19. Artin's Conjecture and Elliptic Analogues

M. Ram Murty

1. Introduction

A well-known conjecture of Emil Artin predicts that every natural number a unequal to unity or a perfect square is a primitive root $(\mathrm{mod}\, p)$ for infinitely many primes p. In 1967, Hooley [8] proved this conjecture assuming the generalized Riemann hypothesis (GRH) for the Dedekind zeta functions of certain Kummer extensions. In fact, he establishes an asymptotic formula for the number of such primes up to x. He also remarks in [9] that to deduce a positive density of primes for which a is a primitive root $(\mathrm{mod}\, p)$ it suffices to assume that the corresponding Dedekind zeta functions of the number fields $\mathbb{Q}(a^{1/q})$ do not vanish for $\mathrm{Re}(s) > 1 - 1/2e$.

In 1984, Rajiv Gupta and the author [2] proved that given three prime numbers a, b, c, one of

$$\{ac^2,\ a^3b^2,\ a^2b,\ b^3c^2,\ b^2c,\ a^2c^3,\ ab^3,\ a^3bc^2,\ bc^3,\ a^2b^3c,\ a^3c,\ ab^2c^3,\ abc\}$$

is a primitive root $(\mathrm{mod}\, p)$ for infinitely many primes p. Their method used a lower bound sieve inequality implied by a theorem of Fouvry and Iwaniec. In [5], the authors improved upon this to show that one of the seven numbers

$$\{a,\ b,\ c,\ a^2b,\ ab^2,\ a^2c,\ ac^2\}$$

is a primitive root for infinitely many primes p. By using the Chen-Iwaniec switching and the celebrated theorem of Bombieri, Friedlander and Iwaniec, Heath-Brown [6] refined the above result to show that in fact one of a, b, c is a primitive root $(\mathrm{mod}\, p)$ for infinitely many primes p. The number of such primes obtained by the method is

$$\gg \frac{x}{\log^2 x}.$$

In [6], the result is slightly more general: given three non-zero integers a, b, c which are multiplicatively independent such that none of a, b, c, $-3ab$, $-3ac$, $-3bc$, abc is a perfect square, then one of a, b, c is a primitive root $(\mathrm{mod}\, p)$ for infinitely many primes p. In this paper, we will show

Research supported by NSERC, FCAR and NSF Grant DMS 9304580.

Sieve Methods, Exponential Sums, and their Applications in Number Theory
Greaves, G.R.H., Harman, G., Huxley, M.N., Eds.

Theorem 1. *Let a, b, c be three non-zero integers which are multiplicatively independent such that none of a, b, c, $-3ab$, $-3ac$, $-3bc$, abc is a perfect square. Suppose further that for some $\epsilon > 0$, and each prime q the Dedekind zeta function of $\mathbb{Q}(a^{1/q}, b^{1/q}, c^{1/q})$ has no zeroes in $\mathrm{Re}(s) > 1 - \epsilon$. Then one of a, b, c is a primitive root $(\mathrm{mod}\, p)$ for a positive density of primes p.*

In 1976, Lang and Trotter [13] formulated elliptic analogues of the Artin primitive root conjecture. Suppose E is an elliptic curve over $\mathbb{Q}$ with a rational point of infinite order. A natural question is: how often does the prescribed point generate $E(\mathbb{F}_p)$, the group of points $(\mathrm{mod}\, p)$?

More precisely, let a be a rational point of infinite order. The problem is to determine the density of primes p for which $E(\mathbb{F}_p)$ is generated by $\overline{a}$, the reduction of a $(\mathrm{mod}\, p)$. (Here, in addition to primes of bad reduction, we may need to exclude primes dividing the denominators of the co-ordinates of a.) Such a point will be called a *primitive point* for these primes. Lang and Trotter conjectured that the density of primes for which a is a primitive point always exists. This is the elliptic analogue of Artin's primitive root conjecture.

Of course, situations may (and do) arise when the density is zero. In such a case the set of primes for which a is a primitive point is finite (and often empty). If this is the case, then it is so for obvious reasons. However, if the density is positive, then there are infinitely many such primes.

In considering the elliptic analogue, we see that two assertions are being made about a prime p for which a is a primitive point: first, that $E(\mathbb{F}_p)$ is cyclic and second, that it is generated by the image of a $(\mathrm{mod}\, p)$. Is it even true that $E(\mathbb{F}_p)$ is cyclic infinitely often?

It was Serre [21] who pointed out the relevance of this question. In a course at Harvard in the fall of 1976, he proved that Hooley's method of proving Artin's primitive root conjecture can be adapted to show that the set of primes p for which $E(\mathbb{F}_p)$ is cyclic has a density, assuming the GRH for the Dedekind zeta functions of fields obtained by adjoining the l-division points of E to $\mathbb{Q}$. (These fields should be viewed as the elliptic analogues of the classical cyclotomic extensions.)

In 1980, the author [19] eliminated the use of GRH in Serre's argument for elliptic curves with complex multiplication (CM). More precisely, he proved that the number of primes p for which $E(\mathbb{F}_p)$ is cyclic is

$$\delta_E \frac{x}{\log x} + o\left(\frac{x}{\log x}\right)$$

where

$$\delta_E = \sum_{k=1}^{\infty} \frac{\mu(k)}{n(k)},$$

and $n(k) = [\mathbb{Q}(E[k]) : \mathbb{Q}]$ is the degree of the extension obtained by adjoining the k-division points of E to $\mathbb{Q}$. As noted by Serre, $\delta_E > 0$ if and only if E has an irrational 2-division point. That is, if E has the Weierstrass model

$$y^2 = x^3 + cx + d$$

we require that $x^3 + cx + d$ has an irrational root. It is not difficult to see that the density is positive in this case. Indeed, for l prime and greater than some constant C (say),

$$n(l) \asymp l^2$$

in the CM case and

$$n(l) \asymp l^4$$

in the non-CM case, by a celebrated theorem of Serre. Moreover, since $\mathbb{Q}(E[l])$ contains the lth cyclotomic field, we easily see that

$$\delta_E \geq \tfrac{1}{2} \prod_{2<l\leq C} \left(1 - \frac{1}{l-1}\right) \prod_{l>C} \left(1 - \frac{1}{n(l)}\right) > 0.$$

