How we solve Diophantine equations

Alex Bartel

April 13, 2011

Introduction

A **Diophantine problem** is the problem of finding *integer* or *rational* solutions to a given polynomial equation in one or several variables with rational coefficients.

Examples

Examples

- Find $(x, y) \in \mathbb{Q}^2$ satisfying $x^2 - 5y^2 = 3$.

Examples

- Find $(x, y) \in \mathbb{Q}^2$ satisfying $x^2 - 5y^2 = 3$.
- Find $(x, y) \in \mathbb{Z}^2$ satisfying $x^2 + y^2 = -3$.

Examples

- Find $(x, y) \in \mathbb{Q}^2$ satisfying $x^2 - 5y^2 = 3$.
- Find $(x, y) \in \mathbb{Z}^2$ satisfying $x^2 + y^2 = -3$.
- Find $(x, y, z) \in \mathbb{Z}^3$ satisfying $x^2 - 5y^2 = 3z^2$. This is a *homogeneous* equation of degree 2.

Examples

- Find $(x, y) \in \mathbb{Q}^2$ satisfying $x^2 - 5y^2 = 3$.
- Find $(x, y) \in \mathbb{Z}^2$ satisfying $x^2 + y^2 = -3$.
- Find $(x, y, z) \in \mathbb{Z}^3$ satisfying $x^2 - 5y^2 = 3z^2$. This is a *homogeneous* equation of degree 2.

Examples

- Find $(x, y) \in \mathbb{Q}^2$ satisfying $x^2 - 5y^2 = 3$.
- Find $(x, y) \in \mathbb{Z}^2$ satisfying $x^2 + y^2 = -3$.
- Find $(x, y, z) \in \mathbb{Z}^3$ satisfying $x^2 - 5y^2 = 3z^2$. This is a *homogeneous* equation of degree 2.
- Given an integer $n \geq 3$, find all $(x, y, z) \in \mathbb{Z}^2$ satisfying $x^n + y^n = z^n$. This is the famous Fermat equation.

Non-Examples

Non-Examples

- $n! = m(m+1)$ is not a Diophantine equation in the above sense, because of the factorial.

Non-Examples

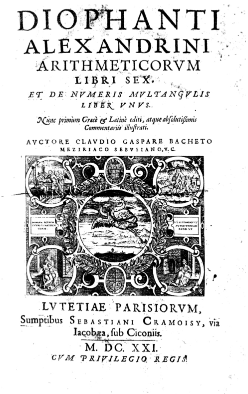
- $n! = m(m+1)$ is not a Diophantine equation in the above sense, because of the factorial.
- $x^x y^y = z^z$ is a very interesting equation, but not polynomial in the variables, so not Diophantine.

Non-Examples

- $n! = m(m+1)$ is not a Diophantine equation in the above sense, because of the factorial.
- $x^x y^y = z^z$ is a very interesting equation, but not polynomial in the variables, so not Diophantine.
- $\pi x + ey + \pi^e z = 0$ is not Diophantine, because the coefficients are irrational.

History

A 16th century edition of “Arithmetica” by Diophantus of Alexandria, translated into Latin:



DIOPHANTI
ALEXANDRINI
ARITHMETICORVM
LIBRI SEX.
ET DE NVMERIS MVLTANGVLIS
LIBER VNVS.
Nunc primùm Græcè & Latinè editi, atque absolutissimis Commentariis illustrati.
AVCTORE CLAVDIO GASPARE BACHETO MEZIRIACO SEBVSIANO, V.C.

LVTETIAE PARISIORVM,
Sumptibus SEBASTIANI CRAMOISY, via Iacobæa, sub Ciconiis.
M. DC. XXI.
CVM PRIVILEGIO REGIS.

We want to find rational solutions to $x^2 - 5y^2 = 3$ or, equivalently, integral solutions to $x^2 - 5y^2 = 3z^2$ with $z \neq 0$.

