From: Proceedings of the Ramanujan Centennial International Conference, 1 (1988) 45-53

RECENT DEVELOPMENTS IN ELLIPTIC CURVES

M. Ram Murty

Dedicated to the memory of Srinivasa Ramanujan

I will begin with a discussion of some ancient problems in mathematics:

Problem 1. Is there always a prime number between two consecutive squares: $n^2 < p < (n+1)^2$?

Problem 2. Are there infinitely many primes p of the form n^2+1 ?

Problem 3. For $n \geq 3$, does the equation $x^n + y^n = z^n$ with $x, y, z, \in \mathbf{Z}$ imply that $xyz = 0$?

The complete solution to all of these problems is unknown at present. The surprising thing is that all of these problems have connection with the theory of elliptic curves. The profound connection relating Fermat's Last Theorem (Problem 3) to the Taniyama conjecture that every elliptic curve is modular, was made by Gerhard Frey and we have heard in his talk the beautiful ideas that have opened up a tantalizing avenue of research.

It is unknown at present whether there is always a prime number between two consecutive square numbers. It is known by methods of analytic number theory that there is always a prime number between two consecutive cubes. In the case of Problem 1, it is not difficult to show that it is equivalent to showing that for every prime p, the existence of some elliptic curve E defined over $\mathbf{F}_p$ such that $|E(\mathbf{F}_p)|$ is a prime number. Indeed, a theorem of Deuring states that for every integer t satisfying $|t| \leq 2\sqrt{p}$, there is an elliptic curve E over $\mathbf{F}_p$ such that $|E(\mathbf{F}_p)| = p+1-t$. Utilising this fact, the equivalence is easily established.

This lecture is concerned about Problem 2. Consider the elliptic curve

$$E: \qquad y^2 = x^3 - x.$$

This curve has good reduction outside of 2 and so for $p > 2$ it makes sense to consider the curve (mod p). Let $p+1-a_p$ denote the number of points of E (mod p). The number a_p satisfies the inequality

$$|a_p| \leq 2\sqrt{p}.$$

One can show that for this curve if $a_p = 2$ infinitely often then, $p = n^2+1$. The converse is almost correct, but not quite. If $p = n^2+1$, then $a_p = \pm 2$. These are part of general conjectures of Lang and Trotter [3]. Let E be an elliptic curve defined over $\mathbf{Q}$ and let $p+1-a_p$ be the number of points of E (mod p). Lang and Trotter [3] conjecture that the number of primes p such that $a_p = a$ for any given value of a satisfies an asymptotic law of the form

$$\#\{p \leq x: \quad a_p = a\} \sim C_E x^{1/2}/\log x,$$

as $x \to \infty$. (The only case ruled out from this conjectural law is when E has complex mutliplication and $a = 0$. In this case, it is a classical theorem of Deuring that $a_p = 0$ for

roughly half of the primes.) In the case that the curve has complex multiplication, one can relate these conjectures to the distribution of primes in quadratic progressions and are consistent with conjectures made by Hardy and Littlewood. But if E has no complex multiplications, then these are new conjectures and nothing was known about them until recently.

For example, are there infinitely many primes such that $a_p = 0$ for curves without complex multiplication ? This question was answered very recently by Noam Elkies [2]. Let E be an elliptic curve defined over $\mathbf{Q}$. Elkies [2] has recently proved that E has infinitely many primes of supersingular reduction. One can show that this is equivalent to $a_p = 0$ for curves defined over $\mathbf{Q}$. His proof is ingenious and simple. His proof, though, does not give an effective lower bound for the number of such primes. The method of [2] only yields a slowly growing recursive function. The purpose of this lecture is to obtain an effective lower bound for the number of such primes assuming the generalised Riemann hypothesis (GRH). The assumption of the GRH seems indispensible to obtaining some quantitative result. We approach nowhere near the conjectured law of Lang and Trotter. The method is the same as Elkies [2] except in the last stages where we invoke the generalised Riemann hypothesis and estimates from the theory of the Epstein zeta function.

