Lecture 2

Fermat's little theorem

Recall the Euler function

$$\varphi(n) = n \cdot \prod_{p|n}(1 - \frac{1}{p})$$

Fermat's little theorem

Recall the Euler function

$$\varphi(n) = n \cdot \prod_{p|n}(1 - \frac{1}{p})$$

How to compute it?

Fermat's little theorem

Recall the Euler function

$$\varphi(n) = n \cdot \prod_{p|n} (1 - \frac{1}{p})$$

How to compute it? We need to factor n, which is a hard problem.

Fermat's little theorem

Recall the Euler function

$$\varphi(n) = n \cdot \prod_{p|n}(1 - \frac{1}{p})$$

How to compute it? We need to factor n, which is a hard problem.

$$a^{\varphi(n)} \equiv 1 \pmod{n}.$$

Applications to cryptography

- A, B want to exchange messages

Applications to cryptography

- A, B want to exchange messages
- Suppose we have large (distinct) primes p, q such that
$$(p-1)(q-1) \mid ed - 1$$
for some e, d.
- Public: $N = pq, e$
- Secret: p, q, d

Applications to cryptography

- A wants to send a message $M < N$
- A computes $X := M^e \pmod{N}$ and sends it via open channels
- B computes $X^d \equiv M \pmod{N}$

Applications to cryptography

- A wants to send a message $M < N$
- A computes $X := M^e \pmod{N}$ and sends it via open channels
- B computes $X^d \equiv M \pmod{N}$

Proof:

$$(M^e)^d \equiv M^{ed} \equiv M^{r\varphi(N)+1} \equiv M \pmod{N}$$

Applications to cryptography

- A wants to send a message $M < N$
- A computes $X := M^e \pmod{N}$ and sends it via open channels
- B computes $X^d \equiv M \pmod{N}$

Proof:

$$(M^e)^d \equiv M^{ed} \equiv M^{r\varphi(N)+1} \equiv M \pmod{N}$$

This is OK if $(M, N) = 1$, which is almost always so; if not, change the message slightly.

Applications to cryptography

Security: C intercepts the message, knows N, e, needs M.

Applications to cryptography

Security: C intercepts the message, knows N, e, needs M. For this, needs to solve the congruence

$$ed \equiv 1 \pmod{\varphi(N)}.$$

Applications to cryptography

Security: C intercepts the message, knows N, e, needs M. For this, needs to solve the congruence

$$ed \equiv 1 \pmod{\varphi(N)}.$$

Unknown: $d, \varphi(N)$.

Applications to cryptography

Security: C intercepts the message, knows N, e, needs M. For this, needs to solve the congruence

$$ed \equiv 1 \pmod{\varphi(N)}.$$

Unknown: $d, \varphi(N)$. Currently, there are no fast algorithms to compute $\varphi(N)$ – one needs to factor N.

Applications to cryptography

Public key: Suppose there are $A_1, \ldots, A_m$ participants, and they want to exchange information so that it remains secret to others.

Applications to cryptography

Public key: Suppose there are $A_1, \ldots, A_m$ participants, and they want to exchange information so that it remains secret to others.

- A_i picks p_i, q_i large primes, puts $N_i = p_i q_i$, and chooses residues $e_i, d_i \pmod{\varphi(N_i)}$, with

$$e_i d_i \equiv 1 \pmod{\varphi(N_i)}.$$

Applications to cryptography

Public key: Suppose there are $A_1, \ldots, A_m$ participants, and they want to exchange information so that it remains secret to others.

- A_i picks p_i, q_i large primes, puts $N_i = p_i q_i$, and chooses residues $e_i, d_i \pmod{\varphi(N_i)}$, with

$$e_i d_i \equiv 1 \pmod{\varphi(N_i)}.$$

- The numbers (e_i, N_i) are published in yellow pages

Applications to cryptography

Public key: Suppose there are $A_1, \ldots, A_m$ participants, and they want to exchange information so that it remains secret to others.

- A_i picks p_i, q_i large primes, puts $N_i = p_i q_i$, and chooses residues $e_i, d_i \pmod{\varphi(N_i)}$, with

$$e_i d_i \equiv 1 \pmod{\varphi(N_i)}.$$

- The numbers (e_i, N_i) are published in yellow pages
- If A_i wants to send M to A_j, computes $M^{e_j} \pmod{N_j}$ and sends it.