Idea: Consider the equation $x^2 - 5y^2 = 3z^2$ modulo 3:

$$x^2 - 5y^2 \equiv 0 \pmod 3 \quad \Rightarrow$$

Idea: Consider the equation $x^2 - 5y^2 = 3z^2$ modulo 3:

$$x^2 - 5y^2 \equiv 0 \pmod{3} \quad \Rightarrow \quad x \equiv y \equiv 0 \pmod{3}$$

Idea: Consider the equation $x^2 - 5y^2 = 3z^2$ modulo 3:

$$\begin{aligned} x^2 - 5y^2 \equiv 0 \pmod 3 \quad &\Rightarrow \quad x \equiv y \equiv 0 \pmod 3 \\ &\Rightarrow \quad x^2 \equiv y^2 \equiv 0 \pmod 9 \end{aligned}$$

Idea: Consider the equation $x^2 - 5y^2 = 3z^2$ modulo 3:

$$\begin{aligned} x^2 - 5y^2 \equiv 0 \pmod 3 \quad &\Rightarrow \quad x \equiv y \equiv 0 \pmod 3 \\ &\Rightarrow \quad x^2 \equiv y^2 \equiv 0 \pmod 9 \\ &\Rightarrow \quad z \equiv 0 \pmod 3 \end{aligned}$$

Idea: Consider the equation $x^2 - 5y^2 = 3z^2$ modulo 3:

$$\begin{aligned} x^2 - 5y^2 \equiv 0 \pmod{3} \quad &\Rightarrow \quad x \equiv y \equiv 0 \pmod{3} \\ &\Rightarrow \quad x^2 \equiv y^2 \equiv 0 \pmod{9} \\ &\Rightarrow \quad z \equiv 0 \pmod{3} \\ &\Rightarrow \quad x^2 - 5y^2 \equiv 0 \pmod{27} \\ &\Rightarrow \quad \ldots \end{aligned}$$

Since x and y cannot be divisible by arbitrarily large powers of 3, we obtain a contradiction, so there are no integer solutions to $x^2 - 5y^2 = 3z^2$.

This is the **method of infinite descent**, due to Pierre de Fermat.

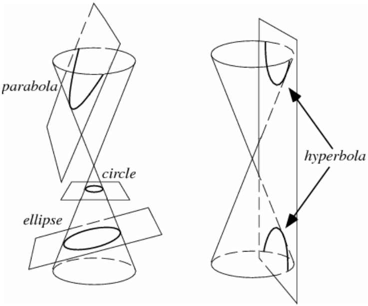
Moral of the story: for an equation to have integer solutions, it must have solutions modulo p^n for any prime number p and any $n \in \mathbb{N}$. It must also have real solutions.

Theorem (H. Minkowski): A homogeneous equation of degree 2 has an integer solution *if and only if* it has a real solution and solutions modulo all prime powers. In other words, the obvious necessary conditions are also sufficient.

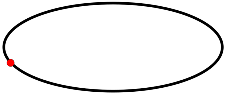
Theorem (H. Minkowski): A homogeneous equation of degree 2 has an integer solution *if and only if* it has a real solution and solutions modulo all prime powers. In other words, the obvious necessary conditions are also sufficient.
We say that equations of degree 2 satisfy the **Hasse principle**.

Theorem (H. Minkowski): A homogeneous equation of degree 2 has an integer solution *if and only if* it has a real solution and solutions modulo all prime powers. In other words, the obvious necessary conditions are also sufficient.
We say that equations of degree 2 satisfy the **Hasse principle**.
This reduces the decision problem to a finite computation, since given an equation, the above condition will be automatically satisfied for almost all primes.

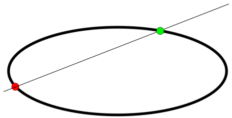
Moreover, a quadratic equation in two variables has either no rational solutions or infinitely many. Once we find one, we find them all:



Moreover, a quadratic equation in two variables has either no rational solutions or infinitely many. Once we find one, we find them all:



Moreover, a quadratic equation in two variables has either no rational solutions or infinitely many. Once we find one, we find them all:



Equations of higher degree often do not satisfy the Hasse principle.