In the non-CM case, it is still unknown if $E(\mathbb{F}_p)$ is cyclic for a positive density of primes whenever E has an irrational 2-division point. However, Gupta and the author [3] proved that if E has an irrational 2-division point then the number of primes $p \leq x$ for which $E(\mathbb{F}_p)$ is cyclic is

$$\gg \frac{x}{\log^2 x}.$$

The method used to prove Theorem 1 can be utilised to prove

Theorem 2. *Let E be an elliptic curve over $\mathbb{Q}$ without complex multiplication. Suppose E has an irrational 2-division point. Suppose for some $\epsilon > 0$ and for each prime q that the Dedekind zeta function of the fields $\mathbb{Q}(E[q])$ does not have any zeroes in the region $\mathrm{Re}(s) > 1 - \epsilon$ Then $E(\mathbb{F}_p)$ is cyclic for a positive density of prime numbers. That is, the number of such primes $p \leq x$ is $\geq cx/\log x$ for some positive constant c.*

Returning to the original conjecture of Lang and Trotter, it was recognized by Serre, Lang and Trotter that the method of Hooley cannot be adapted to the elliptic curve case owing to the large error terms introduced by the Chebotarev density theorem. This problem was, however, circum-

vented by Gupta and the author [4] in the CM case. They proved: if E is an elliptic curve over $\mathbb{Q}$, with CM, and a is a rational point of infinite order, then the number of primes p for which $E(\mathbb{F}_p)$ is generated by a has a density, assuming the GRH for the Dedekind zeta functions associated to extensions of the form $\mathbb{Q}\big(E[l], l^{-1}a\big)$. (These extensions are the elliptic analogues of the classical Kummer extensions.) If E is an elliptic curve over $\mathbb{Q}$ with CM by k, then k can be one of nine fields. If k is one of

$$\mathbb{Q}\big(\sqrt{-11}\big), \quad \mathbb{Q}\big(\sqrt{-19}\big), \quad \mathbb{Q}\big(\sqrt{-43}\big), \quad \mathbb{Q}\big(\sqrt{-67}\big), \quad \mathbb{Q}\big(\sqrt{-163}\big),$$

then it is shown on p. 30 of [4] that the density is positive. It is also shown to be positive in certain instances when k is one of the four remaining fields. At the end of their paper, they proved: there is a finite set S (which can be given explicitly) such that, for some $a \in S$, $E(\mathbb{F}_p) = \langle \overline{a} \rangle \pmod{p}$ for infinitely many primes p, provided the Mordell-Weil rank of $E(\mathbb{Q})$ is at least 6. They did not give the size of S, but an examination of their paper shows that $|S| = 2^{18}$.

We will show

Theorem 3. *Let E be an elliptic curve with CM. Suppose*

$$\{P_1, \ldots, P_6\}$$

are independent points of infinite order in $E(\mathbb{Q})$. Then, for infinitely many primes p, one of $P_1, \ldots, P_6$ generates a subgroup of $E(\mathbb{F}_p)$ of index bounded by 4.

Remark. This is a substantial improvement of the result of Gupta and Murty. Note that we assume that the rank of $E(\mathbb{Q})$ is at least 6. Mestre [14] has shown that there are infinitely many elliptic curves E defined over $\mathbb{Q}$ with j-invariant equal to zero (and hence with CM) such that this holds. Such curves are twists of the curve $y^2 = x^3 + 1$. By a more careful and detailed analysis, it should be possible to obtain index 1 in the case where E has an irrational 2-division point.

We will now give a brief description of the basic strategy involved in proving these theorems. Let us first consider Theorem 1. In [6] the lower bound sieve method combined with the Chen-Iwaniec switching method gave rise to $\gg x/\log^2 x$ primes $p \leq x$ such that either $p - 1 = 2^e q$ for some odd prime q or $p - 1 = 2^e q_1 q_2$ with $q_1 < q_2$ and q_1 satisfying $p^\alpha < q < p^\delta$ for some $\alpha > \frac{1}{4}$ and $\delta < \frac{1}{2}$. By imposing a suitable initial congruence condition, one can also ensure that none of a, b, c is a quadratic residue $\pmod{p}$ for these primes and that e is bounded. It is now clear that if

$p-1=2^e q$ with q prime then each of a, b, c is a primitive root $(\mathrm{mod}\, p)$ for all but finitely many such primes. So we only need to deal with the second case. By essentially the pigeonhole principle one can show that for almost all of these primes the subgroup generated by a, b, c $(\mathrm{mod}\, p)$ cannot have order $< x^{1-\alpha}$, which would be the case if either q_1 or q_2 divides the index of $[\mathbb{F}_p^* : \langle a, b, c\rangle]$. But now there are only two possible orders for each of a, b, c. Two must have the same order by the pigeonhole principle again! Once more by this principle, this can happen for at most $O\big(x^{1-2\delta}\big)$ such primes $p \le x$.

The essential ingredients in the proof are the sieve exponents $\alpha > \frac{1}{4}$ and $\delta < \frac{1}{2}$. As indicated on p. 34 of [6], the theorem of Bombieri, Friedlander and Iwaniec alluded to above gives $\alpha = .276$. Since all that is needed in the proof is an exponent greater than $\frac{1}{4}$, there is some room for introducing certain degrees of freedom. We relax the conditions on $p-1$ and consider primes of the form $p-1 = 2^e mq$ or $p-1 = 2^e mq_1q_2$ where q, q_1, q_2 are primes satisfying the same constraints above and $m < x^\epsilon$ for some small $\epsilon > 0$. This relaxation produces a positive proportion of primes satisfying these conditions. The argument briefly indicated above shows that for almost all these primes one of a, b, c has order divisible by $2^e q$ (in the first case) and $2^e q_1 q_2$ (in the second case). We still need to rule out the possibility that a prime divisor q of m can divide the index of one of $[\mathbb{F}_p^* : \langle a\rangle]$, $[\mathbb{F}_p^* : \langle b\rangle]$, $[\mathbb{F}_p^* : \langle c\rangle]$. This is done by the effective Chebotarev density theorem. This theorem implies that the number of primes $p \le x$ for which a prime q divides the index $[\mathbb{F}_p^* : \langle a\rangle]$ is

$$\frac{\mathrm{li}\, x}{q(q-1)} + O\left(x^{1-\epsilon}\right)$$

uniformly for $q < x^\epsilon$, if we are assuming a quasi-Riemann hypothesis of the type stated in Theorem 1. (The best unconditional result is due to Pappalardi ([17], p. 40) who has proved an asymptotic formula of the type

$$\frac{\mathrm{li}\, x}{q(q-1)} + O\left(\frac{x}{\log^A x}\right)$$

uniformly for $q < \log^{1-\eta} x$.) Invoking this result in the appropriate range leads to Theorem 1.

Theorems 2 and 3 are proved analogously using the elliptic analogues of the appropriate pigeonhole arguments. (See §6 below.)

It is a pleasure to thank C.S. Rajan, V. Kumar Murty, John Friedlander and Henryk Iwaniec for useful discussions, and the Institute for Advanced Study for its hospitality and financial support.