More precisely, let K denote a quadratic extension of $\mathbf{Q}$ and denote by $\zeta_K(s)$ the Dedekind zeta function of K. Let $\pi_0(x)$ denote the number of primes $p \leq x$ for which the curve E has supersingular reduction.

We prove:

Theorem Suppose that for every quadratic extension K of $\mathbf{Q}$, $\zeta_K(s)$ satisfies the Riemann hypothesis. Then,

$$\pi_0(x) \geq (\log\log x)^{1/2}.$$

The proof of Elkies [2] was based on a criterion of Deuring [1]. Let p be a prime at which E has good reduction and let E_p be the reduction of $E \pmod{p}$. Then the criterion of Deuring states that E_p is supersingular if and only if it has complex multiplication by an order in an imaginary quadratic extension of $\mathbf{Q}$ in which p is ramified or inert. As was noted in [2], E_p will have complex multiplication by some order if its j-invariant is the invariant of an ideal in that order.

Therefore, given any order $\mathcal{O}$, we associate the modular polynomial

$$P_{\mathcal{O}}(X) = \prod_{\mathcal{A} \in]\updownarrow(\mathcal{O})} (X - j(\mathcal{A})),$$

where $j(\mathcal{A})$ denotes the j-invariant attached to the elliptic curve $\mathbb{C}/\mathcal{A}$ and the product is over representatives of proper ideal classes of the class group of $\mathcal{O}$, denoted $cl(\mathcal{O})$. As the j-invariant is a class invariant, the product is independent of the choice of representatives. It is classical that $P_{\mathcal{O}}(X) \in \mathbb{Z}[X]$ of degree $h(\mathcal{O})$, the class number of $\mathcal{O}$.

As in [2], let $P_D(X)$ be the polynomial attached to the order

$$\mathbf{Z}[\frac{\mathbf{D}+\sqrt{-\mathbf{D}}}{\mathbf{2}}].$$

Denote the j-invariant of E by J. Then E_p has complex multiplication by the order of discriminant $-D$ if

$$P_D(J) \equiv 0 \pmod{p}.$$

If in addition, $\left(\frac{-D}{p}\right) \neq 1$, then p will be a supersingular prime for E.

We need the following lemmas:

Lemma 1 Let ℓ be a prime congruent to 3 (mod 4). Then

$$P_\ell(X) \equiv (X-1728)R_\ell(X)^2 \pmod{\ell}$$

and

$$P_{4\ell}(X) \equiv (X-1728)Q_\ell(X)^2 \pmod{\ell},$$

where R_ℓ and Q_ℓ are certain polynomials.

Proof See [2].

Lemma 2 Let $h(\mathcal{O})$ be odd and $a \in \mathbb{R}$. Then $P_{\mathcal{O}}(a) > 0$ if and only if $a > j(\mathcal{O})$.

Proof By theory of complex multiplication, we know that

$$j(\mathcal{A}^{-1}) = \overline{j(\mathcal{A})},$$

so that we can pair up the proper ideal classes $\mathcal{A} \neq \mathcal{O}$ to deduce that the sign of $P_{\mathcal{O}}(a)$ is determined by the factor corresponding to the principal class. Thus, $P_{\mathcal{O}}(a) > 0$ if and only if $a > j(\mathcal{O})$. This proves the lemma.

We recall a few properties of the j-function. The j-function has a Fourier expansion:

$$j(z) = e^{-2\pi iz} + 744 + \sum_{n=1}^{\infty} c_n e^{2\pi inz}$$

where the coefficients c_n are natural numbers. Indeed, by the theory of modular forms, one can show that

$$j(z) = \frac{\{1+240\sum_{n=1}^{\infty}(\sum_{d|n} d^3)e^{2\pi inz}\}^3}{e^{2\pi iz}\prod_{n=1}^{\infty}(1-e^{2\pi inz})^{24}},$$

