BULLETIN (New Series) OF THE
AMERICAN MATHEMATICAL SOCIETY
Volume 46, Number 3, July 2009, Pages 485–487
S 0273-0979(09)01261-0
Article electronically published on April 13, 2009

SELECTED MATHEMATICAL REVIEWS

related to the paper in the previous section by
NICOLAS KATZ

MR0823264 (87h:11051) 11G05;11G40, 11R45

Murty, V. Kumar

Explicit formulae and the Lang-Trotter conjecture.

Number theory (Winnipeg, Man., 1983).

The Rocky Mountain Journal of Mathematics **15** (1985), *no.* 2, 535–551.

Let E be an elliptic curve defined over the rationals, and let $\pi_E(x)$ count the number of primes $p < x$ such that E_p, the reduction of $E \bmod p$, is supersingular, i.e. E_p has $p+1$ points over $\mathrm{GF}(p)$. M. Deuring [Nachr. Akad. Wiss. Göttingen Math.-Phys. Kl. II **1953**, 85–94; MR0061133 (15,779d); ibid. **1955**, 13–42; MR0070666 (17,17c); ibid. **1956**, 37–76; MR0079611 (18,113e); ibid. **1957**, 55–80; MR0089227 (19,637a)] showed that $\pi_E(x) \sim \frac{1}{2}\pi(x)$ if E has complex multiplication, where $\pi(x)$ is the number of primes $\le x$. For non-CM curves, S. Lang and H. F. Trotter [*Frobenius distributions in* GL_2*-extensions*, Lecture Notes in Math., 504, Springer, Berlin 1976; MR0568299 (58 #27900)] conjectured that $\pi_E(x) \sim c_E x^{1/2}/\log x$ where $c_E > 0$. J.-P. Serre [Inst. Hautes Études Sci. Publ. Math. No. 54 (1981), 323–401; MR0644559 (83k:12011)] proved for non-CM curves that $\pi_E(x) \le x/(\log x)^{5/4-\varepsilon}$ unconditionally, and that $\pi_E(x) \ll x^{3/4}$ assuming the Riemann hypothesis for all Artin L-functions. His proofs use an effective version of the Chebotarev density theorem due to the reviewer and A. M. Odlyzko [*Algebraic number fields*: *L-functions and Galois properties* (Durham, 1975), 409–464, Academic Press, London, 1977; MR0447191 (56 #5506)]. Let $p+1+a_p$ denote the number of points of E_p and set $a_p = 2p^{1/2}\cos\theta p$. Sato and Tate conjectured that for any interval I in $(0,2\pi)$, $\#\{p \le x : \theta p \in I\} \sim \mu_E(I)\pi(x)$ where μ_E is a certain specific measure. The author of this paper considers the L-functions defined by $L_k(s) = \prod_p \prod_{n=0}^{k}(1-\alpha_p^n \overline{\alpha}_p^{k-n} p^{-s})^{-1}$, where α_p, $\overline{\alpha}_p$ are the roots of $x^2 - a_p x + p = 0$. Under the assumptions that these L-functions analytically continue to $\mathbf{C}$, satisfy appropriate functional equations, and satisfy the analogue of the Riemann hypothesis, the author shows that the Sato-Tate conjecture follows in the form $\#\{p \le x : p \in I\} = \mu_E(I)\pi(x) + O(x^{1/2}(\log x)(\log Nx)f(x))$ where $f(x) \to \infty$ as $x \to \infty$ and $x > f^{-1}(1/\mu_E(I))$. This implies that $\pi_E(x) \le c_E^* x^{3/4}(\log x)$ in the non-CM case, and more generally that $\#\{p \le x; a_p = a\} \le cx^{3/4}\log x$, where c is a constant depending on E and a. The L-functions studied are attached to the symmetric powers $\mathrm{Sym}^k(\sigma_l)$ of a compatible system of l-adic representations σ_l attached to E. The methods involve proving an analogue of an effective Chebotarev density theorem for these L-functions.

{For the entire collection see MR0823239 (87a:11007)}

From MathSciNet, April 2009

J. C. Lagarias

MR0903384 (88i:11034) 11G05; 14G25

Elkies, Noam D.

The existence of infinitely many supersingular primes for every elliptic curve over Q.

Inventiones Mathematicae **89** (1987), *no.* 3, 561–567.

In this important paper, the author confirms one of the outstanding conjectures in the study of elliptic curves, namely that every curve defined over the field $\mathbf{Q}$ of rational numbers has infinitely many supersingular primes. Indeed he shows this for any elliptic curve defined over a number field of odd degree over $\mathbf{Q}$.

Suppose that E is an elliptic curve defined over $\mathbf{Q}$ which has good reduction at a prime p. Its reduction E_p mod p is supersingular if and only if its endomorphism ring contains an order O_D of discriminant $-D$ in an imaginary quadratic field in which p either ramifies or remains prime. Let P_D be the monic polynomial in x whose roots are all the j-invariants of the isomorphism classes of elliptic curves over $\overline{\mathbf{Q}}$ with complex multiplication by O_D. Let J denote the j-invariant of E. If p divides the numerator of $P_D(J)$, then by the Deuring lifting theorem, E_p has complex multiplication by $O_{D'}$ for some D' (perhaps differing from D by a square). If in addition $-D$ is not a p-adic square, then p is a supersingular prime. The author's main lemma shows that if l is a prime congruent to 3 mod 4, then modulo l, both P_l and P_{4l} factor as $(x-1728)$ times a square.