2. Sieve preliminaries

For a positive integer k, we define $\tau_k(n)$ as the the number of ways of writing n as a product of k positive integers. An arithmetical function $\lambda(q)$ is said to be of level Q and of order k if

$$\lambda(q) = 0 \quad \text{for} \quad q > Q, \qquad \big|\lambda(q)\big| \leq \tau_k(q).$$

The function λ is *well-factorable* if for any $Q_1, Q_2 \geq 1$ with $Q_1 Q_2 = Q$ there exist two arithmetical functions λ_1, λ_2 of levels Q_1, Q_2 and of order k such that $\lambda = \lambda_1 * \lambda_2$. (Here $*$ indicates the Dirichlet convolution of two arithmetical functions.) Well-factorable coefficients appear in the error term of the Rosser-Iwaniec linear sieve (see the lemma below). We make the convention that $\lambda(q)$ will always denote a well-factorable function of level Q and of order k. It is clear that if λ' is another arithmetical function of level Q' (with $Q' \leq Q$) and of order k' then the arithmetical function $\lambda * \lambda'$ is well-factorable of level QQ' and of order $k + k'$.

We now state the formula of the Rosser-Iwaniec sieve. For $\mathcal{A}$ a finite sequence of integers and $\mathcal{P}$ a set of prime numbers we are interested in evaluating, for $z \geq 2$,

$$S(\mathcal{A}, \mathcal{P}, z) = \#\big\{a \in \mathcal{A} : \big(a, P(z)\big) = 1\big\},$$

where

$$P(z) = \prod_{p \leq z;\, p \in \mathcal{P}} p.$$

If d is a squarefree integer with all its prime factors belonging to $\mathcal{P}$, we denote

$$\mathcal{A}_d = \big\{a \in \mathcal{A} : d \,|\, a\big\}$$

and write its cardinality (as a multiset) as

$$|\mathcal{A}_d| = \frac{\omega(d)}{d} X + r_d(\mathcal{A}), \tag{1}$$

where $X > 1$ is independent of d and $\omega(d)$ is a multiplicative function satisfying

$$0 \leq \omega(p) < p \quad \text{for} \quad p \in \mathcal{P}. \tag{2}$$

One thinks of X as an approximation to the size of $\mathcal{A}$ and $r_1(\mathcal{A})$ as the error in the approximation. We define

$$V(z) = \prod_{p < z;\, p \in \mathcal{P}} \left(1 - \frac{\omega(p)}{p}\right) \tag{3}$$

and suppose that

$$\frac{V(z_1)}{V(z_2)} \leq \frac{\log z_2}{\log z_1}\left(1+\frac{K}{\log z_1}\right) \quad \text{for} \quad z_2 \geq z_1 \geq 2$$

where K is some constant > 1. Then

Lemma 1. (Rosser-Iwaniec sieve) *Let $0 < \epsilon < \frac{1}{8}$, $2 \leq z \leq Q^{1/2}$. Under* (1), (2), (3) *above, we have*

$$S(\mathcal{A},\mathcal{P},z) \leq XV(z)\big(F(\log Q/\log z)+E\big)+\sum_{l<L}\sum_{q|P(z)}\lambda_l^+(q)r_q(\mathcal{A}),$$
$$S(\mathcal{A},\mathcal{P},z) \geq XV(z)\big(f(\log Q/\log z)-E\big)-\sum_{l<L}\sum_{q|P(z)}\lambda_l^-(q)r_q(\mathcal{A}).$$

Here, L depends only on ϵ, and λ_l^+, λ_l^- are well-factorable functions of order 1 and of level Q. The constant E satisfies

$$E = O\left(\epsilon + \epsilon^{-8}e^K/\log^{\frac{1}{3}}Q\right).$$

The continuous functions $F(s)$ and $f(s)$ are defined recursively by

$$F(s) = 2e^\gamma/s, \quad f(s) = 0 \qquad \text{for} \quad s \leq 2,$$
$$\big(sF(s)\big)' = f(s-1), \quad \big(sf(s)\big)' = F(s-1) \quad \text{for} \quad s > 2,$$

and γ denotes Euler's constant.

Proof. See [10] and [11].

Lemma 2. *Let $(u,v) = 1$. For any q such that $(q,v) = 1$, define u^* to be the solution of the congruences $u^* \equiv u \pmod v$, $u^* \equiv 1 \pmod q$. Suppose that $\epsilon > 0$ and $A > 0$. Then, for any well-factorable function λ of level $x^{4/7-\epsilon}$, one has*

$$\sum_{(q,v)=1}\lambda(q)\left(\pi(x,qv,u^*)-\frac{\operatorname{li} x}{\phi(qv)}\right) \ll \frac{x}{\log^A x},$$

where the implied constant depends only on u, v, ϵ and A.

Proof. This is Heath-Brown's ([6], p. 29) slight adjustment of Theorem 10 of [1].

Lemma 3. *Let*

$$\pi(X;a,d,l) = \sum_{\substack{ap\leq X\\ ap\equiv l \,(\mathrm{mod}\, d)}} 1$$

and let $f(a)$ be a real-valued function satisfying the conditions

$$\sum_{n\leq x}|f(n)| \ll x\log^{c_1} x, \qquad \sum_{n\leq x}\sum_{d|n}|f(d)| \ll x\log^{c_2} x,$$

where c_1, c_2 are positive constants. Given $A>0$, there is a $B=B(A,c_1,c_2)$ such that

$$\sum_{d\leq \frac{\sqrt{X}}{\log^B X}} \max_{y\leq X}\max_{(l,d)=1}\left|\sum_{\substack{a\leq X^{1-\epsilon}\\ (a,d)=1}} f(a)\Big(\pi(y;a,d,l)-\frac{\pi(y;a,1,1)}{\phi(d)}\Big)\right| \ll \frac{X}{\log^A X}$$

and $0<\epsilon<1$.

Proof. This is Theorem 3, combined with the remark on p. 281 of [16].

Lemma 4. *Fix a prime $p_1 < x^{1/2}$. Then the number of primes $p\leq x$ such that $p-1=4p_1p_2$ with p_2 a prime is*

$$\ll \frac{x}{p_1\log^2 x}.$$

Proof. This is a standard application of Brun's sieve (see e.g. Theorem 3.12 of [7]).

3. An application of the lower bound sieve

Our goal in this section and the next is to set up the apparatus to prove Theorem 4 stated below. We begin as in [6].

