The Arithmetic of Elliptic Curves*

David Hansen

11/13/08

1 Some Motivation

Let's start with a classical Diophantine question. Let p be a prime. When can p be written as a sum of two integral squares? It's clear that a necessary condition for this is that $p \equiv 1 \bmod 4$; squares are all 0 or 1 mod 4. Now, it's perfectly fair to guess that, aside from this necessary condition, perhaps there is no elegant sufficient condition! After all, primes are defined by multiplicative properties, and this is a problem about addition of integers.

Nevertheless, here is a theorem of Fermat:

Theorem. *The necessary condition we have given is also sufficient. In other words, the equation $x^2 + y^2 = p$ has a solution in integers if and only if $p \equiv 1 \bmod 4$.*

Now, we might ask, is there a similar criterion for representing a prime as a sum of two cubes? We phrase this formally as

Question A. *Given a prime p, is there an elegant criterion to decide if the equation $x^3 + y^3 = p$ has a solution in rational numbers?*

I don't want to spoil the surprise, but I will mention that in the 19th century, Sylvester and Lucas showed that if $p \equiv 2 \text{ or } 5 \bmod 9$, there is no such solution. Our complete answer to this will come from the theory of "elliptic curves", which we will approach shortly. Before that, however, I want to motivate with another Diophantine problem. This one is even older, and goes back to the Greeks. The question is very simple: which right triangles with rational sides can have rational area? By scaling we can in fact restrict to squarefree integral area. We are trying to find a solution in rational numbers to the system of equations $a^2 + b^2 = c^2$, $\frac{1}{2}ab = n$. Eliminating a variable brings us to the single equation $y^2 = x^3 - n^2x$; a solution (x, y) to this corresponds to a triangle with sides $\left(\frac{n^2-x^2}{y}, \frac{2nx}{y}, \frac{n^2+x^2}{y}\right)$. An integer n for which such a solution exists is called a *congruent number.* It was known to Fermat that 1 is not congruent; in fact the smallest congruent number is 5, corresponding to the triangle $\left(\frac{40}{6}, \frac{9}{6}, \frac{41}{6}\right)$.

Question B. *Given an integer n, is there an elegant criterion to decide if the equation $y^2 = x^3 - n^2x$ has a solution in rational numbers? (And, therefore, if there exists a rational right triangle with area n?)*

*This is the text for a talk delivered at Williams College on November 13, 2008

2 Elliptic Curves - The Basics

The two curves we arrived at in the above problems are more similar than they might first appear; after a rational transformation, the curve in Question A becomes $y^2 = x^3 - 432p^2$. So both these curves are of the form

$$E : y^2 = x^3 + ax + b$$

for special choices of a, b. This is an *elliptic curve*. The name is something of a misnomer, and will be explained shortly.

Now, you might ask, of all the possible plane curves we could study, why are these special? The answer is quite startling: they are also groups! Even more excitingly, the group law is *rational*, in the sense that if P and Q are two points on E with rational coordinates, then $P + Q$ is also a point with rational coordinates. Now how do we define the group law? Draw the line through P and Q; this intersects the curve in one other point. Reflect this new point across the y-axis; this is $P + Q$. Explicitly, if $P = (x_1, y_1)$ and $Q = (x_2, y_2)$, then

$$P + Q = \left(\lambda^2 - a - x_1 - x_2, -\lambda x_3 - \nu\right)$$

with $\lambda = \frac{y_2 - y_1}{x_2 - x_1}$ and $\nu = y_1 - \lambda x_1$. What is the identity in this group law? It's the point $\mathcal{O}$ which is "infinitely far up" the y-axis. It is not so hard to check that this group law is commutative. To double a point, do the obvious thing - draw a tangent line! This is sometimes called the "chord-and-tangent" procedure.

Now, whenever we encounter a discrete group in mathematics, the most natural question to ask is whether or not it's finitely generated. In the language of elliptic curves, we are asking for a finite set of rational points such that any point in $E(\mathbb{Q})$ can be gotten by applying chord-and-tangent in some finite (though perhaps complicated) manner. There is a slight subtlety here; there are rational torsion points, or in other words points with $nP = \mathcal{O}$. For example, if $x^3 + ax + b = 0$ has a rational root r, then $P = (r, 0)$ is two-torsion. So we can modify our question and ask - aside from torsion, is $E(\mathbb{Q})$ finitely generated? This question was first raised by Poincare, who assumed the answer was yes. The first rigorous proof was provided by Mordell.