Equations of higher degree often do not satisfy the Hasse principle.
Famous example, due to Ernst Selmer:

$$3x^3 + 4y^3 + 5z^3 = 0$$

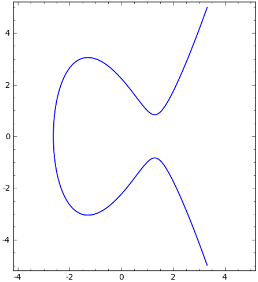
has a non-zero solution in the reals and non-zero solutions modulo all prime powers, but no integral solutions!

Equations of degree 3 differ from those of degree 2 in many other ways. E.g. an equation of the form $y^2 = x^3 + ax + b$, $a, b \in \mathbb{Q}$, can have 0, or finitely many, or infinitely many solutions.

An equation of the form

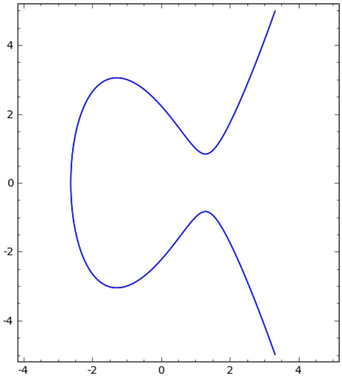
$$E:\ y^2 = x^3 + ax + b,\quad a, b \in \mathbb{Q}$$

describes an elliptic curve.



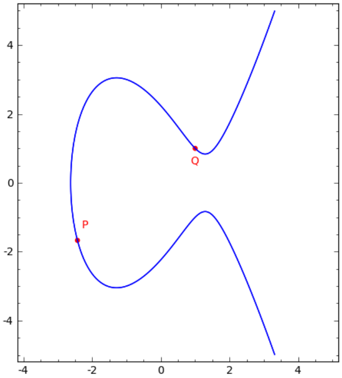
Addition law on elliptic curves

Given a point on the curve E, we cannot quite repeat the conic trick for finding a new point, but given two points, we can find a third one:



Addition law on elliptic curves

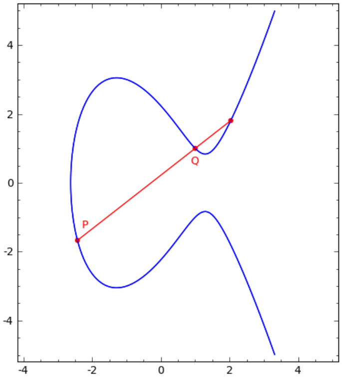
Given a point on the curve E, we cannot quite repeat the conic trick for finding a new point, but given two points, we can find a third one:



What is a Diophantine equation
The Hasse principle
Elliptic curves
Birch and Swinnerton-Dyer conjecture
Unique factorisation

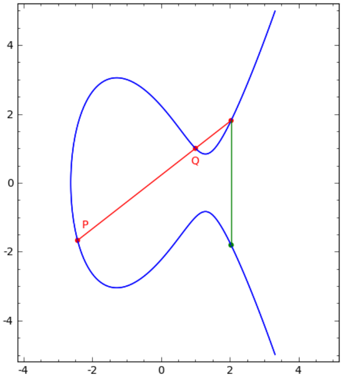
Addition law on elliptic curves

Given a point on the curve E, we cannot quite repeat the conic trick for finding a new point, but given two points, we can find a third one:



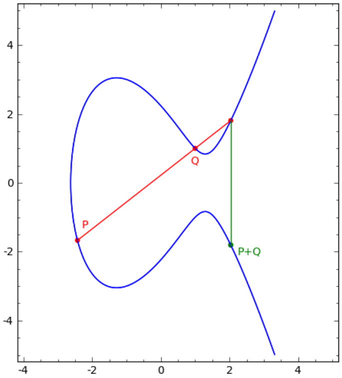
Addition law on elliptic curves

Given a point on the curve E, we cannot quite repeat the conic trick for finding a new point, but given two points, we can find a third one:



Addition law on elliptic curves

Given a point on the curve E, we cannot quite repeat the conic trick for finding a new point, but given two points, we can find a third one:



Under this operation, the set of rational points on the elliptic curve becomes an abelian group, denoted by $E(\mathbb{Q})$.