Let $K=2^k$ with $k=1$, 2 or 3 and let u and v be coprime integers such that $K\,|\,(u-1)$, $16\,|\,v$ and $\big((u-1)/K, v\big)=1$. Fix an integer m coprime to v. Define

$$\mathcal{A}_m = \left\{\frac{p-1}{Km} : p\leq x,\ p\equiv u\ (\mathrm{mod}\, v),\ p\equiv 1\ (\mathrm{mod}\, m)\right\};$$

$\mathcal{P}_m$ will denote the set of odd primes coprime to vm. We will use Lemma 1 to derive a lower bound for $S(\mathcal{A}_m,\mathcal{P}_m,z)$. Indeed, if q is coprime to vm, we may write

$$\#\{a\in\mathcal{A}_m : q\,|\,a\} = \pi(x,vqm,u^*) = \frac{\mathrm{li}\, x}{\phi(qvm)} + r_{vqm} \quad \text{(say)}.$$

The conditions $u \equiv 1 \pmod K$, $v \equiv 0 \pmod K$ and $(q, v) = 1$ imply that if $p \equiv u \pmod v$ then the conditions $p \equiv 1 \pmod{Kq}$ and $p \equiv 1 \pmod q$ are equivalent. Define

$$X = \frac{\operatorname{li} x}{\phi(v)\phi(m)}, \qquad \omega(d) = \frac{d}{\phi(d)}.$$

Applying Lemma 1 yields, for $z = x^\alpha$, $Q = x^\mu$,

$$S(\mathcal{A}_m, \mathcal{P}_m, x^\alpha) \geq X \prod_{\substack{p \leq x^\alpha \\ p \nmid vm}} \left(1 - \frac{1}{p-1}\right) \{f(\mu/\alpha) - \epsilon\} - \sum_{l<L} \sum_{q \mid P_m(x^\alpha)} \lambda_l^-(q) r_{qm},$$

for some well-factorable functions λ_l^- of level x^μ, where L depends only on ϵ.

Fix an integer N and sum the above inequality over $m \leq z$ with $(m, N) = 1$ and $z \leq x^{\epsilon_1}$ (with ϵ_1 sufficiently small and to be chosen later) to obtain

$$\sum_{\substack{m \leq z \\ (m,N)=1}} S(\mathcal{A}_m, \mathcal{P}_m, x^\alpha) \geq \sum_{m \leq z} \frac{\operatorname{li} x}{\phi(vm)} \prod_{\substack{p \leq x^\alpha \\ p \nmid vm}} \left(1 - \frac{1}{p-1}\right) \{f(\tfrac{4}{7}\alpha) - \epsilon\} + O\left(\frac{x}{\log^A x}\right),$$

by Lemma 1 and Lemma 2 and noting that summing over m introduces only new well-factorable functions of essentially the same level. The sum on the right is an enumeration of disjoint sets and is easily evaluated:

$$\frac{1}{\phi(vm)} \prod_{\substack{p \leq x^\alpha \\ p \nmid vm}} \left(1 - \frac{1}{p-1}\right) = \frac{1}{\phi(vm)} \prod_{2 < p \mid vm} \frac{p-1}{p-2} \prod_{2 < p \leq x^\alpha} \left(1 - \frac{1}{p-1}\right),$$

and it is not difficult to see by standard methods of analytic number theory that the sum is, for some constant c_1 (which may depend on v),

$$\geq c_1 \frac{\phi(N)}{N} \frac{x \log z}{\log^2 x} \left\{ \frac{2e^{-\gamma}}{\alpha} f(\tfrac{4}{7}\alpha) - \epsilon \right\} + O\left(\frac{x}{\log^A x}\right).$$

4. The upper bound sieve

As in [6], we employ the Chen-Iwaniec switching method. We now consider

$$\mathcal{B}_m = \{1 + Kmp_1p_2p_3 \leq x \ : \ p_i \geq x^\alpha, \ 1 + Kmp_1p_2p_3 \equiv u \pmod v\},$$

where the different orderings of p_1, p_2, p_3 are to be counted as distinct so that $\mathcal{B}_m$ is a multiset. If $(q, mv) = 1$ then

$$\#\{b \in \mathcal{B}_m : q|m\} = \#\{p_1p_2p_3 \leq y \ : \ p_i \geq x^\alpha, \ p_1p_2p_3 \equiv l \pmod{mqv/K}\},$$

where $y = (x-1)/Km$ and l is the common solution of

$$Kml + 1 \equiv u \pmod v \qquad Kl + 1 \equiv 0 \pmod q.$$

Let

$$g_m(a) = \#\{mp_2p_3 = a : p_2, p_3 \geq x^\alpha\}$$

and note that $g_m(a) \leq \tau_3(a)$. By the upper bound sieve (Lemma 1) we obtain

$$S(\mathcal{B}_m, \mathcal{P}_m, x^{\frac{1}{2}-\epsilon'}) \leq Y \prod_{\substack{p \leq x^{1/2-\epsilon'} \\ p \nmid vm}} \left(1 - \frac{\omega(p)}{p}\right)(F(1) + \epsilon) + R_m,$$

where

$$Y = \frac{1}{\phi(mv/K)} \sum_{a \leq yx^{-\alpha}} g_m(a)(\pi(y/a) - \pi(x^\alpha)),$$

$$F(1) = 2e^\gamma, \qquad R_m = \sum_{\substack{q \leq x^{1/2}\log^{-A} x \\ (q, mv)=1}} \lambda_l^+(q) r_q(\mathcal{B}_m),$$

$$r_q(\mathcal{B}_m) = \sum_{a \leq yx^{-\alpha}} g_m(a)(E(y; a, mqv/K, l) - E(ax^\alpha; a, mqv/K, l))$$

$$E(y; a, mqv/K, l) = \pi(y; a, mqv/K, l) - \frac{\pi(y/a)}{\phi(mqv/K)}.$$

Again, we sum over $m \leq z$, $(m, N) = 1$:

$$\sum_{m \leq z} S(\mathcal{B}_m, \mathcal{P}_m, x^{\frac{1}{2}-\epsilon'}),$$

and find that the main term of the upper bound is

$$\leq c_1 \frac{\phi(N)x\log z}{N\log^2 x}\left(8e^{-\gamma}IF(1)+\epsilon'\right),$$

where

$$I=\int_{\alpha}^{1-2\alpha}\log\left(\frac{1-\alpha-\theta}{\alpha}\right)\frac{d\theta}{\theta(1-\theta)}.$$

The error term is

$$\sum_{m\leq z}\sum_{l<L}\sum_{q<x^{1/2-\epsilon'}}\lambda_l^+(q)r_q(\mathcal{B}_m),$$

and we can apply Pan's theorem (Lemma 3) with

$$f(a)=\sum_{m\leq z}g_m(a)$$

which is bounded by a divisor function. Hence for some $\epsilon_1>0$ we have established the following:

Theorem 4. *Let $(u,v)=1$ and N be fixed integers and $z\leq x^{\epsilon_1}$. The number of primes $p\leq x$ such that* (i) $p\equiv u \pmod v$ (ii) *every odd prime divisor q of $p-1$ satisfies one of the conditions*

$$q\geq x^{\frac{1}{4}+\epsilon} \quad \text{or} \quad q|m \text{ with } m\leq z,\ (m,N)=1$$

is at least

$$\gg \frac{\phi(N)x\log z}{N\log^2 x}.$$

Proof. As on p. 31 of [6], the quantity we want to enumerate is at least

$$\sum_{\substack{m\leq z\\(m,N)=1}} S(\mathcal{A}_m,\mathcal{P}_m,x^{\alpha})-\tfrac{1}{6}S(\mathcal{B}_m,\mathcal{P}_m,x^{\frac{1}{2}})+O(x^{1-\alpha}).$$

By the lower bound obtained in section 3 and the upper bound obtained above, we are done after analyzing the constants. But this is the same analysis as on p. 34 of [6].

