NOAM D. ELKIES

Distribution of supersingular primes

Astérisque, tome 198-199-200 (1991), p. 127-132
<http://www.numdam.org/item?id=AST_1991__198-199-200__127_0>

Distribution of supersingular primes

Noam D. Elkies

Let E be a fixed elliptic curve over $\mathbf{Q}$ without complex multiplication, and let j_E be its j-invariant. A *supersingular prime* for E is a rational prime p such that (i) E has good reduction mod p, and (ii) the reduced curve $E_p = E \bmod p$ is supersingular; observe that condition (i) excludes only finitely many primes (those dividing the discriminant of E), and condition (ii) depends only on j_E. Following [7] we define $\pi_0(x)$ to be the number of supersingular $p < x$, and ask for the asymptotic behavior of $\pi_0(x)$ as $x \longrightarrow \infty$. A naïve heuristic suggests that, since (for $p \geq 5$) E_p is supersingular if and only if it has $p+1$ points over $\mathbf{F}_p$, while in general its number of $\mathbf{F}_p$-points could differ from $p+1$ by as much as $\pm 2p^{1/2}$, each p is supersingular with "probability" roughly $p^{-1/2}$, and so (summing over $p < x$) the expected value of $\pi_0(x)$ should be roughly $x^{1/2}/\log x$. Refinements of this heuristic, together with numerical evidence gathered for several curves E, led Lang and Trotter to make the

CONJECTURE[7]: *$\pi_0(x) = (C + o(1))x^{1/2}/\log x$, for some explicit $C > 0$ depending on j_E.*

But it is not even immediately obvious that either $\pi_0(x) = o(\pi(x))$ (that is, that the supersingular primes have density zero) or that $\pi_0(x) \neq O(1)$ (i.e. that there are infinitely many such primes). The former was proved by Serre in 1968 [8] by applying the Čebotarev Density Theorem to the number fields generated by the coordinates of the torsion points of E; later [9] he combined this idea with sieve techniques to obtain the upper bound

$\pi_0(x) \ll x/\log^{3/2-\epsilon}$ (the exponent $3/2-\epsilon$ was recently improved by D. Wan [10] to $2-\epsilon$), and further proved that under the Generalized Riemann Hypothesis (GRH) for these number fields the same method would yield $\pi_0(x) \ll x^{3/4}$. The infinitude of supersingular primes was proved by me in 1986, and generalized in my thesis to curves defined over an arbitrary number field with a real embedding [2, 3]. The main purpose of this report is to describe recent progress on an upper bound for $\pi_0(x)$. We start, however, with a few remarks on the lower bounds that can be obtained from the methods of [2], both to put the upper bounds in context and to introduce some ideas that also figure prominently in these new upper bounds.

For positive $D \equiv 0$ or $3 \bmod 4$, let $P_D(X)$ be the minimal polynomial of the algebraic integer $j((D+\sqrt{-D})/2)$. In [2] it was shown that, if $\{p_1, p_2, \ldots, p_n\}$ is a finite set of primes containing all of E's primes of bad reduction, and $l \equiv 3 \bmod 4$ a sufficiently large prime of which all the p_i are quadratic residues (the existence of such l is guaranteed by Dirichlet's theorem on primes in arithmetic progressions), then one of $P_l(j_E)$ and $P_{4l}(j_E)$ is divisible by a prime p_{n+1}, distinct from each of $p_1, \ldots, p_n$, which is a new supersingular prime for E. Iterating this procedure we not only obtain the infinitude of supersingular primes, but also an implicit upper bound on p_n, and thus equivalently a lower bound on $\pi_0(x)$: Dirichlet's theorem gives an effective bound on the least admissible l, and the absolute value of the numerator of $P_D(j_E)$ (and thus also its factor p_{n+1}) is easily bounded above by $O(\exp C \cdot D^{1/2} \log^2 D)$. Unfortunately this bound on p_n is astronomical—an n-fold iterated exponential!—unless we assume the GRH for real Dirichlet characters. Applying the standard explicit formulas for the number of primes in an arithmetic progression, we then find that $\pi_0(x) \gg \log\log\log x$; this bound, since independently discovered by Brown [1], has been improved by R. Murty to $\pi_0(x) \gg (\log\log x)^{1/2}$. A better method is to assume that the $p_i (1 \le i \le n)$ already comprise all the supersingular primes less than x, and then use not only the first but all admissible primes $l \ll x^{1/2}$, obtaining many new supersingular primes between x and $x' \ll \exp(Cx^{1/4}\log^2 x)$, all distinct by [4]. Assuming again the GRH, we find that either $\pi_0(x) \gg \log x$ or there are enough admissible $l \ll x^{1/2}$ to ensure $\pi_0(x') \gg \log x'$; either way we obtain the bound (Theorem 2 in my thesis):