Theorem. *Let $E/\mathbb{Q}$ be an elliptic curve. Then the group of rational points $E(\mathbb{Q})$ is finitely generated; more specifically, there exists an integer $r(E) \geq 0$ such that*

$$E(\mathbb{Q}) \simeq \mathbb{Z}^{r(E)} \oplus E(\mathbb{Q})_{tors}.$$

There is a totally explicit bound on the torsion group; a theorem of Mazur gives $|E(\mathbb{Q})_{tors}| \leq 16$, and a theorem of Nagell and Lutz gives an explicit criterion for when a point is torsion. This does not concern us here; the rank is much more interesting. In fact, we'll pose the following rather vague

Fundamental Question. *How does the rank $r(E)$ vary as E varies?*

We're going to provide a conditional answer to this question, but it will be enough to spectacularly resolve Questions A and B. To do this, we will turn for a little while to "local" behavior. The discriminant of E is defined as

$\Delta = 4a^3 + 27b^2$. This integer has the lovely property that, for every prime not dividing Δ, the reduction modulo p of E is a non-singular curve. We can hence count points over $\mathbb{F}_p$. Set

$$N_p(E) = |E(\mathbb{F}_p)| = \#\{(x,y) \in (\mathbb{Z}/p\mathbb{Z})^2 \text{ s.t. } y^2 \equiv x^3 + ax + b \bmod p\}.$$

So, we're really counting how often x^3+ax+b is a square modulo p, for $0 < x < p$. Well, an initial guess would be that this polynomial is a square half the time, and a non-square the other half of the time. Counting the point "at infinity," this leads to the guess $N_p \approx p + 1$. In fact, this estimate is very close to the truth, as the following result of Hasse shows.

Theorem. *For $p \nmid \Delta$, we have $|N_p - p - 1| \leq 2\sqrt{p}$.*

OK, that's all well and good, but do these local point counting numbers have anything to do with the global structure of the curve over $\mathbb{Q}$? Bryan Birch and Peter Swinnerton-Dyer considered this question in the early 1960's, and they decided to do some computer experiments (at the time, still a novel idea in number theory). They considered the product

$$\phi(x,E) = \prod_{p \leq x} \frac{N_p(E)}{p}.$$

Their guess, which they hoped to see borne out in numerical data, was that if E had large rank over $\mathbb{Q}$, then the individual terms would tend to be slightly larger than p on average and so this function would show some growth as $x \to \infty$. What they saw was even more surprising, and led them to the following guess.

Conjecture (Birch/Swinnerton-Dyer, weak form). *As x grows, ϕsatisfies*

$$\phi(x,E) = (\log x)^{r(E)+o(1)}.$$

We can phrase this even more attractively. Define $a_p(E)$ by $N_p(E) = p + 1 - a_p(E)$. By Hasse's theorem, this is bounded by $|a_p| \leq 2\sqrt{p}$. We define the L-function of E by the product

$$L(s,E) = \prod_{p \nmid \Delta} \frac{1}{1 - a_p p^{-s} + p^{1-2s}};$$

the Hasse estimate guarantees that this product converges for $\Re(s) > 3/2$. An extremely deep theorem of Wiles asserts that $L(s,E)$ possesses an *analytic continuation* to the whole complex plane. (This is analogous to the series $1 + x + x^2 + x^3 ...$ only making sense for $|x| < 1$, but being "extended" to the whole plane as $1/(1-x)$) Note that $L(1,E)$ "equals" $\phi(\infty, E)^{-1}$. This is of course total nonsense, but it suggests that there should be a relation between the growth of ϕ and the behavior of $L(s,E)$ near $s = 1$; in fact, one can in fact prove rigoursly the following result:

Conjecture (Birch/Swinnerton-Dyer, strong form). *If $\phi(x,E) = (\log x)^{r(E)+o(1)}$, then $L(s,E)$ has a zero at $s = 1$ of order $r(E)$. The conjecture is then*

$$\operatorname{rank}(E) = \operatorname{ord}_{s=1} L(s,E).$$

This conjecture is astonishing. The progress to date has been minimal; it is known to be true if $E(\mathbb{Q})$ has rank 0 or 1, by the work of many authors.

3 Motivation Revisited

Now I'm going to astound you with answers to questions A and B.

Answer A. *If* $p \equiv 2, 5 \bmod 9$*, there is no solution. If* $p \equiv 4, 7, 8 \bmod 9$*, there is a solution. Now, define polynomials recursively by* $f_0(t) = 1$*,* $f_1(t) = t^2$ *and generally*

$$f_{n+1}(t) = (1 - t^3)f_n'(t) + (2n + 1)t^2 f_n(t) - n^2 t f_{n-1}(t).$$

Set $A_k = f_{3k}(0)$*; note that these are integers. Then there is a solution for* $p \equiv 1 \bmod 9$ *if and only if* $p|A_{2(p-1)/9}$*.*

Now, as for question B...

Answer B. *Let* n *be odd and squarefree. Define integers* A_n *and* B_n *by*

$$A_n = \#\{(x, y, z) \in \mathbb{Z}^3 \text{ s.t. } 2x^2 + y^2 + 8x^2 = n\}$$

and

$$B_n = \#\{(x, y, z) \in \mathbb{Z}^3 \text{ s.t. } 2x^2 + y^2 + 32x^2 = n\}.$$

Then n *is a congruent number if and only if* $A_n = 2B_n$*.*

How does one prove these results? Known results towards the Birch/Swinnerton-Dyer are a crucial ingredient; suffice it to say a great deal of sophisticated mathematics goes into the solutions. These ancient diophantine problems are best approached using the most finely honed tools in modern mathematics.