A similar result can be stated with $p-1$ replaced by $p+1$ in Theorem 4. This will be useful in considering elliptic analogues of the Artin primitive root conjecture in §9.

We can refine Theorem 4 to ensure that if $p-1$ has at least two prime divisors $q_2>q_1>x^{1/4+\epsilon}$ then $q_1<x^{1/2-\delta}$ for some $\delta>0$. To see this, for

fixed q_1 let us enumerate the number of primes $p \leq x$ such that $p-1 = q_1 n$ and n is free of prime factors in the interval $(z, x^{1/2})$. By Brun's sieve, the number of such primes is

$$\ll \frac{x \log z}{q_1 \log^2 x}.$$

Summing over $x^{1/2-\delta} < q_1 < x^{1/2}$, we get an estimate of

$$\frac{\delta x \log z}{\log^2 x}$$

for the number of such primes. Choosing δ sufficiently small yields

Theorem 4*. *Let $(u,v) = 1$ and N be fixed integers. Let ϵ_1 be as in Theorem 4 and let $z \leq x^{\epsilon_1}$. There is a $\delta = \delta(\epsilon_1) > 0$ such that there are at least*

$$\gg \frac{\phi(N) x \log z}{N \log^2 x}$$

primes $p \leq x$ such that (i) *$p-1$ has no prime factor in the interval $(x^{1/2-\delta}, x^{1/2})$* (ii) *$p \equiv u \pmod{v}$* (iii) *every odd prime divisor q of $p-1$ satisfies one of the conditions*

$$q > x^{\frac{1}{4}+\epsilon}, \quad \text{or} \quad q | m \text{ with } m \leq z, \ (m, N) = 1.$$

If E is an elliptic curve defined over $\mathbb{Q}$ with complex multiplication by an imaginary quadratic field F, then F is one of nine fields of class number one. If p is a prime of good reduction for E and inert in F, then $\left|E(\mathbb{F}_p)\right| = p+1$. Such primes are determined by congruence conditions modulo the discriminant of F and form a set of Dirichlet density $\frac{1}{2}$. We will sieve the sequence

$$\mathcal{S} = \{p+1 : p \leq x, \ p \text{ inert in } F\}$$

and apply the same reasoning to deduce

Theorem 5. *Let F be one of the nine imaginary quadratic fields with class number one. Let N be a fixed integer. There is an $\epsilon_1 > 0$ and a $\delta = \delta(\epsilon_1) > 0$ such that at least*

$$\gg \frac{\phi(N) x \log z}{N \log^2 x}$$

primes $p \leq x$ have the following properties: (i) *$p+1$ has no prime factor in the interval $\left(x^{1/2-\delta}, x^{1/2}\right)$* (ii) *$p$ is inert in F* (iii) *every odd prime divisor q of $p+1$ satisfies one of the conditions*

$$q > x^{\frac{1}{4}+\epsilon} \quad \text{or} \quad q | m \text{ with } m \leq z, \ (m, N) = 1 \quad \text{where} \quad z \leq x^{\epsilon_1}.$$

In addition, the power of 2 dividing $p+1$ is bounded.

5. Results on the Chebotarev density theorem

We record in this section two lemmas derived from the effective Chebotarev density theorem (see [15], [22], and [12]).

Lemma 5. *Let a be squarefree and q an odd prime. The number of primes $p \leq x$ such that $q \mid [\mathbb{F}_p^* : \langle a \rangle]$ is*

$$\frac{\operatorname{li} x}{q(q-1)} + O\left(\frac{x}{\log^A x}\right),$$

for any $A > 0$ and uniformly for $q \leq \log^{1/4} x$. Suppose that for some $\epsilon > 0$ and each prime q the Dedekind zeta function of $\mathbb{Q}(a^{1/q})$ has no zeroes for $\operatorname{Re}(s) > 1 - \epsilon$. Then the number of primes $p \leq x$ such that $q \mid [\mathbb{F}_p^* : \langle a \rangle]$ is

$$\frac{\operatorname{li} x}{q(q-1)} + O\left(x^{1-\epsilon/2}\right)$$

uniformly for $q \leq x^\epsilon$.

Proof. See p. 243 of [20] for the first part of the assertion in the lemma. For the second part, one derives it easily by the standard method (for instance as in [9]). As remarked earlier, Pappalardi [17] has extended the range of validity of the first part of the lemma.

Lemma 6. *Let E be an elliptic curve defined over $\mathbb{Q}$ without CM. Let q be a prime such that $q > c(E)$, where $c(E)$ depends only on E. Then the number of primes $p \leq x$ such that $E(\mathbb{F}_p)$ contains a subgroup of type (q, q) is*

$$\frac{\operatorname{li} x}{(q^2-1)(q^2-q)} + O\left(\frac{x}{\log^A x}\right),$$

for any $A > 0$, uniformly for $q \leq (\log x)^{1/6}$. If we assume that for each prime q the Dedekind zeta function of $\mathbb{Q}(E[q])$ has no zeroes in $\operatorname{Re}(s) > 1-\epsilon$, then the number of primes $p \leq x$ such that $E(\mathbb{F}_p)$ contains a subgroup of type (q, q) is

$$\frac{\operatorname{li} x}{(q^2-1)(q^2-q)} + O\left(x^{1-\epsilon/2}\right)$$

uniformly for $q \leq x^\epsilon$.

Proof. This is again a direct application of the effective Chebotarev density theorem. The proofs are analogous to those in the previous lemma.

