Diophantine Equations: Teacher's Version

Alison Miller

June 20, 2011

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 problemss over $\mathbb{Q}$ can be reduced to Diophantine problems over $\mathbb{Z}$. Homogeneous diophantine problems over $\mathbb{Z}$ are equivalent to the same problems over $\mathbb{Q}$.

If you want to know more about this, look at Bjorn Poonen's website. 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!

Cool stuff commented out: (Brief p-adics interlude. There are rings called $\mathbb{Z}_p$ and $\mathbb{Q}_p$ that I won't talk about in class. Here's why. A diophantine problem has a solution over $\mathbb{Z}_p$ iff it has a solution over $\mathbb{Z}/p^n$ for all n. Diophantine problems over $\mathbb{Q}_p$ can be reduced to diophantine equations over $\mathbb{Z}_p$, likewise to $\mathbb{Q}$ and $\mathbb{Z}$.)

Also you can do diophantine problems in polynomial rings; you saw one on Aaron's 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 $n^k < X < n^{k+1}$ 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: this method does not work for integer solutions.
- 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.

  Cool optional stuff: Let ζ_n be an nth root of unity. Let G be a subgroup of $\mathbb{Z}/n\mathbb{Z}^*$ and $\alpha_G = \sum_{g \in G} \zeta_n^g$. Let $f_G(x)$ be the minimal polynomial of α. Then for all primes p not dividing some discriminant (which should be something like n; what is it?) f_G has a root mod p (which is equivalent to f has n roots mod p?) if and only if the reduction of p is an element of α.

  Cool optional stuff: Example: G is the subgroup of quadratic residues. Exercise: $f_G = x^2 \pm p$, where the sign depends upon what p is mod 4.

  cool optional stuff: Example: $G = \{1, -1\}$, $n = 7$. Then the polynomial is $x^3 + x^2 - 2x - 1$, which has root $\zeta_7 + \zeta_7^{-1}$.

- 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 (IMO Shortlist 2002)**.** *classic specialization problem. also on Team Contest.* Is there an integer m such that the equation $\frac{1}{a} + \frac{1}{b} + \frac{1}{c} = \frac{m}{a+b+c}$ has infinitely many solutions in positive integers a, b, c?

3. *reciprocity. IMO shortlist. Move to example.* Find all integer solutions of the equation

$$\frac{x^7-1}{x-1} = y^5 - 1.$$

4 (IMO Shortlist 2002)**.** *classic example of sandwiching*

Let P be a cubic polynomial given by $P(x) = ax^3 + bx^2 + cx + d$, where a, b, c, d are integers and $a \neq 0$. Suppose that $xP(x) = yP(y)$ for infinitely many pairs x, y of integers with $x \neq y$. Prove that the equation $P(x) = 0$ has an integer root.

4 Problems

5 (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 $x \geq y$.

6. Let λ be a complex number. 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.

Descent by 2-isogeny; why can't I do this?

7. 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.

8. Suppose that x, y are positive integers such that both $x(y+1)$, $y(x+1)$ are perfect squares. Show that exactly one of x, y is a perfect square.

extra?

9 (IMO Shortlist 2000)**.** Show that for infinitely many n, there exists a triangle with integer sidelengths such that its semiperimeter is n times its inradius.

10 (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 $n = 3^m$.

11 (MOP 2000?)**.** Suppose p, N, D are positive integers 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 $N = x^2 + Dy^2$.

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

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

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

13 (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.

14 (IMO Shortlist 2003). An integer n is said to be good if $|n|$ is not the square of an integer. Determine all integers m with the following property: m can be represented, in infinitely many ways, as a sum of three distinct good integers whose product is the square of an odd integer.

15 (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.

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.

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

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

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

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

18 (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 at your level.

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

Cox, Primes of the form $x^2 + ny^2$. (The first third is written for people with a background of only elementary number theory.)

Noam Elkies, /On the Areas of Rational Triangles/.

Poonen, /Undecidability in Number Theory/ (?)