Problems and References for the UML / Junior Seminar

Andrew Wiles, Steven Miller

October 23, 2001

1 General Information

The main webpage for last year's UML / Junior Seminar is
http://www.math.princeton.edu/~mathlab/index.html

Information and Handouts about this year's Seminar is available at
http://www.math.princeton.edu/~mathlab/jr01/main.html

MathSciNet (http://www.ams.org/mathscinet) is an outstanding way to look up authors and articles. Often you can download the articles you find (not always, but some have an [article] button you can click to display the text). Regardless, there are usually very helpful reviews.

2 Problems and References

Problem 1: Rank of a Curve. Building on investigations from last year, can one see the rank of the elliptic curve by investigating (smoothed) sums of a_p and a_p^2? Let $\lambda_p = \frac{a_p}{\sqrt{p}}$. Similar to the proof of the Prime Number Theorem we can show

$$\sum_\rho \frac{x^\rho}{\rho} = -\sum_{p \leq x} \lambda_p \log p - \sum_{p \leq \sqrt{x}} \lambda_p^2 \log p + 2x^{\frac{1}{2}} + small, \tag{2.1}$$

where ρ runs thru the zeros of the elliptic curve. We've normalized so the critical strip is $0 \leq s \leq 1$. The Generalized Riemann Hypothesis asserts that all the zeros have $Re(s) = \frac{1}{2}$.

Let r_a be the multiplicity of the zero at the critical point $s = \frac{1}{2}$. We can show the above implies

$$\frac{1}{x^{\frac{1}{2}}} \sum_{p \leq x} \lambda_p \log p = (1 - 2r_a) + O\Big(\sum_{\rho \neq \frac{1}{2}} \frac{x^{\rho - \frac{1}{2}}}{\rho} \Big). \tag{2.2}$$

Instead of having a sharp cut-off, we could instead study a smoothed version of the above. If we assume the Generalized Riemann Hypothesis, we might expect the sum to oscillate around
$1 - 2r_a$.

References: See Oana Pascu's investigations from last year: http://www.math.princeton.edu/˜mathlab/projects/ellcurves/main.html.

Especially see her writeup (which you can also reach by going to the webpage of her report): http://www.math.princeton.edu/˜mathlab/projects/ellcurves/op/curvecubic.doc

Additionally, look at my handout on the Explicit Formula for Elliptic Curves (available from this year's homepage).

Problem 2: The Parity Conjecture. We can analytically continue the L-function of an elliptic curve, and we get a functional equation $\Lambda(s, E) = \epsilon_E \Lambda(2 - s, E)$, where $\epsilon_E = \pm 1$. The Parity Conjecture asserts that (in the limit) $\epsilon_E = 1$ and $\epsilon_E = -1$ are equally likely. Alternatively, one could see if the Parity Conjecture still holds if, instead of considering the family of all elliptic curves, we instead consider a one-parameter family $y^2 = x^3 + A(t)x + B(t)$.

References: Birch, B. J.; Stephens, N. M. The parity of the rank of the Mordell-Weil group. Topology 5 1966 295–299. This computes the parity of a one-parameter family of elliptic curves. Rohrlich, David E. Variation of the root number in families of elliptic curves. Compositio Math. 87 (1993), no. 2, 119–151. Brumer, Armand; McGuinness, Oisn: The behavior of the Mordell-Weil group of elliptic curves. Bull. Amer. Math. Soc. (N.S.) 23 (1990), no. 2, 375–382.

Problem 3: Conductors. $\Lambda(s,E) = (2\pi)^{-s} N^{\frac{s}{2}} \Gamma(s) L(s)$, where N is the conductor, and has the same prime factors as the discriminant. Study how the conductor varies in a family (say the family of all elliptic curves, or maybe a one-parameter family). In many applications (for example, trying to bound the average rank or investigating density functions) what enters our equations is not N but $\log N$. For example, consider the family $\mathcal{F}_N = \{E_{a,b} : y^2 = x^3 + ax + b, a \in [N^2, 2N^2], b \in [N^3, 2N^3]\}$. Then $\Delta_{a,b}$ is of size N^6 for all curves in this family. How does $\log N_{a,b}$ vary?

References:

Problem 4: Excess Rank. Consider one-parameter families of elliptic curves. By construction, we can often force points of infinite order on our curves. Let us assume we have a family where we have forced r points on each curve E_t. By the Birch and Swinnerton-Dyer Conjecture, the geometric rank of the group of rational points should equal the order of vanishing of the associated L-function at the critical point. Assuming the Parity Conjecture, we might expect half the curves to have rank r, and half to have rank $r+1$. (The functional equation being odd forces another zero). Previous investigations (see, for example, Fermigier) for many curves with small values for t have shown that this is not the case; ie, that for small t, for many families about 32% have rank r, 48% have rank $r+1$, 18% have rank $r+2$, and 2% have rank $r+3$. Is this a general phenomenon that persists in the limit, or the result of small numbers?