Lemma 7. *Let E be an elliptic curve defined over $\mathbb{Q}$ and with CM. Let a be a point of infinite order in $E(\mathbb{Q})$. There is a constant $c_2(E)$ such that for a prime $q > c_2(E)$ the number of primes $p \leq x$ such that $q \mid [E(\mathbb{F}_p) : \langle a \rangle]$ is*

$$\frac{\operatorname{li} x}{n(q)} + O\left(\frac{x}{\log^A x}\right),$$

for any $A > 0$, uniformly for $q \leq \log^{1/5} x$ and $n(q) \asymp q^4$. If, for some $\epsilon > 0$ and each prime q, the Dedekind zeta function of $\mathbb{Q}(E[q], q^{-1}a)$ has no zero in $\operatorname{Re}(s) > 1 - \epsilon$ then the number of primes $p \leq x$ such that $q \mid [E(\mathbb{F}_p) : \langle a \rangle]$ is

$$\frac{\operatorname{li} x}{n(q)} + O(x^{1-\epsilon/2})$$

uniformly for $q \leq x^\epsilon$.

Proof. Again, we apply the effective Chebotarev density theorem as in [2], [3] and [4].

6. Further lemmata

In this section, we formalize the pigeonhole principle in a quantitative manner as in [2] and [4].

Lemma 8. *Let $a_1, \ldots, a_r$ be r multiplicatively independent integers. The number of primes p such that the image of $\langle a_1, \ldots, a_r \rangle \pmod p$ has order not exceeding y is $O(y^{1+1/r})$.*

Below we discuss the elliptic analogues of Lemma 8.

Suppose we have a free subgroup Γ of rational points of rank (over $\mathbb{Z}$) equal to r. Let $P_1, \ldots, P_r$ be r independent generators of Γ. We will make use of the canonical height pairing of Néron and Tate to estimate the number of primes p for which the image Γ_p of $\Gamma \pmod p$ is small. Such a situation arises naturally as follows. Suppose that $q \mid [E(\mathbb{F}_p) : \Gamma_p]$ and that $q > z$. For primes $p \leq x$ this means that

$$|\Gamma_p| \leq \frac{x}{z}.$$

Thus, if z is large, the image of $\Gamma \pmod p$ is small. If we can show that the number of primes satisfying the above inequality is small, we can conclude that for most primes $q \nmid [E(\mathbb{F}_p) : \Gamma_p]$ with $q > z$. This is our basic strategy.

Recall that the canonical height pairing of Néron and Tate is a positive semidefinite bilinear pairing on $E(\overline{\mathbb{Q}})$ with the property that $\langle P, P \rangle = 0$ if and only if P is a torsion point. This height pairing is related to the naïve height of Weil in the following way. If $P = (x, y) \in E(\mathbb{Q})$ then, writing $x = r/s$ with r, s coprime integers, we define the x-height of P as

$$h_x(P) = \log \max(|r|, |s|).$$

Observe that the image of $P \pmod p$ is the identity element if and only if $p \mid s$. Since the number of prime divisors of s is bounded by $2\log|s|$ we note that the number of primes for which P reduces to the identity element on $E(\mathbb{F}_p)$ is bounded by $2h_x(P)$. (Recall that the identity element on E is the point at infinity.) If we let $H(P) = \langle P, P\rangle$ then, for $P \in E(\mathbb{Q})$,

$$H(P) = h_x(P) + O(1),$$

where the implied constant depends only on E. So we can use $H(P)$ as an upper bound for the number of primes p for which P reduces to the identity on $E(\mathbb{F}_p)$.

Lemmas 9 and 10 appear in [4] and are reproduced here for the sake of completeness.

Lemma 9. *The number of r-tuples of integers $(n_1, \dots, n_r)$ satisfying*

$$H(n_1P_1 + \cdots + n_rP_r) \le x$$

is

$$\frac{(\pi x)^{r/2}}{\sqrt{R}\Gamma\left(\frac{1}{2}r+1\right)} + O\left(x^{\frac{1}{2}(r-1)+\epsilon}\right)$$

where $R = \det(\langle P_i, P_j\rangle)$.

Proof. We want to determine the integer solutions of

$$\left\langle \sum_{i=1}^{r} n_iP_i, \sum_{i=1}^{r} n_iP_i \right\rangle \le x,$$

which is the same as

$$\sum_{i,j} n_in_j\langle P_i, P_j\rangle \le x.$$

This is tantamount to counting lattice points in the r-dimensional ellipsoid determined by the above quadratic form. By a result of Walfisz [23] the number of such lattice points is given by the expression stated in the lemma. (Note that in [4], the reference to Walfisz [23] appears with an incorrect year.)

Lemma 10. *The number of primes p such that $|\Gamma_p| \le y$ is $O\left(y^{1+2/r}\right)$.*

Proof. Consider the set S of all r-tuples $(n_1, \dots, n_r)$ satisfying

$$H(n_1P_1 + \cdots + n_rP_r) \le Cy^{2/r},$$

where C is any constant chosen so that

$$\frac{(C\pi)^{r/2}}{\sqrt{R}\Gamma\left(\frac{1}{2}r+1\right)} > 1$$

with C greater than the O- constant implied by Lemma 3. Then by Lemma 3 the number of elements of S is $> y$. If p is a prime such that $|\Gamma_p| < y$

then we must have for two distinct r-tuples $(n_1, \ldots, n_r)$ and $(m_1, \ldots, m_r)$ the congruence

$$n_1P_1 + \cdots + n_rP_r \equiv m_1P_1 + \cdots + m_rP_r \pmod{p}.$$

Since $P_1, \ldots, P_r$ are $\mathbb{Z}$-independent, the point

$$Q = \sum_{i=1}^{r}(n_i - m_i)P_i$$

is non-zero and the above congruence $(\mathrm{mod}\, p)$ implies that p divides the denominator of Q. As remarked above, the number of such primes is bounded by $2h_x(Q)$ because a natural number n has at most $2\log n$ prime factors. Moreover Q is not a torsion point since $P_1, \ldots, P_r$ are independent over $\mathbb{Z}$. Therefore, $H(Q) \neq 0$ and

$$2h_x(Q) \ll H(Q).$$

Since $H(Q) \leq 2Cy^{2/r}$ the number of such Q is $O(y)$ by Lemma 3. Since each Q gives rise to only $O(y^{2/r})$ primes dividing the denominator of Q, the total number of prime factors satisfying $|\Gamma_p| < y$ is $O(y^{1+2/r})$, as desired.