THEOREM A: *Under GRH for real Dirichlet characters,* $\pi_0(x) \gg \log\log x$.

It occurred to me in 1987 that these ideas might be useful for getting an upper bound on $\pi_0(x)$; one version of this idea, mentioned in my thesis, is the

OBSERVATION (with R. Murty): *If, for some positive θ, each supersingular prime p of E divides $P_D(j_E)$ for some $D \ll p^\theta$, then* $\pi_0(x) \ll x^{3\theta/2}\log x$.

Indeed, by the above estimate on the size of $P_D(j_E)$, the product of all of E's supersingular primes less than x would divide the product of the numerators of $P_D(j_E)$ over $D \ll x^\theta$, which is bounded by

$$\prod_{D \ll x^\theta} \exp(C \cdot D^{1/2}\log^2 D) \ll \exp O(x^{3\theta/2}\log^2 x);$$

so the sum of these primes' logarithms would be $\ll x^{3\theta/2}\log^2 x$, and their number $O(x^{3\theta/2}\log x)$. [Several remarks are in order here: First, that for this Observation to be of any use we must have θ strictly less than $2/3$; second, that this proof fails only when E has complex multiplication, because that's exactly when one of the $P_D(j_E)$ vanishes (and fail it must in that case, since for a CM curve $\pi_0(x) \sim \pi(x)/2$); third, that the bound $\pi_0(x) \ll x^{3\theta/2}\log x$ would be unconditional, not depending on GRH or other unproved hypotheses, provided the same was true of the proof of $D \ll p^\theta$; and last, that we can save a factor of $\log x$ by more carefully estimating the size of $\prod_{D \ll x^\theta} P_D(j_E)$, obtaining $D \ll p^\theta \Rightarrow \pi_0(x) \ll x^{3\theta/2}$.]

Thus the problem of estimating θ, which I raised in [2] in the context of computing large supersingular primes, assumes a new theoretical significance. Now p divides $P_D(j_E)$ if and only if the supersingular curve E_p has complex multiplication by $(D+\sqrt{-D})/2$, that is, if the quadratic order $\mathbf{Z}[\frac{1}{2}(D+\sqrt{-D})]$ imbeds into the endomorphism ring A of E_p, or equivalently if A contains an endomorphism α whose discriminant $(\alpha-\bar{\alpha})^2 = \mathrm{Tr}^2(\alpha) - 4\deg(\alpha)$ is $-D$. Thus the least D such that p divides $P_D(j_E)$ is the smallest nonzero value attained by the positive-definite quadratic form $(4\deg - \mathrm{Tr}^2)$ on the rank-3 lattice $A_1 = A/\mathbf{Z}$. In [2] I used a simple geometry-of-numbers argument to estimate this value: A_1 has covolume $2p$ (this follows from Deuring's theorem that A has reduced discriminant p), so it must contain a nonzero vector of norm at most $2p^{2/3}$. Unfortunately this gives only $\theta = 2/3$, the smallest useless value of θ.

