = \sum_{n\le x} \mu^2(n)g(n) = x(\log x)^{a-1+o(1)}.$$

The upperbound for $G(x)$ is treated by the inequality of Halberstam and Richert under the form

$$G(x) \ll \frac{x}{\log x}\sum_{n\le x}\frac{\mu^2(n)g(n)}{n} \ll \frac{x}{\log x}\exp\sum_{p\le x}\frac{g(p)}{p} \ll x(\log x)^{a-1+o(1)}$$

the last inequality coming from (9.3) after a partial summation.

For the lower bound, we start from the inequality

$$G(x) \ge \sum_{m\le x^{\frac13}}\ \sum_{x^{\frac13}<p\le x/m} \mu^2(m)g(m)g(p) \gg \sum_{m\le x^{\frac13}} \mu^2(m)\frac{g(m)}{m}\cdot\frac{x}{\log x}$$

by (9.3). Put $z = x^{\frac13}$, $t = z^{\varepsilon}$ and denote by $P(m)$ the greatest prime factor of m, then we have

$$\sum_{m\le z}\mu^2(m)\frac{g(m)}{m} \ge \sum_{P(m)\le t}\mu^2(m)\frac{g(m)}{m} - \sum_{\substack{P(m)\le t\\ m>z}}\mu^2(m)\frac{g(m)}{m}. \tag{9.5}$$

By (9.4), the first sum is greater than

$$\prod_{p\le t}\left(1+\frac{g(p)}{p}\right) \ge \exp\left(\sum_{p\le t}\frac{g(p)}{p} - O\left(\sum\frac{g^2(p)}{p^2}\right)\right) \gg \exp\left(\sum_{p\le t}\frac{g(p)}{p}\right).$$

We appeal to Rankin's method to bound from above the second sum, we choose $\alpha = \frac{1}{\log t}$ and write

$$\begin{aligned}\sum_{\substack{P(m)\le t\\ m>z}}\mu^2(m)\frac{g(m)}{m} &\le \sum_{P(m)\le t}\mu^2(m)\frac{g(m)}{m}\left(\frac{m}{z}\right)^{\alpha} \le z^{-\alpha}\prod_{p\le t}\left(1+\frac{g(p)}{p}p^{\alpha}\right)\\ &\le e^{-1/\varepsilon}\exp\left\{\sum_{p\le t}\frac{g(p)}{p} + O\left(\alpha\sum_{p\le t}\frac{g(p)}{p}\log p\right)\right\} \ll e^{-1/\varepsilon}\exp\sum_{p\le t}\frac{g(p)}{p}\end{aligned}$$

by (9.4). We fix a very small value to ε, and by (9.3) and (9.5), we get

$$\sum_{m\leq z}\mu^2(m)\frac{g(m)}{m} \gg \exp\sum_{p\leq t}\frac{g(p)}{p} = (\log x)^{a+o(1)}$$

This ends the proof of Lemma 12.

For the proof of Theorem 8, we are concerned by a lower bound for $\mathcal{H}(y)$, in that context the function $g(p)$ satisfies $g(p) = O(p^\varepsilon)$, so (9.4) is satisfied. The trivial inequality $\mathcal{H}(y) \geq \frac{G(y)}{\sqrt{y}}$ ends the proof of Theorem 8.

10. **Concluding remarks.** These results can be generalized to the context of supersingular Drinfeld modules. This has been done by C. David [Davi] in her doctoral thesis. Indeed, since we have the analogue of the Riemann hypothesis in the Drinfeld context, stronger results can be established unconditionally which improve upon Brown's results [Br2].

REFERENCES

[Bi] B. Birch, *How the number of points of an elliptic curve over a fixed prime field varies*, J. London Math. Soc. **43**(1968), 57–60.

[Bo] E. Bombieri, *Le grand crible en théorie analytique des nombres*, Astérisque, Soc. Math. de France **18** (1974/1987).

[Br1] M. L. Brown, *Note on supersingular primes of elliptic curves over* **Q**, Bull. London Math. Soc. **20**(1988), 293–296.

[Br2] ———, *Singular Moduli and Supersingular Moduli of Drinfeld Modules*, Inven. Math. **110**(1992), 419–439.

[Dave] H. Davenport, *Multiplicative Number Theory (Second Edition)*, Graduate Texts in Math. **74**, Springer Verlag, 1980.

[Davi] C. David, *Supersingular Reduction of Drinfeld Modules*, Ph.D. Thesis, McGill University Montreal, 1993.

[De] M. Deuring, *Die Typen der Multiplikatorenringe elliptischer Funktionenkörper*, Abh. Math. Sem. Univ. Hamburg **14**(1941), 197–272.

[Do] D. Dorman, *Special values of the elliptic modular function and factorisation formulae*, J. Reine Angew. Math. **383**(1988), 207–220.

[El1] N. Elkies, *The existence of infinitely many supersingular primes for every elliptic curve over* **Q**, Invent. Math. **89**(1987), 561–567.

[El2] ———, *Supersingular primes of a given elliptic curve over a number field*, Ph.D. Thesis, Harvard Univ., 1987.

[El3] ———, *Distribution of Supersingular Primes*, Astérisque, J. Arithmétiques de Luminy 1989 **198–200** (1991), 127–132.

[Ga] P. X. Gallagher, *The large sieve and probalistic Galois theory*, Proc. Symp. Pure Math. **XXIV**(1973), 91–101.

[G-Z] B. H. Gross and D. Zagier, *On singular moduli*, J. Reine Angew. Math. **335**(1985), 191–220.

[He] H. Heilbronn, *Zeta functions and L-functions*, Algebraic Number Theory, (eds. J. W. S. Cassels and A. Fröhlich), Academic Press, 1967, 204–230.

[Hl] M. E. Hlawka, *Bemerkungen zum grossen Sieb von Linnik*, Österreich Akad. Wiss. Math.-Natur. S.B. II **178**(1970), 13–18.

[Ho] C. Hooley, *Applications of Sieve Methods to the Theory of Numbers*, Cambridge Tracts in Math. **70**, 1976.

[Hu] M. Huxley, *The large sieve inequality for algebraic number fields*, Mathematika **15**(1968), 178–187.

[Ju] M. Jutila, *On the mean-value of* $L(\frac{1}{2},\chi)$, Analysis **1**(1981), 149–161.

[Ka] M. Kaneko, *Super singular j-invariants* mod p, Osaka J. Math. **26**(1989), 849–855.

[L-T] S. Lang and H. Trotter, *Frobenius in* GL_2 *extensions*, Lecture Notes in Math. **504**, Springer Verlag, 1976.

[Mu] R. Murty, *Recent developments in the theory of elliptic curves*, Proc. of the Ramanujan Centennial International Conf., 1987, 45–54.

[MMS] R. Murty, K. Murty and N. Saradha, *Modular forms and the Chebotarev density theorem*, Amer. J. Math. **110**(1988), 253–281.

[Sc] W. M. Schmidt, *Equations over finite fields. An elementary approach*, Lecture Notes in Math. **536**, Springer Verlag, 1976.

[St] H. M. Stark, *Some effective Cases of the Brauer-Siegel Theorem*, Invent. Math. **23**(1974), 135–152.

[Se] J-P. Serre, *Quelques applications du théorème de densité de Chebotarev*, Inst. Hautes Études Sci. Publ. Math. **54**(1982), 123–201.

Mathématique- Bâtiment 425
Université de Paris-Sud
F-91405 Orsay Cedex
France

Department of Mathematics
McGill University
Montreal, Quebec
H3A 2K6

https://doi.org/10.4153/CJM-1996-004-7 Published online by Cambridge University Press