Effective methods for Diophantine problems

Michael Bennett

University of British Columbia

BIRS Summer School : June 2012

What are Diophantine equations?

According to Hilbert, a *Diophantine equation* is an equation of the form

$$D(x_1, \ldots, x_m) = 0,$$

where D is a polynomial with integer coefficients.

Hilbert's 10th problem : Determination of the solvability of a Diophantine equation. Given a diophantine equation with any number of unknown quantities and with rational integral numerical coefficients: To devise a process according to which it can be determined by a finite number of operations whether the equation is solvable in rational integers.

What are Diophantine equations? (take 2)

A few more opinions :

Wikipedia pretty much agrees with Hilbert

Mordell, in his book “Diophantine Equations”, never really defines the term (!)

Wolfram states
“A Diophantine equation is an equation
in which only integer solutions are allowed”.

Back to Hilbert's 10th problem

Determination of the solvability of a Diophantine equation. Given a diophantine equation with any number of unknown quantities and with rational integral numerical coefficients: To devise a process according to which it can be determined by a finite number of operations whether the equation is solvable in rational integers.

Matiyasevich's Theorem

(building on work of Davis, Putnam and Robinson) is that, in general, no such process exists.

Matiyasevich's Theorem

(building on work of Davis, Putnam and Robinson) is that, in general, no such process exists.

But . . .

Matiyasevich's Theorem

(building on work of Davis, Putnam and Robinson) is that, in general, no such process exists.

But ...

Hilbert's problem is still open over $\mathbb{Q}$ (and over O_K for most number fields)

Matiyasevich's Theorem

(building on work of Davis, Putnam and Robinson) is that, in general, no such process exists.

But ...

Hilbert's problem is still open over $\mathbb{Q}$ (and over O_K for most number fields)

It is not yet understood what happens if the number of variables is "small"

Perhaps we should simplify (?) things...

1. We could try to answer Hilbert's question for plane curves; i.e. try to decide whether an equation of the shape $f(x,y) = 0$ has integral or rational solutions.

2. We could try to bound the number of such solutions.

3. We could try to find an algorithm for explicitly solving such equations.

However....

- A complete answer to Problem 1 is unavailable – no algorithm is known to determine whether a curve has a rational point!
- Problem 2 has some partial answers (Rémond).
- Problem 3 is open, even in the case of genus 2...

So, what can we prove?

So, what can we prove?

Sticking to curves – let C be a nonsingular algebraic curve of genus g over, say, $\mathbb{Q}$. Then the set of rational points on C is

So, what can we prove?

Sticking to curves – let C be a nonsingular algebraic curve of genus g over, say, $\mathbb{Q}$. Then the set of rational points on C is

1. infinite or empty if $g = 0$ (conic section)

So, what can we prove?

Sticking to curves – let C be a nonsingular algebraic curve of genus g over, say, $\mathbb{Q}$. Then the set of rational points on C is

1. infinite or empty if $g = 0$ (conic section)

2. empty or C is an elliptic curve, if $g = 1$ (so that the rational points form a finitely generated abelian group, via Mordell), or

So, what can we prove?

Sticking to curves – let C be a nonsingular algebraic curve of genus g over, say, $\mathbb{Q}$. Then the set of rational points on C is

1. infinite or empty if $g = 0$ (conic section)
2. empty or C is an elliptic curve, if $g = 1$ (so that the rational points form a finitely generated abelian group, via Mordell), or
3. at most finite if $g > 1$ (Faltings' theorem née Mordell's conjecture).

So, what can we prove?

Sticking to curves – let C be a nonsingular algebraic curve of genus g over, say, $\mathbb{Q}$. Then the set of integral points on C is

1. infinite or empty, or somewhere in between, if $g = 0$
2. at most finite if $g > 0$ (Siegel's theorem).

A Diversion : Local-Global Principles

Consider

$$x^2 + y^2 = -1,$$

$$x^2 + y^2 = 3,$$

and

$$x^2 + y^2 = 5.$$

A Diversion : Local-Global Principles

Consider

$$x^2 + y^2 = -1,$$

$$x^2 + y^2 = 3,$$

and

$$x^2 + y^2 = 5.$$

Solutions over $\mathbb{Q} \implies$ solutions over $\mathbb{R}$ and $\mathbb{Q}_p$ for all p.