from which the positivity of the coefficients is easily deduced. Therefore,

$$j(iy) \geq e^{2\pi y}. \tag{1}$$

Lemma 3 If

$$\ell > \left(\frac{\log(|J|+745)}{\pi}\right)^2$$

then

$$P_\ell(J)P_{4\ell}(J) < 0.$$

Proof From lemma 2, we know that $P_{4\ell}(J) < 0$ if

$$J < j(2\ell + \sqrt{-\ell}) = j(\sqrt{-\ell}).$$

Hence, by (1), it follows that $P_{4\ell}(J) < 0$ if $J < e^{2\pi\sqrt{\ell}}$. This proves, that if

$$\ell > \left(\frac{\log|J|}{2\pi}\right)^2,$$

then $P_{4\ell}(J) < 0$. To complete the proof, we must show that $P_\ell(J) > 0$ if ℓ satisfies the lower bound specified in the lemma. Indeed, since

$$c_n e^{-2\pi n y} = \int_0^1 j(x+iy)e^{-2\pi i n x}dx,$$

we deduce that for any $y > 0$,

$$c_n e^{-2\pi n y} \leq \max_{0\leq x\leq 1} |j(x+iy)| \leq j(iy).$$

It is classical [7] that $j(i) = 1728$, so that from the above, we obtain the inequality

$$c_n \leq 1728e^{2\pi n}.$$

(We remark that sharper inequalities for c_n can be derived, but they are not essential to our purpose.) Hence, if $y \geq 3$,

(†) $$|j(x+iy)| \leq e^{-2\pi y} + 745.$$

By lemma 2, $P_\ell(J) > 0$ if

$$J > j(\frac{\ell+\sqrt{-\ell}}{2}).$$

Thus, we need:

$$J > -e^{\pi\sqrt{\ell}} + 744 + \sum_{n=1}^{\infty}(-1)^n c_n e^{-\pi n\sqrt{\ell}}.$$

Utilising the above bound for c_n, we easily see that if

$$J > -e^{\pi\sqrt{\ell}} + 745,$$

then $P_\ell(J) > 0$. Thus, if

$$\ell > \left(\frac{\log(|J| + 745)}{\pi}\right)^2,$$

the desired inequality is satisfied. This completes the proof of the lemma.

The ineffective versions of the above lemmas are contained in Elkies [2]. The lemmas below are the new ideas we need to obtain an effective lower bound.

Lemma 4 Let $p_1, p_2, ..., p_k$ be given prime numbers. For each quadratic extension K of $\mathbf{Q}$, suppose that $\zeta_K(s)$ satisfies the Riemann hypothesis. Then, the smallest prime $\ell \equiv 3 \pmod 4$ such that

$$(*) \qquad \left(\frac{p_i}{\ell}\right) = 1, \quad 1 \le i \le k,$$

satisfies

$$\ell \le c2^{2k}\left(\sum_{i=1}^{k} \log p_i\right)^2,$$

for some absolute constant c.

Proof The number of primes $\ell \le y, \quad \ell \equiv 3 \pmod 4$, such that $(*)$ is satisfied is clearly

$$(2) \qquad \sum_{\ell \le y} \frac{1}{2^{k+1}}\left(1 + \left(\frac{-1}{\ell}\right)\right) \prod_{i=1}^{k}\left(1 + \left(\frac{p_i}{\ell}\right)\right).$$

On the Riemann hypothesis, it is known [6] that

$$\sum_{\ell \le y}\left(\frac{d}{\ell}\right) = O(y^{\frac{1}{2}} \log dy),$$

where the above constant implied by the O symbol is absolute. Therefore, if we expand the product in (2), we obtain

$$(3) \qquad \frac{\pi(y)}{2^{k+1}} + O(y^{\frac{1}{2}} \log dy),$$

where $\pi(y)$ denotes the number of primes $\ell \le y$ and $d = p_1 p_2 \cdots p_k$. Hence, if c is a sufficently large constant, and

$$y = c2^{2k}\left(\sum_{i=1}^{k} \log p_i\right)^2,$$

then we see that the term in (3) is strictly positive. Therefore, the smallest ℓ satisfying $(*)$ satisfies the inequality

$$\ell \leq c2^{2k}\left(\sum_{i=1}^{k}\log p_i\right)^2,$$

as desired.