Under this operation, the set of rational points on the elliptic curve becomes an abelian group, denoted by $E(\mathbb{Q})$.

Theorem (Mordell): Given any elliptic curve E, the group $E(\mathbb{Q})$ is finitely generated. Thus, it is isomorphic to $\Delta \oplus \mathbb{Z}^{r(E)}$, where Δ is a finite abelian group, and $r(E) \geq 0$.

The integer $r(E)$ is called the *rank* of E and is a very mysterious invariant.

One important ingredient in the proof of Mordell's theorem is Fermat's technique of infinite descent. This technique has been vastly generalised.

Even though elliptic curves do not satisfy the Hasse principle, we can still try to count solutions modulo primes. Denote the number of solutions modulo p by $N_E(p)$. It turns out that $N_E(p) = p + 1 - a_p$, where

$$|a_p| \leq 2\sqrt{p}.$$

So, $N_e(p) \sim p$ as $p \to \infty$.

In the 1960s, Bryan Birch and Peter Swinnerton-Dyer computed

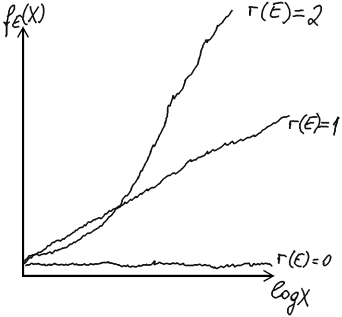
$$f_E(X) = \prod_{p \leq X} \frac{N_E(p)}{p}$$

for large X and for many curves E. They plotted the points for various X on logarithmic paper and obtained plots like this one:

In the 1960s, Bryan Birch and Peter Swinnerton-Dyer computed

$$f_E(X) = \prod_{p \leq X} \frac{N_E(p)}{p}$$

for large X and for many curves E. They plotted the points for various X on logarithmic paper and obtained plots like this one:



Birch and Swinnerton-Dyer conjecture

This led them to conjecture that

$$f_E(X) \sim c_E(\log X)^{r(E)}.$$

This is the naive form of the famous Birch and Swinnerton-Dyer conjecture. It is a very deep kind of local-global principle, of which the Hasse principle is the simplest example.

Integral points on elliptic curves

Suppose that we want to find integer solutions to

$$y^2 = x^3 - 2.$$

Integral points on elliptic curves

Suppose that we want to find integer solutions to

$$y^2 = x^3 - 2.$$

Idea: Work in the slightly bigger ring $R = \mathbb{Z}[\sqrt{-2}] = \{a + b\sqrt{-2} \mid a, b \in \mathbb{Z}\}$.

What is a Diophantine equation

The Hasse principle

Elliptic curves

Birch and Swinnerton-Dyer conjecture

Unique factorisation

Factorise

$$x^3 = y^2 + 2 = (y + \sqrt{-2})(y - \sqrt{-2}).$$

Factorise

$$x^3 = y^2 + 2 = (y + \sqrt{-2})(y - \sqrt{-2}).$$

Step 1. Show that the two factors $(y + \sqrt{-2})$ and $(y - \sqrt{-2})$ are coprime in the ring $R = \mathbb{Z}[\sqrt{-2}]$.