So we understand curves, right?

The problem is that the theorems of Faltings and Siegel and *ineffective*, in that their proofs do not provide a way to determine the implicit finite set (in case the genus of the curve satisfies $g > 1$, or $g > 0$, respectively).

So we understand curves, right?

The problem is that the theorems of Faltings and Siegel and *ineffective*, in that their proofs do not provide a way to determine the implicit finite set (in case the genus of the curve satisfies $g > 1$, or $g > 0$, respectively).

We are interested in **effective methods** (and not just for curves!).

A Diversion : Motivation

Why do we study Diophantine equations?

A Diversion : Motivation

Why do we study Diophantine equations?

1. They arise “naturally” in other areas of math.

A Diversion : Motivation

Why do we study Diophantine equations?

1. They arise "naturally" in other areas of math.
2. They provide valuable test-cases for theorems and conjectures coming from, say, algebraic geometry.

A Diversion : Motivation

Why do we study Diophantine equations?

1. They arise “naturally” in other areas of math.
2. They provide valuable test-cases for theorems and conjectures coming from, say, algebraic geometry.
3. It beats working.

Case study : The Ramanujan-Nagell equation

Consider the sequence of integers $2^n - 7$, $n \geq 3$:

$$\mathbf{1}, \mathbf{9}, \mathbf{25}, 57, \mathbf{121}, 249, 505, 1017,$$

$$2041, 4089, 8185, 16377, \mathbf{32761},$$

$$65529, 131065, 262137, 524281,$$

$$1048569, 2097145, 4194297, \ldots$$

Case study : The Ramanujan-Nagell equation

Consider the sequence of integers $2^n - 7$, $n \geq 3$:

$$\mathbf{1}, \mathbf{9}, \mathbf{25}, 57, \mathbf{121}, 249, 505, 1017,$$

$$2041, 4089, 8185, 16377, \mathbf{32761},$$

$$65529, 131065, 262137, 524281,$$

$$1048569, 2097145, 4194297, \ldots$$

Ramanujan's Question of 1913 (Journal of the Indian Mathematical Society) : Are the numbers in bold the only squares in the sequence?

A Class of Diophantine Equations

This is an example of a

Polynomial-Exponential Equation.

For a fixed, irreducible polynomal $f(x)$ with integer coefficients and degree at least 2, we have

$$P(f(x)) \to \infty,$$

where $P(m)$ denotes the greatest prime divisor of an integer m. To quantify this statement for a fixed $f(x)$ can turn out to be quite difficult (**linear forms in logarithms**).

Conjecture proved

In 1959, Chowla, Lewis and Skolem published a proof in the Proceedings of the American Mathematical Society, but....

Conjecture proved

In 1959, Chowla, Lewis and Skolem published a proof in the Proceedings of the American Mathematical Society, but....

Earlier that year, Shapiro and Slotnick had published a result that implied the conjecture in the I.B.M. Journal of Research Developments! (more on this later), but...

Conjecture proved

In 1959, Chowla, Lewis and Skolem published a proof in the Proceedings of the American Mathematical Society, but....

Earlier that year, Shapiro and Slotnick had published a result that implied the conjecture in the I.B.M. Journal of Research Developments! (more on this later), but...

As pointed out by Schinzel in 1960, he and Browkin had published an equivalent result as early as 1956, but....

Conjecture already proved!

In an Elementary Number Theory textbook of 1951, Trygve Nagell has this problem as an exercise for (undergraduate) students . . .

And Credit Goes To...

Nagell (1948) in a Norwegian journal....

In the years since, there have been no less than fifty papers published on this problem and its generalizations, and at least three surveys written (including one by Helmut Hasse).

Appearances of the Ramanujan-Nagell equation

- Coding Theory
- Differential Algebra
- Classification of Finite Simple Groups
- Design Theory
- Algebraic Geometry

The I.B.M. Journal of Research Developments?

A problem in coding theory:
The sphere $S_e(a)$ of radius e centered at the vector $a \in F_q^N$ is the set

$$S_e(a) = \left\{ x \in F_q^N \mid D(x, a) \leq e \right\},$$

where $D(x, a)$ denotes the *Hamming distance* between the vectors x and a; i.e. the number of nonzero components in $x - a$.