The proof of the theorem roughly parallels Euclid's demonstration of the infinitude of primes in $\mathbf{Z}$! Suppose that S is a finite set of primes containing all the primes at which E has bad or supersingular reduction. Let l be any prime congruent to 3 mod 4 not in S, such that p is a square mod l for all p in S, and sufficiently large so that $P_l(J)>0$ and $P_{4l}(J)<0$. Then $P_l(J)P_{4l}(J)$ is a negative rational number which is a perfect square modulo l (by the main lemma), and whose denominator is a perfect square (being the denominator of J to an even power). Hence the absolute value of its numerator is not a square modulo l (since -1 is not a square modulo l). But then the absolute value of the numerator must be divisible by a prime p which is either l or a quadratic nonresidue modulo l. Hence p is a supersingular prime which is not in S.

From MathSciNet, April 2009

David Grant

MR1677267 (2000g:11045) 11G05; 11F30, 11N36

David, Chantal; Pappalardi, Francesco

Average Frobenius distributions of elliptic curves.

International Mathematics Research Notices **1999**, *no.* 4, 165–183.

Let E be an elliptic curve defined over the rationals. For any prime p of good reduction, let $a_p(E)$ denote the trace of the Frobenius morphism of E mod p. For a fixed integer r, what can be said about the number $\pi_r(x)=\pi_r(x,E)$ of primes $p\le x$ such that $a_p(E)=r$? If $r=0$ and E has complex multiplication, then a classical theorem of Deuring says that the number of such primes $p\le x$ is $\sim x/2\log x$ as $x\to\infty$. If $r=0$ and E has no complex multiplication, then a theorem of N. D. Elkies [Invent. Math. **89** (1987), no. 3, 561–567; MR0903384 (88i:11034)] shows there are infinitely many such primes. Later, E. Fouvry and the reviewer [Canad. J. Math. **48** (1996), no. 1, 81–104; MR1382477 (97a:11084)] proved that for any $\epsilon > 0$, $\pi_0(x) \geq (\log\log\log x)^{1-\epsilon}$ for x sufficiently large and that $\pi_0(x) \gg \log\log x$ for infinitely many $x \to \infty$. Earlier, Elkies and the reviewer noted that the generalized Riemann hypothesis for classical Dirichlet L-functions implies that $\pi_0(x) > \log\log x$ for x sufficiently large and $\pi_0(x) > \log x$ for infinitely many $x \to \infty$. Unconditionally, they observed that $\pi_0(x) = O(x^{3/4})$ can be derived by using a result of M. Kaneko [Osaka J. Math. **26** (1989), no. 4, 849–855; MR1040429 (91c:11033); see also N. D. Elkies, Astérisque No. 198-200 (1991), 127–132 (1992); MR1144318 (93b:11070); M. R. Murty, in *Proceedings of the Ramanujan Centennial International Conference (Annamalainagar, 1987)*, 45–53, Ramanujan Math. Soc., Annamalainagar, 1988; MR0993343 (90f:11036)]. S. Lang and H. Trotter [*Frobenius distributions in* GL_2*-extensions*, Lecture Notes in Math., 504, Springer, Berlin, 1976; MR0568299 (58 #27900)] conjectured that if E has no complex multiplication, then $\pi_0(x) \sim C\sqrt{x}/\log x$ for some positive constant C, as $x \to \infty$. More generally, Lang and Trotter conjectured that for $r \neq 0$, and E any elliptic curve over Q, $\pi_r(x) \sim C_{E,r}\sqrt{x}/\log x$ for some suitable constant $C_{E,r}$. If proved, this conjecture also implies the classical conjecture of Hardy and Littlewood that there are infinitely many primes of the form n^2+1.

In the paper of Fouvry and the reviewer [op. cit.], the average of $\pi_0(x,E)$ is studied as E varies over a family of elliptic curves $y^2 = x^3 + ax + b$. The authors of the paper under review extend these results for $r \neq 0$ and study $\pi_r(x,E)$ as E varies. More precisely, let $\pi_r(x;a,b)$ denote the number of primes $p \leq x$ such that $a_p(E) = r$ for the curve $E\colon Y^2 = X^3 + aX + b$. The main theorem of the paper is that for $c > 0$,

$$\frac{1}{4AB}\sum_{|a|\leq A, |b|\leq B} \pi_r(x;a,b) = C_r\frac{\sqrt{x}}{\log x} + O\left((1/A+1/B)x^{3/2} + \frac{x^{5/2}}{AB} + \frac{\sqrt{x}}{\log^c x}\right)$$

where (for p denoting a prime number) we have

$$C_r = \frac{2}{\pi}\prod_{p|r}\left(1-\frac{1}{p^2}\right)^{-1}\prod_{(p,r)=1}\frac{p(p^2-p-1)}{(p-1)(p^2-1)}.$$

Thus, the Lang-Trotter conjecture holds "on average". The techniques of Fouvry and the reviewer do not extend automatically to the case $r \neq 0$ and the authors must circumvent this by a clever application of a classical theorem of Barban, Davenport and Halberstam.

From MathSciNet, April 2009

M. Ram Murty