Factorise

$$x^3 = y^2 + 2 = (y + \sqrt{-2})(y - \sqrt{-2}).$$

Step 1. Show that the two factors $(y + \sqrt{-2})$ and $(y - \sqrt{-2})$ are coprime in the ring $R = \mathbb{Z}[\sqrt{-2}]$.
Step 2. Deduce that $(y + \sqrt{-2}) = u \cdot \alpha^3$ for a unit $u \in R^\times$ and some $\alpha = a + b\sqrt{-2} \in R$. But the only units in R are ± 1 and they are both cubes, so can be incorporated into α.

Factorise

$$x^3 = y^2 + 2 = (y + \sqrt{-2})(y - \sqrt{-2}).$$

Step 1. Show that the two factors $(y + \sqrt{-2})$ and $(y - \sqrt{-2})$ are coprime in the ring $R = \mathbb{Z}[\sqrt{-2}]$.
Step 2. Deduce that $(y + \sqrt{-2}) = u \cdot \alpha^3$ for a unit $u \in R^\times$ and some $\alpha = a + b\sqrt{-2} \in R$. But the only units in R are ± 1 and they are both cubes, so can be incorporated into α.
Step 3. Expand and equate coefficients to find the only solutions are $b = 1$, $a = \pm 1$, which correspond to $x = 3$, $y = \pm 5$.

This method depended on two facts about the ring R:

This method depended on two facts about the ring R:

- We needed to know the units of that ring.

This method depended on two facts about the ring R:

- We needed to know the units of that ring.
- We implicitly used in Step 2 that in R, any element can be factorised uniquely into irreducibles, just like in $\mathbb{Z}$.

If we tried to do this for the equation

$$y^2 = x^3 - 1,$$

working in the ring $\mathbb{Z}[\sqrt{-1}]$, then we would have to be careful with the units, since there are the additional units $\pm i$ (they are still all cubes, but in other circumstances they might not be). In fact, if $d > 0$ is square-free and congruent to 3 modulo 4, then $\mathbb{Z}[\sqrt{d}]$ has infinitely many units!

If we tried to do this for the equation

$$y^2 = x^3 - 1,$$

working in the ring $\mathbb{Z}[\sqrt{-1}]$, then we would have to be careful with the units, since there are the additional units $\pm i$ (they are still all cubes, but in other circumstances they might not be). In fact, if $d > 0$ is square-free and congruent to 3 modulo 4, then $\mathbb{Z}[\sqrt{d}]$ has infinitely many units!
If we tried to do this for the equation

$$y^2 = x^3 - 6,$$

then things would go completely wrong, since the ring $\mathbb{Z}[\sqrt{-6}]$ does not have unique factorisation into irreducibles.

The rings we considered above are called rings of integers of quadratic fields. If we adjoin square roots of negative elements, then the field is called imaginary quadratic. Otherwise, it is real quadratic.

The rings we considered above are called rings of integers of quadratic fields. If we adjoin square roots of negative elements, then the field is called imaginary quadratic. Otherwise, it is real quadratic.

The failure of unique factorisation is measured by a certain abelian group, called the class group of the ring. The class group is 1 if and only if such a a ring has unique factorisation.

There are lots of difficult questions one can ask about class groups.

The rings we considered above are called rings of integers of quadratic fields. If we adjoin square roots of negative elements, then the field is called imaginary quadratic. Otherwise, it is real quadratic.

The failure of unique factorisation is measured by a certain abelian group, called the class group of the ring. The class group is 1 if and only if such a a ring has unique factorisation.

There are lots of difficult questions one can ask about class groups.

Open question: Are there infinitely many real quadratic fields, whose ring of integers has unique factorisation?

For imaginary quadratic fields, Kurt Heegner, a German high school teacher, determined the finite list of those whose rings of integers have trivial class group in 1952.

For imaginary quadratic fields, Kurt Heegner, a German high school teacher, determined the finite list of those whose rings of integers have trivial class group in 1952.
To do that, he introduced a new idea, which was later used by Bryan Birch to produce rational points on elliptic curves. These so-called Heegner points were then used in the 80's in a series of difficult papers by many people to prove a special case of the Birch and Swinnerton-Dyer conjecture in 1990.