Coding theory (continued)

Since there are $q-1$ ways to change an individual entry, we have

$$|S_e(a)| = \sum_{i=0}^{e} \binom{N}{i} (q-1)^i.$$

If C is a code in F_q^N with minimum Hamming distance D and we let $e = [(D-1)/2]$, then we obtain the *sphere packing bound* :

$$|C| \left(\sum_{i=0}^{e} \binom{N}{i} (q-1)^i \right) \le q^N.$$

The sphere packing bound

expresses the fact that spheres of Hamming radius e centered at the codewords of C are disjoint, and the union of these spheres is a subset of F_q^N. An e-error correcting code for which equality holds in the sphere-packing bound is called *perfect*.

In such a situation, we have that

$$\sum_{i=0}^{e} \binom{N}{i} (q-1)^i \text{ divides } q^N.$$

Perfect codes

A reasonable place to look for perfect codes, then, is to examine when

$$\sum_{i=0}^{e} \binom{N}{i} (q-1)^i$$

is actually a power of q. In case $e=2$, we have

$$\binom{N}{0} + \binom{N}{1} (q-1) + \binom{N}{2} (q-1)^2 = q^k.$$

Some special cases

If $q = 3$, this is just the Diophantine equation

$$2N^2 + 1 = 3^k.$$

The solution

$$2 \cdot 11^2 + 1 = 3^5$$

corresponds to the $[11, 6, 5]$ ternary Golay code. This consists of 3^6 codewords of length 11 and minimum distance 5.
If $q = 2$, the equations becomes

$$(2N + 1)^2 + 7 = 2^{k+3}.$$

This is what led Shapiro and Slotnick to the Ramanujan-Nagell equation.

An Amazing Code?

So maybe the identity

$$181^2 + 7 = 2^{15}$$

corresponds to a remarkable code! Unfortunately, not – there's more going on here than just the sphere-packing-bound.

In fact, in a series of beautiful papers, beginning in the early 1970's, van Lint, Tietäváinen, and Zinoviev and Leontiev showed that the only perfect multiple-error-correcting codes are the binary and ternary Golay codes, and the binary repetition codes.

But....

The Diophantine equations associated to perfect codes are still mostly unsolved; even the equation corresponding to $q = p$ prime and $e = 2$ is open!

A number of similar questions in coding theory with other metrics have been tackled via Diophantine equations.

Case study 2 : Approximating π

We have

$$3 + \frac{10}{71} < \pi < 3 + \frac{1}{7}$$

(Archimedes), via inscribed and circumscribed 96-gons. Ludolph van Ceulen extended this approach to compute 35 decimal digits of π; he had

$$3.14159265358979323846264338327950288...$$

engraved on his tombstone.

Early improvements

Gregory used the Maclaurin series for $\arctan = \tan^{-1}$:

$$\arctan(x) = x - x^3/3 + x^5/5 - x^7/7 + \cdots$$

Taking $x = 1$, this requires about $10,000$ terms to get 4 decimal places of accuracy!

Machin used the relation

$$4 \arctan \frac{1}{5} - \arctan \frac{1}{239} = \frac{\pi}{4}$$

to get 100 digits correctly.

William Shanks (described as "a man of independent means") over slightly more than 20 years used this formula to compute the first 527 digits of π.

Can we do better?

The equation

$$m \arctan \frac{1}{x} + n \arctan \frac{1}{y} = k \cdot \frac{\pi}{4}$$

has the known solutions

$$\arctan \frac{1}{2} + \arctan \frac{1}{3} = \frac{\pi}{4},$$

$$2 \arctan \frac{1}{2} - \arctan \frac{1}{7} = \frac{\pi}{4},$$

$$2 \arctan \frac{1}{3} + \arctan \frac{1}{7} = \frac{\pi}{4}$$

and

$$4 \arctan \frac{1}{5} - \arctan \frac{1}{239} = \frac{\pi}{4}.$$

There are, in fact, no others.

How to prove this

Notice that

$$a + i\,b = \sqrt{a^2 + b^2}\; e^{i \arctan(b/a)}$$

so that if we have

$$k \arctan\left(\frac{1}{-1}\right) + m \arctan\frac{1}{x} + n \arctan\frac{1}{y} = 0,$$

then

$$(1-i)^k (x+i)^m (y+i)^n = (1+i)^k (x-i)^m (y-i)^n$$

is real. After a little work, we find that

$$x + i = \epsilon (1+i)^{\delta} (\alpha + i\beta)^n$$

$$y - i = \epsilon' (1-i)^{\delta'} (\alpha + i\beta)^m$$

From which we conclude that

The integers x and y satisfy

$$1 + x^2 = 2^\delta A^n \text{ and } 1 + y^2 = 2^{\delta'} A^m,$$

where A is an integer and $\delta, \delta' \in \{0, 1\}$.