References: Fermigier, Stéfane Étude expérimentale du rang de familles de courbes elliptiques sur Q. (French) [Experimental study of the rank of families of elliptic curves over Q] Experiment. Math. 5 (1996), no. 2, 119–130. (Note: I've translated this into English). See also Fermigier, Stéfane Zéros des fonctions L de courbes elliptiques. (French) [Zeros of L-functions of elliptic curves] Experiment. Math. 1 (1992), no. 2, 167–173. Brumer, Armand; McGuinness, Oisn: The behavior of the Mordell-Weil group of elliptic curves. Bull. Amer. Math. Soc. (N.S.) 23 (1990), no. 2, 375–382. Brumer, Armand The average rank of elliptic curves. I. Invent. Math. 109 (1992), no. 3, 445–472. Gouva, F.; Mazur, B. The square-free sieve and the rank of elliptic curves. J. Amer. Math. Soc. 4 (1991), no. 1, 1–23. (Available on-line thru MathSciNet).

Problem 5: Elliptic Surfaces. Let $\mathcal{F}$ be a parametrized family of Elliptic Curves. For a curve $E \in \mathcal{F}$, denote the curve by $y^2 = f_E(x)$. For a prime p and a curve $E \in \mathcal{F}$, let

$$a_E(p) = \sum_{x=0}^{p-1} \left(\frac{f_E(x)}{p}\right) = O(\sqrt{p}) \tag{2.3}$$

Silverman and Rosen have shown that, if our family is parametrized by a variable t, summing $a_E(p) = a_{E_t}(p)$ is related to the rank over $\mathbf{Q}(T)$. Specifically, let $\mathcal{E}$ be the elliptic surface $y^2 + a_1(T)xy + a_3(T) = x^3 + a_2(T)x + a_6(T)$, $a_i(T) \in \mathbf{Z}[T]$, $\Delta(T) \neq 0$. (Note: in this case, our family F will often be $\{E_t : t \in [N, 2N]\}$. Let $A_{\mathcal{E}}(p) = \frac{1}{p}\sum_{t=0}^{p-1} a_{E_t}(p)$. (Note: $A_{\mathcal{E}}(p)$ is bounded independently of p). Silverman and Rosen show (assuming Tate's conjecture for Elliptic Surfaces, including the weak non-vanishing assumption that $L_2(\mathcal{E}, s)$ does not vanish on the line $Re(s) = 2$)

$$\lim_{X\to\infty} \sum_{p \leq X} -A_{\mathcal{E}}(p) \log p = \textbf{rank } \mathcal{E}(\mathbf{Q}(T)). \tag{2.4}$$

For curves of the form $y^2 = x^3 + A(t)x + B(t)$, we can often prove the necessary assumptions. It is possible to cleverly choose families so that $A_{\mathcal{E}}(p)$ is constant. One can also (by numerical experimentation) find families where $A_{\mathcal{E}}(p)$ varies, but is an integer (and always in some range $[-N, M]$). Since we are dividing by p, it is not at all immediate that we should get an integer, and in fact, there are plenty of curves where we don't. Could these be the coefficients of an interesting form (say, something associated to Dirichlet L-series, or Galois representations, ...)?

References: Nagao, Koh-ichi $Q(T)$-rank of elliptic curves and certain limit coming from the local points. With an appendix by Nobuhiko Ishida, Tsuneo Ishikawa and the author. Manuscripta Math. 92 (1997), no. 1, 13–32. Rosen, Michael; Silverman, Joseph H. On the rank of an elliptic surface. Invent. Math. 133 (1998), no. 1, 43–67.

Problem 6: Torsion Groups. For any elliptic curve, we can calculate its torsion group; moreover, only a few groups may appear as the result.

In the family of all elliptic curves, what are the relative frequencies of each group? If we specialize to interesting one-parameter families, what are the relative frequencies here?

References: Mazur, B. Rational isogenies of prime degree (with an appendix by D. Goldfeld). Invent. Math. 44 (1978), no. 2, 129–162. Mazur, B. Modular curves and the Eisenstein ideal. Inst. Hautes Études Sci. Publ. Math. No. 47 (1977), 33–186 (1978). Qiu, Derong; Zhang, Xianke Explicit classification for torsion cyclic subgroups of rational points with even orders of elliptic curves. Chinese Sci. Bull. 44 (1999), no. 21, 1951–1953.