Let $\mathcal{A}_\infty, ..., \mathcal{A}_\wr$ be the inequivalent ideal classes of the order

$$\mathbb{Z}[\frac{\ell+\sqrt{-\ell}}{2}],$$

where $h = h(-\ell)$ is the class number of the order. Then, it is classical that to each $\mathcal{A}_\rangle$ we can associate a binary quadratic form

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

with

$$b_i^2 - 4a_i c_i = -\ell, \quad c_i \geq a_i \geq |b_i|.$$

It follows that $a_i \leq \sqrt{\ell/3}$. Moreover,

$$j(\mathcal{A}_\rangle) = |(\frac{-\lfloor_\rangle + \sqrt{-\ell}}{\in\dashv_\rangle}).$$

We will need the following estimate:

Lemma 5

$$|P_\ell(J)| \leq 2^h \exp\big(C\sqrt{\ell}\sum_{i=1}^{h}\frac{1}{a_i}\big)$$

where $C = \log(|J| + 745)$.

Proof Clearly, from the preceding discussion,

$$|P_\ell(J)| \leq \prod_{i=1}^{h}(|J| + |j(\frac{-b_i+\sqrt{-\ell}}{2a_i})|).$$

Now, from (†), we have that

$$|j(\frac{-b_i+\sqrt{-\ell}}{2a_i})| \leq \exp(\frac{\pi\sqrt{\ell}}{a_i}) + 745.$$

As $a_i \leq \sqrt{\ell/3}$, we find that for $C = \log(|J| + 745)$,

$$\begin{aligned} |P_\ell(J)| &\leq \prod_{i=1}^{h} (|J| + 745 + \exp(\frac{C\sqrt{\ell}}{a_i})) \\ &\leq 2^h \prod_{i=1}^{h} \exp(\frac{C\sqrt{\ell}}{a_i}) \\ &= 2^h \exp\big(C\sqrt{\ell} \sum_{i=1}^{h} \frac{1}{a_i}\big), \end{aligned}$$

as desired.

Since $h(-4\ell) = 3h(-\ell)$, $P_{4\ell}$ is also a polynomial of odd degree. Moreover the zeroes of $P_{4\ell}(X)$ are obtained by applying the Hecke operator T_2 to the roots of $P_\ell(X)$ (see [2]), so that the zeroes of $P_{4\ell}(X)$ are

$$j(\frac{z_i}{2}), \quad j(\frac{z_i + 1}{2}), \quad j(2z_i)$$

where

$$z_i = \frac{-b_i + \sqrt{-\ell}}{2a_i}, \quad 1 \leq i \leq h.$$

We therefore obtain by the same method:

Lemma 6

$$|P_{4\ell}(J)| \leq 2^h \exp\big(4C\sqrt{\ell} \sum_{i=1}^{h} \frac{1}{a_i}\big).$$

We need to bound

$$\sum_{i=1}^{h} \frac{1}{a_i}.$$

For this we utilise classical identities involving the Epstein zeta functions and the zeta function of a quadratic field. If K is an imaginary quadratic field, we set

$$f_\ell(s) = \sum_{i=1}^{h} a_i^{-s}.$$

It is known (see Mordell [5]) that

$$\zeta_K(s) = \zeta(2s) f_\ell(s) + \ell^{\frac{1}{2}-s} f_\ell(1-s) \frac{\zeta(2s-1)\Gamma(s-\frac{1}{2})\sqrt{\pi}}{\Gamma(s)} + O(h\ell^{-s/2})$$

uniformly for $\frac{1}{2} \leq s < 1$. Assuming the generalised Riemann hypothesis for $\zeta_K(s)$, we have that $\zeta_K(s) < 0$ in this interval. Thus, setting

$$s = 1 - \frac{1}{\log \ell},$$

we deduce that

$$\sum_{i=1}^{h} \frac{1}{a_i} \ll L(1,\chi) \log \ell$$

where χ is the quadratic character corresponding to k. Such an estimate was first obtained by Mahler [4] in 1934. Combining this estimate with Lemmas 5 and 6 yields:

Lemma 7

$$|P_\ell(J)P_{4\ell}(J)| \leq 2^{2h} \exp(5C\sqrt{\ell}L(1,\chi)\log \ell).$$

We are now ready to prove our main theorem.