The arctan identities mentioned earlier correspond to

$$1 + 2^2 = 5 \text{ and } 1 + 7^2 = 2 \cdot 5^2,$$

$$1 + 2^2 = 5 \text{ and } 1 + 3^2 = 2 \cdot 5,$$

$$1 + 3^2 = 2 \cdot 5 \text{ and } 1 + 7^2 = 2 \cdot 5^2,$$

$$1 + 5^2 = 2 \cdot 13 \text{ and } 1 + 239^2 = 2 \cdot 13^4.$$

Ljunggren's Theorem

Theorem

(Ljunggren, 1942) : If x and y are positive integers satisfying

$$x^2 + 1 = 2y^4,$$

then $(x, y) = (1, 1)$ or $(x, y) = (239, 13)$.

Størmer had earlier handled all other cases of

$$x^2 + 1 = 2^\delta A^n.$$

Regarding Ljunggren's proof

Mordell : "One cannot imagine a more involved solution . . . . One could only wish for a simpler proof".

Regarding Ljunggren's proof

Mordell : "One cannot imagine a more involved solution . . . . One could only wish for a simpler proof".

Guy : Problem D6 in *Unsolved Problems in Number Theory* is to find an elementary solution.

Case Study 3 : The Generalized Fermat Equation

We consider the equation

$$x^p + y^q = z^r$$

where x, y and z are relatively prime integers, and p, q and r are positive integers with

$$\frac{1}{p} + \frac{1}{q} + \frac{1}{r} < 1.$$

- $(p, q, r) = (n, n, n)$: Fermat's equation
- $y = 1$: Catalan's equation
- considered by Beukers, Granville, Tijdeman, Zagier, Beal (and many others)

A simple case

$$x^p + y^q = z^r$$

where x, y and z are relatively prime integers, and p, q and r are positive integers with

$$\frac{1}{p} + \frac{1}{q} + \frac{1}{r} = 1.$$

- $(p, q, r) = (2, 6, 3), (2, 4, 4), (4, 4, 2), (3, 3, 3), (2, 3, 6)$
- each case corresponds to an elliptic curve of rank 0
- the only coprime nonzero solutions is with $(p, q, r) = (2, 3, 6)$ – corresponding to $3^2 - 2^3 = 1$

For example : $x^3 + y^3 = z^3$

We write

$$Y = \frac{36(x-y)}{x+y} \text{ and } X = \frac{12z}{x+y},$$

so that

$$Y^2 = X^3 - 432.$$

For example : $x^3 + y^3 = z^3$

We write

$$Y = \frac{36(x-y)}{x+y} \quad \text{and} \quad X = \frac{12z}{x+y},$$

so that

$$Y^2 = X^3 - 432.$$

This is 27A in Cremona's tables – it has rank zero and

$$E(\mathbb{Q}) \simeq \mathbb{Z}/3\mathbb{Z}.$$

A less simple case

$$x^p + y^q = z^r$$

where x, y and z are relatively prime integers, and p, q and r are positive integers with

$$\frac{1}{p} + \frac{1}{q} + \frac{1}{r} > 1.$$

- $(2, 2, r), (2, q, 2), (2, 3, 3), (2, 3, 4), (2, 4, 3), (2, 3, 5)$
- in each case, the coprime integer solutions come in finitely many two parameter families (the canonical model is that of Pythagorean triples)
- in the $(2, 3, 5)$ case, there are precisely 27 such families (as proved by J. Edwards, 2004)

Back to

$$x^p + y^q = z^r$$

where x, y and z are relatively prime integers, and p, q and r are positive integers with

$$\frac{1}{p} + \frac{1}{q} + \frac{1}{r} < 1.$$

Some solutions

$$1^n + 2^3 = 3^2,$$

$$2^5 + 7^2 = 3^4,$$

$$3^5 + 11^4 = 122^2,$$

$$2^7 + 17^3 = 71^2,$$

$$7^3 + 13^2 = 2^9,$$

$$43^8 + 96222^3 = 30042907^2,$$

$$33^8 + 1549034^2 = 15613^3,$$

$$17^7 + 76271^3 = 21063928^2,$$

$$1414^3 + 2213459^2 = 65^7,$$

$$9262^3 + 15312283^2 = 113^7.$$

Conjecture (weak version $0)

There are at most finitely many other solutions.