7. Primitive roots

We are now ready to prove Theorem 1. Consider the primes enumerated by Theorem 4* with u and v chosen so that $p \equiv u \pmod{v}$ implies each of a, b, c is a quadratic non-residue $(\mathrm{mod}\, p)$. This can be done because

$$\sum_{p \leq x}\left\{1 - \left(\frac{-3}{p}\right)\right\}\left\{1 - \left(\frac{a}{p}\right)\right\}\left\{1 - \left(\frac{b}{p}\right)\right\}\left\{1 - \left(\frac{c}{p}\right)\right\}$$

is asymptotic to $\pi(x)$ as $x \to \infty$, in view of the conditions imposed on a, b and c. Let us fix y and let

$$N = \prod_{p \leq y} p.$$

With $u \pmod{v}$ and N as above and $z = x^{\epsilon/3}$ we consider the primes enumerated by Theorem 4*. If p is one of these primes, then two cases arise: $p - 1 = 2^e mq$ or $p - 1 = 2^e mq_1q_2$, with q, q_1, q_2 primes satisfying the various conditions of Theorem 4*. If q divides the index of $\langle a\rangle, \langle b\rangle, \langle c\rangle$ $(\mathrm{mod}\, p)$ then by Lemma 8 the number of such primes is $O(x^{2\epsilon})$. If q_1 or q_2 divides the index of $\langle a, b, c\rangle$ $(\mathrm{mod}\, p)$ again by Lemma 8 (and $r = 3$) the number of such primes is $O(x^{1-\epsilon'})$. Hence the order of $\langle a, b, c\rangle$ $(\mathrm{mod}\, p)$ is divisible by q in the first case and q_1q_2 in the second case. Also 2^e divides the order of each of a, b, c $(\mathrm{mod}\, p)$ because none of a, b, c is a quadratic residue $(\mathrm{mod}\, p)$. Suppose in the second case each of the orders of a, b, c $(\mathrm{mod}\, p)$ is not divisible by q_1. Then the subgroup generated by a, b, c

$(\mathrm{mod}\, p)$ has order $< x^{3/4-\epsilon}$, and by Lemma 8 (and $r = 3$) the number of such primes is $O(x^{1-\epsilon})$. So we may suppose that one of the orders of a, b, c is divisible by q_1. Suppose without loss of generality that the order of a $(\mathrm{mod}\, p)$ is divisible by q_1. If $q_2 \mid [\mathbb{F}_p^* : \langle a \rangle]$ then, noting that $q_1 < x^{1/2-\delta}$ and again applying Lemma 8 with $r = 1$, we deduce that the number of such primes is $O(x^{1-2\delta})$. Thus we have

$$\geq \frac{c_1 \phi(N) x \log z}{N \log^2 x}$$

primes $p \leq x$ such that if $l \mid [\mathbb{F}_p^* : \langle a \rangle]$ then $l \mid m$, where $(m, N) = 1$ as in Theorem 4*. Now we invoke Lemma 5. The number of primes $p \leq x$ such that $l \mid [\mathbb{F}_p^* : \langle a \rangle]$ is

$$\frac{\mathrm{li}\, x}{l(l-1)} + O(x^{1-\epsilon}).$$

We sum this in the range $y < l < x^{\epsilon/3}$. This gives an estimate of

$$\ll \frac{\mathrm{li}\, x}{y} + O(x^{1-\epsilon}).$$

Since

$$\frac{\phi(N)}{N} = \prod_{p \leq y} \left(1 - \frac{1}{p}\right) \sim \frac{e^{-\gamma}}{\log y}$$

by Mertens' theorem, we can choose y sufficiently large so that

$$\frac{c_1 \epsilon e^{-\gamma}}{3 \log y} \gg \frac{1}{y}.$$

This completes the proof of Theorem 1.

8. Cyclicity of $E(\mathbb{F}_p)$

We now prove Theorem 2 and proceed as in [3] with minor variations. Let us observe that if $E(\mathbb{F}_p)$ contains a subgroup of type (q, q) then $q | p - 1$. This is because the field obtained by adjoining the q-division points of E to $\mathbb{Q}$ contains the cyclotomic field of the q-th roots of unity, by the theory of the Weil pairing. Moreover, the condition that $E(\mathbb{F}_p)$ contains a subgroup of type (q, q) is equivalent to the condition that p splits completely in $\mathbb{Q}(E[q])$. Now fix y, and set

$$N = \prod_{p \leq y} p$$

and $z = x^{\epsilon/3}$. Apply Theorem 4* and partition each of the primes enumerated into disjoint sets S_a according to the value of

$$a_p(E) = p + 1 - \#E(\mathbb{F}_p).$$

In each S_a we count the number of primes p such that $E(\mathbb{F}_p)$ is not cyclic. If, for a prime $q > x^{1/4+\epsilon}$, $E(\mathbb{F}_p)$ contains a (q,q) group then q is uniquely determined, for otherwise the size of $E(\mathbb{F}_p)$ would be greater than $x^{1+2\epsilon}$. In addition $p \equiv a-1 \pmod{q^2}$. By Hasse's inequality $|a_p| \leq 2\sqrt{p}$ and so we can never have $p = a-1$. Thus, the number of such primes is

$$\ll \frac{x}{q^2} \ll x^{\frac{1}{2}-2\epsilon}.$$

Summing this over $|a| \leq 2\sqrt{x}$ gives a total estimate of $O\big(x^{1-2\epsilon}\big)$ for the number of such primes enumerated by Theorem 4*. After eliminating these primes from our enumeration we infer that if $E(\mathbb{F}_p)$ is not cyclic then p splits completely in some $\mathbb{Q}\big(E[l]\big)$ with $l \leq x^{\epsilon/3}$ and $(l,N)=1$. By Lemma 6, the number of such primes on the quasi-Riemann hypothesis is

$$\ll \frac{\operatorname{li} x}{l^4} + O\big(x^{1-\epsilon}\big)$$

and we sum this over $y < l < x^{\epsilon/3}$ to deduce an estimate of

$$\ll \frac{\operatorname{li} x}{y}$$

such primes. Again, choosing y sufficiently large ensures that we have a positive density of primes for which $E(\mathbb{F}_p)$ is cyclic.

9. Primitive points on elliptic curves

We use Theorem 5 with $z=1$ and $N=1$. Let p be a prime enumerated by Theorem 5. Suppose first that $p+1 = 2^e p_1$. Then, $(\mathrm{mod}\, p)$, each one of $P_1, \ldots, P_6$ has order dividing $2^e p_1$. If the order divides 2^e, then p divides the 2^e-division polynomial evaluated at each of the P_i. Since e is bounded, there are only finitely many such p. So for p sufficiently large, the order divides p_1 and so the index is bounded by 2^e in this case.