But computations suggested that this bound might not be best possible. Indeed, recently Kaneko obtained [6]:

THEOREM: *E_p has an endomorphism of discriminant $(-D)$ for some positive $D \leq 4\sqrt{p/3}$.*

Sketch of proof: Note that while in general a supersingular j-invariant in characteristic p need only lie in $\mathbf{F}_{p^2}$, the j-invariant of E_p is necessarily in $\mathbf{F}_p$ (though most of its endomorphisms can only be defined once we extend scalars to $\mathbf{F}_{p^2}$). Thus A contains a square root ϕ of $-p$, namely the Frobenius endomorphism. Kaneko now uses Ibukiyama's classification [5] of such quaternion algebras A to show that $A/\mathbf{Z}$ contains a rank-2 sublattice of determinant $4p$, whence the Theorem follows. This sublattice consists of the lattice vectors orthogonal to the image of the Frobenius endomorphism ϕ

in A_1. When Serre read this he remarked that the order of magnitude of the determinant of the sublattice, and thus the bound $D \ll \sqrt{p}$, could be easily obtained by "pure thought" without invoking the explicit classification in [5]: the Galois involution of $\mathbf{F}_{p^2}$ induces an involution ι of A (conjugation by ϕ) whose invariant subring A^+ is either $\mathbf{Z}[\phi]$ or possibly $\mathbf{Z}[\frac{1}{2}(1+\phi)]$ if $p \equiv 3 \bmod 4$; let $A^- \subset A$ be the anti-invariant sublattice $\{\alpha : \iota\alpha = -\alpha\}$ of rank 2. Then $A^+ \oplus A^-$ is of bounded index in A (the quotient is an elementary abelian 2-group of rank at most 4), so since A has determinant p^2 and A^+ has determinant at least p, the determinant of A^- with the quadratic form $\deg(\cdot)$ is $\ll p$. Also A^- is orthogonal to A^+ and so in particular to 1, whence any $\alpha \in A^-$ has trace zero and determinant $-4\deg(\alpha)$. Therefore the image of A^- in $A/\mathbf{Z}$ is again a rank-2 lattice of determinant $\ll p$ and we are done.

Either way we thus have $\theta = 1/2$ and conclude:

THEOREM B: $\pi_0(x) \ll x^{3/4}$.

Note that this is exactly the bound obtained by Serre under GRH; it is unclear what if any significance this coincidence has.

Details of the analytic estimates used in the proofs of Theorems A and B will appear elsewhere.

References

[1] Brown, M.L.: Note on supersingular primes of elliptic curves over $\mathbb{Q}$. *Bull. London Math. Soc.* **20** (1988), 293–296.

[2] Elkies, N.D.: The existence of infinitely many supersingular primes for every elliptic curve over $\mathbb{Q}$. *Invent. Math.* **89** (1987), 561–567.

[3] Elkies, N.D.: Supersingular primes for elliptic curves over real number fields. *Compositio Math.* **72** (1989), 165–172.

[4] Gross, B. H., Zagier, D.: On singular moduli, *Jour. für die reine und angew. Math.* **335** (1985), 191–220.

[5] Ibukiyama, T.: On maximal orders of division quaternion algebra of the rational number field with certain optimal embeddings. *Nagoya Math. J.* **88** (1982), 181–195.

[6] Kaneko, M.: Supersingular j-invariants as singular moduli mod p. *Osaka J. Math.* **26** (1989), 849–855.

[7] Lang, S., Trotter, H.: *Frobenius distributions in* GL_2-*extensions.* Lect. Notes Math. 504, 1976.

[8] Serre, J.-P.: *Abelian l-adic representations and elliptic curves.* New York: Benjamin 1968.

[9] Serre, J.-P.: Quelques applications du théorème de densité de Chebotarev. *IHES Publ. Math.* **54** (1981), 123–201.

[10] Wan, D.: On the Lang-Trotter Conjecture. *J. Number Th.* **35** (1990), 247–268.

Noam D. Elkies
Department of Mathematics
Harvard University
Cambridge, MA 02138 USA