Conjecture (weak version \$0)

There are at most finitely many other solutions.

Conjecture (Beal prize problem \$100,000)

Every such solution has $\min\{p, q, r\} = 2$.

Conjecture (weak version \$0)

There are at most finitely many other solutions.

Conjecture (Beal prize problem \$100,000)

Every such solution has $\min\{p, q, r\} = 2$.

Conjecture (strong version $\geq$ \$100,000)

There are no additional solutions.

What we know

Theorem (Darmon and Granville) If A, B, C, p, q and r are fixed positive integers with

$$\frac{1}{p} + \frac{1}{q} + \frac{1}{r} < 1,$$

then the equation

$$Ax^p + By^q = Cz^r$$

has at most finitely many solutions in coprime nonzero integers x, y and z.

The state of the art (?)

(p, q, r)	reference(s)
(n, n, n)	Wiles, Taylor-Wiles
$(n, n, k), k \in \{2, 3\}$	Darmon-Merel, Poonen
$(2n, 2n, 5)$	B.
$(2, 4, n)$	Ellenberg, B-Ellenberg-Ng, Bruin
$(2, 6, n)$	B-Chen, Bruin
$(2, n, 4)$	B-Skinner, Bruin
$(2, n, 6)$	BCDY
$(3j, 3k, n),\ j, k \geq 2$	immediate from Kraus
$(3, 3, 2n)$	BCDY
$(3, 6, n)$	BCDY
$(2, 2n, k),\ k \in \{9, 10, 15\}$	BCDY
$(4, 2n, 3)$	BCDY

The state of the art : continued

(p, q, r)	reference(s)
$(3, 3, n)^*$	Chen-Siksek, Kraus, Bruin, Dahmen
$(2, 2n, 3)^*$	Chen, Dahmen, Siksek
$(2, 2n, 5)^*$	Chen
$(2m, 2n, 3)^*$	BCDY
$(2, 4n, 3)^*$	BCDY
$(3, 3n, 2)^*$	BCDY
$(2, 3, n),\ 6 \leq n \leq 10$	PSS, Bruin, Brown, Siksek
$(3, 4, 5)$	Siksek-Stoll
$(5, 5, 7),\ (7, 7, 5)$	Dahmen-Siksek

The state of the art : continued

The * here refers to conditional results. For instance, in case $(p, q, r) = (3, 3, n)$, we have no solutions if either $3 \leq n \leq 10^4$, or $n \equiv \pm 2$ modulo 5, or $n \equiv \pm 17$ modulo 78, or

$$n \equiv 51, 103, 105 \text{ modulo } 106,$$

or for n (modulo 1296) one of

$$43, 49, 61, 79, 97, 151, 157, 169, 187, 205, 259, 265, 277, 295, 313, 367, 373, 385, 403, 421, 475, 481, 493, 511, 529, 583, 601, 619, 637, 691, 697, 709, 727, 745, 799, 805, 817, 835, 853, 907, 913, 925, 943, 961, 1015, 1021, 1033, 1051, 1069, 1123, 1129, 1141, 1159, 1177, 1231, 1237, 1249, 1267, 1285.$$

Methods of proof

These results have all followed from either

- Chabauty-type techniques, or
- Methods based upon the modularity of certain Galois representations

Methods of proof

These results have all followed from either

- Chabauty-type techniques, or
- Methods based upon the modularity of certain Galois representations

Both of these techniques will be discussed this week.

Open problems (hard edition)

$$x^p - y^q = 2, \quad x^p - y^q = 6, \quad \frac{4}{n} = \frac{1}{x} + \frac{1}{y} + \frac{1}{z},$$

$$(x^2 - 1)(y^2 - 1) = (z^2 - 1)^2,$$

$$x^2 - 2 = y^n, \quad x^n + y^n = z^5, \quad \frac{x^n - 1}{x - 1} = y^q,$$