Now suppose $p+1 = 2^e p_1 p_2$ with $p^\alpha < p_1 < p_2$. If the theorem is false then for all p sufficiently large enumerated by Lemma 1 we must have that the order of each P_i divisible by p_1 or p_2 but not both. If the orders are all divisible by p_2, then the subgroup generated by $P_1, \ldots, P_6 \pmod{p}$ has size $\leq 4p_2 \leq 4p^{1-\alpha}$. By Lemma 4, the number of such primes $p \leq x$ is $O\big(x^{4(1-\alpha)/3}\big)$. Since $\alpha > 1/4$, the number of such primes is $o\big(x/\log^2 x\big)$. By the same reasoning, we conclude that the number of primes for which all the orders are divisible by p_1 is also negligible. Hence, for at least $\gg x/\log^2 x$ primes enumerated by $\mathcal{A}$, the order of each P_i is divisible by p_1 or p_2 and both possibilities occur. Take an element P_1 (say) whose order $(\mathrm{mod}\, p)$

is divisible by p_1. If $p_1 < x^{1/3-\epsilon}$ then an application of Lemma 4 with $r = 1$ shows the number of such primes is $O(x^{1-\epsilon})$. So we may suppose $p_1 > x^{1/3-\epsilon}$. We can in fact suppose $p_1 > x^{1/3+\epsilon}$ because by Lemma 2 the number of primes $p \leq x$ such that $p + 1 = 2^e p_1 p_2$ with

$$x^{\frac{1}{3}-\epsilon} < p_1 < x^{\frac{1}{3}+\epsilon} \quad \text{and} \quad p_2 > x^{\frac{1}{2}-\delta}$$

for some $\delta > 0$ is, by Lemma 2,

$$\ll \frac{x}{p_1 \log^2 x}.$$

Summing this over the range $x^{1/3-\epsilon} < p_1 < x^{1/3+\epsilon}$ gives a contribution of $o(\epsilon x/\log^2 x)$, which is negligible for sufficiently small ϵ. So we may suppose that

$$x^{\frac{1}{3}+\epsilon} < p_1 < p_2.$$

Let us say that p in $\mathcal{A}$ has type (s_1, s_2) if s_1 of $P_1, \ldots, P_6$ have order divisible by p_1 and s_2 have order divisible by p_2. Then we can partition $\mathcal{A}$ according to five types: (1,5), (2,4), (3,3), (4,2), and (5,1).

We now consider each of the five types. If the type of p is (1,5) then five independent points generate a group (mod p) of order $O(p_2) = O(x^{2/3-\epsilon})$, and by Lemma 4 the number of such primes is $O(x^{14/15-\epsilon})$. If the type is (2,4) then four independent points generate a group of order $O(p_2) = O(x^{2/3-\epsilon})$ and again by Lemma 4 the number of such primes is $O(x^{1-\epsilon})$. If the type is (3,3), we have three independent points generating a group of order $p_1 < x^{1/2}$ and by Lemma 4 the number of such primes is $O(x^{5/6})$. The remaining two cases are similarly handled. This completes the proof.

Remark. It is clear that if we use Theorem 5 with $z = x^\epsilon$ and invoke Lemma 7 with a quasi-Riemann hypothesis, the assertion made in Theorem 3 holds for a positive density of primes.

10. Numerical examples

In [18], Quer produces three elliptic curves with complex multiplication such that the $\mathbb{Z}$ rank of the group of rational points is 12. More precisely, let

$$\begin{aligned} D_1 &= -408\,368\,221\,541\,174\,183 \\ D_2 &= -3\,082\,320\,147\,153\,282\,331 \\ D_3 &= -3\,161\,659\,186\,633\,662\,283 \end{aligned}$$

and put

$$E_i: \qquad Y^2 = X^3 + 16D_i$$

for $i = 1, 2, 3$. Then, $\operatorname{rank}_{\mathbb{Z}} E_i(\mathbb{Q}) = 12$. Quer also gives explicit generators. It is remarkable that these generators all have integral co-ordinates.

References

1 E. Bombieri, J.B. Friedlander, and H. Iwaniec: Primes in arithmetic progressions to large moduli. *Acta Math.* **370** (1986), 203–251.

2 R. Gupta and M. Ram Murty: A remark on Artin's conjecture. *Invent. Math.* **78** (1984), 127–130.

3 R. Gupta and M. Ram Murty: Cyclicity and generation of points (mod p) on elliptic curves. *Invent. Math.* **101** (1990), 225–235.

4 R. Gupta and M. Ram Murty: Primitive points on elliptic curves. *Compositio Math.* **58** (1986), 13-44.

5 R. Gupta, M. Ram Murty and V. Kumar Murty: The Euclidean algorithm for S-integers. In *Number Theory*, 189–201 (H. Kisilevsky and J. Labute, eds.). (Canadian Mathematical Society Conference Proceedings **7**) (1987).

6 D.R. Heath-Brown: Artin's conjecture for primitive roots. *Quart. J. Math. Oxford* (2) **37** (1986), 27–38.

7 H. Halberstam and H.-E. Richert: *Sieve Methods.* Academic Press (1974).

8 C. Hooley: On Artin's conjecture. *J. Reine Angew. Math.* **225** (1967), 209–220.

9 C. Hooley: *Applications of Sieve Methods.* Cambridge University Press (1976).

10 H. Iwaniec: Rosser's sieve. *Acta Arith.* **36** (1980), 171–202.

11 H. Iwaniec: A new form of the error term in the linear sieve. *Acta Arith.* **37** (1980), 307–320.

12 J. Lagarias and A. Odlyzko: Effective versions of the Chebotarev density theorem. In *Algebraic Number Fields*, 409–464 (A. Fröhlich, ed.). Academic Press (1977).

13 S. Lang and H. Trotter: Primitive points on elliptic curves. *Bull. Amer. Math. Soc.* **83** (1977), 289–292.

14 J.-F. Mestre: Rang de courbes elliptiques d'invariant donné. *C.R. Acad. Sci. Paris* **314** (1992), 919–922.

15 M. Ram Murty, V. Kumar Murty and N. Saradha: Modular forms and the Chebotarev density theorem. *Amer. J. Math.* **110** (1988), 253–281.

16 C.-D. Pan: A new mean value theorem and its applications. In *Recent Progress in Analytic Number Theory* Vol. 1, 275–287. (H. Halberstam and C. Hooley, eds.). Academic Press (1981).

17 F. Pappalardi: On Artin's conjecture for primitive roots (Ph.D. thesis). McGill University (1993).

18 J. Quer: Corps quadratiques de 3-rang 6 et courbes elliptiques de rang 12. *C.R. Acad. Sci. Paris* **305** (1987), 215–218.

19 M. Ram Murty: On Artin's conjecture. *J. Number Theory* **16** (1983), 147–168.

20 M. Ram Murty: An analogue of Artin's conjecture for abelian extensions. *J. Number Theory* **18** (1984), 241–248.

21 J.-P. Serre: Résumé des cours de 1977-78. *Annuaire du Collège de France* (1978), 67–70 (in Collected Papers, Vol. 3, 465–468 and 713).

22 J.-P. Serre: Quelques applications du théorème de densité de Chebotarev. Publ. I.H.E.S. no. 54 (1981), 123–201.

23 A. Walfisz: Über Gitterpunkte in mehrdimensionalen Ellipsoiden III. *Math. Zeit.* **27** (1927), 245–268.