Diophantine Equations: Corrected Version

Alison Miller

June 30, 2011

Warning! I lied to you in class!

In class I gave you an incorrect statement of Siegel's theorem about integers point on curves of the form $y^2 = f(x)$. The correct statement is the following:

Let $f(x) \in \mathbb{Z}[x]$ be a polynomial of degree at least 3 with distinct roots. Then the equation $y^2 = f(x)$ has only finitely many solutions in $\mathbb{Z}$. (This is actually a special case of the full Siegel's theorem for integer points on more general curves, but it's a form which is easy to cite and apply accurately.)

However, it certainly can have infinitely many solutions in $\mathbb{Q}$ if f has degree 3 or 4. (This is true by the theory of elliptic curves; doing an explicit example is messy but I'd like to see one if anyone has one.)

1 Prologue: Diophantine Problems in general

Given a subset S of $\mathbb{C}$, one can ask if a given polynomial equation $f(a_1, \ldots, a_n) = 0$ has any solutions in S. Generally if one wants a nice theory for this sort of thing, one takes S to be a subring of $\mathbb{C}$. We'll call this a "diophantine equation over S" although the terminology may not be standard.

The difficulty of this depends upon what S is:

- $S = \mathbb{C}$.
- $S = \mathbb{R}$; decidable but painful.
- $S = \mathbb{Q}$; this is where most of the nice mathematical theories are; we don't know whether this is decidable or not.
- $S = \mathbb{Z}$; this is undecidable in general.

Reductions: Diophantine equations over $\mathbb{Q}$ can be reduced to Diophantine equations over $\mathbb{Z}$. Homogeneous diophantine equations over $\mathbb{Z}$ are equivalent to the same ones over $\mathbb{Q}$.

If you want to know more about this, look at Bjorn Poonen's website; it has some very good expository articles. If you want to know more about undecidability for $\mathbb{Z}$, ask Paul Valiant.

Of course, there are rings other than $\mathbb{Z}$. For example, $\mathbb{Z}/n = \mathbb{Z}/n\mathbb{Z} = \{\text{integers mod n}\}$. Finite rings are finite, but still:

- $S = \mathbb{Z}/p\mathbb{Z}$: see Josh's handout.

- $S = \mathbb{Z}/p^n\mathbb{Z}$: see my handout. Also Hensel's lemma.
- $S = \mathbb{Z}/n\mathbb{Z}$: CRT!

Also you can do diophantine problems in polynomial rings; you saw one on Aaron's polynomials handout and there's another one below.

2 Techniques and Heuristics

But all is not lost! With persistence and ingenuity, our intrepid mathematicians can rescue many equations from the depths of unsolvedness!

- Sandwiching: e.g. if you want to prove that some expression X cannot be a perfect kth power, show that $k^n < X < (k+1)^n$ for some n. This method generalizes.
- If you're looking to construct a solution, try clever algebraic specializations/substitutions. Always remember that linear is better than quadratic is better than cubic, etc. But it's nice to make things factor! (Or at least have singularities.)
- Pythagorean triples.
- Pythagoras plus: how to get a general formula for rational solutions to $ax^2 + by^2 = cz^2$ if you already have a single solution. WARNING: The polynomials does not give you all integer solutions (a, b, c) with $\gcd(a, b, c) = 1$; you need to rescale to get those. (Eg, for the Pythagorean triples our standard formula $(m^2 - n^2, 2mn, m^2 + n^2)$ only gives us triples (a, b, c) where b is even; this generalizes.)
- Pell's equation/recurrences.
- Infinite descent. Generally happens when your equation has a lot of symmetries, which generally happens with Pell-type equations.
- Quadratic Reciprocity and another reciprocity-ish law.

  Quadratic reciprocity can be stated in the following form: let $P(x) = x^2 + (-1)^{(p-1)/2}p$. Then if $q \neq p$ is a prime, q divides $P(a)$ for some integer a if and only if q is a square mod p.

  Let $\Phi_n(x)$ be the nth cyclotomic polynomial. If q is a prime not dividing n, q divides $P(a)$ for some integer a if and only if q is 1 mod n.