Problem 7: Points of Low Height. For any elliptic curve, we can try and find points of small height. How does the height of the lowest point (lowest infinite point?) vary in a family? Do curves in a given family with a low point have higher than predicted rank?

References: Check Silverman and Tate (copies should be in the UML). Also look at Silverman's The Arithmetic of Elliptic Curves, Springer Verlag, GTM, 106.

Problem 8: Birch and Swinnerton-Dyer Conjecture. In its simplest form, the B-SD Conjecture states the geometric rank of an elliptic curve should equal the analytic rank (the order of vanishing of the associated L-function at the critical point). For small rank curves, numerically verify.

References: Birch, B. J.; Swinnerton-Dyer, H. P. F. Notes on elliptic curves. I. J. Reine Angew. Math. 212 1963 7–25. Birch, B. J.; Swinnerton-Dyer, H. P. F. Notes on elliptic curves. II. J. Reine Angew. Math. 218 1965 79–108.

Problem 9: Sato-Tate. We know that $|a_p| \leq 2\sqrt{p}$; we can therefore write a_p as $2\cos\theta_p$. How does θ_p vary with p? Fix a one-parameter family. Write $a_{E_t}(p)$ as $2\cos\theta_{E_t}(p)$. For large primes, how do the $\theta_{E_t}(p)$ vary?

References: J. T. Tate, Arithmetical algebraic geometry (Proc. Conf. Purdue Univ., 1963), pp. 93 - 110.

Katz, Nicholas M. Exponential sums over finite fields and differential equations over the complex numbers: some interactions. Bull. Amer. Math. Soc. (N.S.) 23 (1990), no. 2, 269–309 (especially see the beginning of the article).

Problem 10: Lowest Zero. We expect the zeros of an elliptic curve to follow the GUE distribution. To see this may be beyond the computational ability of the UML (to see the convergence may require more computations than we can do on our machines; many such investigations use large amounts of time on supercomputers). We can, however, look at the first few zeros near the critical point. If we are (again) looking at a family, we can study the distribution of the lowest (or second lowest) zero. We may want to normalize with respect to the logarithm of the conductor.

Problem 11: Number of Zeros. By looking at functions related to $\zeta(s)$ and $L(s, E)$, we can construct a real valued function on the line $Re(s) = \frac{1}{2}$ which has the same zeros as $\zeta(s)$ or $L(s, E)$. By looking for sign changes in this function, we can find zeros of either; by standard methods of Complex Analysis, we can do contour integrals to find the number of zeros in a given region. If the number of sign changes equal the contour integral, then we have proved Riemann or Generalized Riemann in a region. Note the contour integral is almost certainly not an integer. We will have to approximate it, and then knowing it is an integer will allow us to move from an approximate counting of the number of zeros to an exact counting.

References: Titchmarsh, The Theory of the Riemann Zeta Function, Chapter XV (I'm not positive about the chapter). This provides a method of finding zeros by looking at the function $e^{i\theta(t)}\zeta(\frac{1}{2}+it)$, t real. For counting the number of zeros, see Davenport, Multiplicative Number Theory, as well as Ellison and Ellison, Prime Numbers.

See also Odlyzko: http://www.research.att.com/~amo/doc/complete.html. Read The $10^{22}nd$ zero of the Riemann zeta function, A. M. Odlyzko. It's the eighth paper listed: you can download and view it in either postscript or PDF.

Akiyama, Shigeki; Tanigawa, Yoshio Calculation of values of L-functions associated to elliptic curves. Math. Comp. 68 (1999), no. 227, 1201–1231. This article is available on-line: http://www.ams.org/jourcgi/amsjournal?fn

=120&pg1=pii&s1=S0025- 5718-99-01051-0 (again, you can find using MathSciNet and looking up the authors).

Problem 12: Primality Testing. The truth of the Generalized Riemann Hypothesis has consequences in designing algorithms to quickly determine if a given number is prime. For more information, see Koblitz. It should be in the UML (this book should be kept in the UML save for quick trips to the copier), and there should be references there for additional reading.

References: Koblitz, Neal A survey of number theory and cryptography. Number theory, 217–239, Trends Math., Birkhäuser, Basel, 2000. Koblitz, Neal, A course in number theory and cryptography; Springer-Verlag, c1987. Koblitz, Neal Elliptic curve cryptosystems. Math. Comp. 48 (1987), no. 177, 203–209. (Available on-line thru MathSciNet).