Proof of the Theorem Let $p_1 < ... < p_k$ be the first k supersingular primes. Then, choosing ℓ to satisfy $(*)$, we obtain

$$\left(\frac{P_\ell(J)P_{4\ell}(J)}{\ell}\right) = 1$$

by Lemma 1. But $P_\ell(J)P_{4\ell}(J) = -S$, where $S > 0$, by Lemma 3. Thus,

$$(\frac{-S}{\ell}) = 1 \Rightarrow (\frac{S}{\ell}) = -1$$

as $\ell \equiv 3 \pmod 4$. Therefore, not all prime divisors of S can be among $p_1, ..., p_k$. Thus,

$$\begin{aligned} p_{k+1} &\leq |P_\ell(J)P_{4\ell}(J)| \\ &\leq 2^{2h} \exp(5C\sqrt{\ell}L(1,\chi)\log \ell) \end{aligned}$$

by Lemma 7. By Lemma 4,

$$\ell \leq c4^k (\sum_{i=1}^{k} \log p_i)^2$$

and since $L(1,\chi) \leq \log \ell$, we obtain

$$\begin{aligned} \log p_{k+1} &\leq 10C_1\sqrt{\ell}(\log \ell)^2 \\ &\leq 10C_1 2^k k(\log p_k)(2k + \log k + \log\log p_k)^2, \end{aligned}$$

for some absolute constant C_1. It now follows easily by induction that

$$\log p_k \leq \exp(k^2).$$

From this inequality, we easily deduce that

$$\pi_0(x) \geq (\log\log x)^{1/2}.$$

This completes the proof of the Theorem.

The above argument was extended by Elkies [2] in his doctoral thesis. By utilising the fact that common prime factors of $P_\ell(J)$ for different ℓ's can be explicitly determined by a theorem of Gross and Zagier [9] on singular moduli, Elkies [2] proved that assuming GRH,

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

in an effective manner. From this effective result, he proves that

$$\pi_0(x) \gg \log\log x,$$

modulo the same hypothesis.

These ideas have further applications. For instance, they can be utilised to prove that for curves

$$E_a : \qquad y^2 = (x^2+1)(x+a), \qquad a \in \mathbf{Q},$$

$E_a(\mathbf{F}_p)$ is cyclic infinitely often, without assuming the GRH. This was previously established by J-P. Serre [8] under the generalised Riemann hypothesis.

REFERENCES

[1] M. Deuring, Die typen der multiplikatorenringer elliptischer funktionkörper, *Abh. Math. Sem. Hamburg Univ.* **14** (1941) 197-272.

[2] N. Elkies, The infinitude of supersingular primes for any elliptic curve over $\mathbf{Q}$, *Inventiones Math.*, **89** (1987) 561-567. (see also N. Elkies, Ph.D. Thesis, Harvard University (1987).

[3] S. Lang and H. Trotter, Frobenius distributions in GL_2 extensions, *Springer Lecture Notes*, **504** (1976).

[4] K. Mahler, On Hecke's theorem on the real zeroes of the L-functions and the class number of quadratic fields, *Journal of the London Math. Soc.*, **9** (1934) 298-302.

[5] L. J. Mordell, On the Riemann hypothesis and imaginary quadratic fields with a given class number, *Journal of London Math. Soc.*, **9** (1934) 289-298.

[6] H. Montgomery, Topics in multiplicative number theory, *Springer Lecture Notes*, **227** (1972).

[7] R. A. Rankin, Modular forms, Cambridge University Press, (1976).

[8] J.-P. Serre, Resumé de cours (1977), Œuvres, Springer-Verlag, (1986).

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

M. Ram Murty, Department of Mathematics, McGill University, Montreal, Canada H3A 2K6