  Exercises: Prove the statements above.
- Look beyond $\mathbb{Z}$: factorizations in $\mathbb{Z}[i]$ and $\mathbb{Z}[\omega]$.

3 Examples

1 (TST 2002)**.** Find in explicit form all ordered pairs of positive integers m, n such that $mn - 1$ divides $m^2 + n^2$.

2 (MOP 2007, Ramanujan?)**.** Show that there exist infinitely many positive integers n such that

$$n = a^3 + b^3 = c^3 + d^3$$

for nonzero positive integers a, b, c, d with $\{a, b\} \neq \{c, d\}$.

3 (New to the revised handout!)**.** Show that any rational number can be written as the sum of three rational cubes in infinitely many ways.

4 (MOP 2000?)**.** Suppose p, N, D are positive integers (p is prime) such that

$$\begin{aligned} p &= x_1^2 + Dy_1^2 \\ Np &= x_2^2 + Dy_2^2 \end{aligned}$$

for some integers x_1, y_1, x_2, y_2. Then show that there are integers x, y such that $N = x^2 + Dy^2$.

5. Let λ be a complex number, $\lambda \neq 0, 1$. Show that if $a(x)$ is a rational function with complex coefficients such that

$$a(x)(a(x) - 1)(a(x) - \lambda)$$

is the square of a rational function, then $a(x)$ is a constant function.

4 Problems

6. Prove that there exists an integer $m \geq 2002$ and m distinct positive integers $a_1, a_2, \ldots, a_m$ such that

$$\prod_{i=1}^{m} a_i^2 - 4\sum_{i=1}^{m} a_i^2$$

is a perfect square.

7 (IMO Shortlist 2001)**.** Consider the system

$$x + y = z + u, \quad 2xy = zu.$$

Find the greatest value of the real constant m such that $m \leq x/y$ for any positive integer solution (x, y, z, u) of the system, with $x \geq y$.

8 (MOP 98)**.** Let p be a prime congruent to 3 mod 4, and let a, b, c, d be integers such that

$$a^{2p} + b^{2p} + c^{2p} = d^{2p}.$$

Show that p divides abc.

9 (China, 2002)**.** Sequence $\{a_n\}$ satisfies: $a_1 = 3$, $a_2 = 7$, $a_n^2 + 5 = a_{n-1}a_{n+1}$, $n \geq 2$. If $a_n + (-1)^n$ is prime, prove that there exists a nonnegative integer m such that $n = 3^m$.

10 (MOP 02)**.** Show that there are infinitely many ordered quadruples of integers (x, y, z, w) such that all six of

$$xy + 1, xz + 1, xw + 1, yz + 1, yw + 1, zw + 1$$

are perfect squares.

5 Problems from the real world

These are diophantine equations over $\mathbb{Q}$ that I found in published math papers; they were constructed as examples of diophantine equations with certain properties (generally failure of local-to-global), but their solutions are elementary.

11 (Reichardt-Lind)**.** Show that there are no rational solutions to the equation

$$x^4 - 17y^4 = 2z^2.$$

12 (Birch-Swinnerton-Dyer)**.** Show that there are no rational solutions to the system of equations

$$\begin{aligned} uv &= x^2 - 5y^2 \\ (u+v)(u+2v) &= x^2 - 5z^2. \end{aligned}$$

13 (Swinnerton-Dyer)**.** Show that if rational numbers x, y, z satisfy the equation

$$x^2 + y^2 = (4z - 7)(z^2 - 2)$$

then $z \geq 7/4$.

6 Further Reading

These are written for mathematicians, so parts will be over your heads, but other parts are understandable with only an olympiad background.

Poonen, Undecidability in Number Theory: `http://www-math.mit.edu/~poonen/papers/h10_notices.pdf`

Cox, Primes of the form $x^2 + ny^2$. (This is a book: the first third is written for people with a background of only elementary number theory, the second two thirds assume more advanced background.)

Noam Elkies, On the Areas of Rational Triangles. `http://www.math.harvard.edu/~elkies/euler_11c.pdf` How Euler solved a really messy diophantine equation, and what made it so messy (that part is very mathematicaly advanced).

Bright, Counterexamples to the Hasse Principle: `http://www.warwick.ac.uk/~maseap/arith/notes/elementary.pdf`