Applications to cryptography

Public key: Suppose there are $A_1, \ldots, A_m$ participants, and they want to exchange information so that it remains secret to others.

- A_i picks p_i, q_i large primes, puts $N_i = p_i q_i$, and chooses residues $e_i, d_i \pmod{\varphi(N_i)}$, with

$$e_i d_i \equiv 1 \pmod{\varphi(N_i)}.$$

- The numbers (e_i, N_i) are published in yellow pages
- If A_i wants to send M to A_j, computes $M^{e_j} \pmod{N_j}$ and sends it.
- To decode, A_j computes

$$(M^{e_j})^{d_j} \equiv M^{e_j d_j} \equiv M^{r\varphi(N_j)+1} \equiv M \pmod{N_j}.$$

Equations

- $3x + 5 = 0$

Equations

- $3x + 5 = 0$
- $x^2 - Dy^2 = 1$

Equations

- $3x + 5 = 0$
- $x^2 - Dy^2 = 1$
- $x^2 + y^2 = z^2$

Equations

- $3x + 5 = 0$
- $x^2 - Dy^2 = 1$
- $x^2 + y^2 = z^2$
- $3x^3 + 4y^3 = 5z^3$

Equations

- $3x + 5 = 0$
- $x^2 - Dy^2 = 1$
- $x^2 + y^2 = z^2$
- $3x^3 + 4y^3 = 5z^3$
- $x^3 + 4y^3 = 25z^3 + 10t^3$

Equations

- $3x + 5 = 0$
- $x^2 - Dy^2 = 1$
- $x^2 + y^2 = z^2$
- $3x^3 + 4y^3 = 5z^3$
- $x^3 + 4y^3 = 25z^3 + 10t^3$
- $x^4 + 2y^4 = z^4 + 4t^4$

Basic questions

- Existence of solutions in $\mathbb{Z}$ or $\mathbb{Q}$?

Basic questions

- Existence of solutions in $\mathbb{Z}$ or $\mathbb{Q}$?
- Qualitative description of the set of solutions: finite, dense?

Basic questions

- Existence of solutions in $\mathbb{Z}$ or $\mathbb{Q}$?
- Qualitative description of the set of solutions: finite, dense?
- Quantitative description: how many solutions?

Diophantus of Alexandria

Solutions in $\mathbb{Z}$ of

$$x^2 + y^2 = z^2$$

are given by

$$x = 2mn$$
$$y = m^2 - n^2$$
$$z = m^2 + n^2$$

with $m, n \in \mathbb{Z}$.

Pell's equation: $x^2 - Dy^2 = 1, \quad D > 0$

$D = 61 \quad x = 1766319049 \quad y = 226153980$

$D = 63 \quad x = 8 \quad y = 1$

$D = 73 \quad x = 2281249 \quad y = 267000$

$D = 97 \quad x = 62809633 \quad y = 6377352$

$D = 99 \quad x = 10 \quad y = 1$

Cubic equations

$$y^2 = x^3 + Ax + B, \quad A, B \in \mathbb{Z}$$

Cubic equations

$$y^2 = x^3 + Ax + B, \quad A, B \in \mathbb{Z}$$

If (x_1, y_1) and (x_2, y_2), with $x_1 \neq x_2$, are solutions then so is (x_3, y_3) with

$$x_3 := -x_1 - x_2 + \delta^2$$
$$y_3 = \delta(x_1 - x_3) - y_1,$$

where

$$\delta := \frac{y_1 - y_2}{x_1 - x_2}.$$

Cubic equations

$$y^2 = x^3 + Ax + B, \quad A, B \in \mathbb{Z}$$

If (x_1, y_1) and (x_2, y_2), with $x_1 \neq x_2$, are solutions then so is (x_3, y_3) with

$$x_3 := -x_1 - x_2 + \delta^2$$
$$y_3 = \delta(x_1 - x_3) - y_1,$$

where

$$\delta := \frac{y_1 - y_2}{x_1 - x_2}.$$

In particular, if $x_1, y_1, x_2, y_2 \in \mathbb{Q}$ then also x_3, y_3.

More equations

- Euler (1769):

$$x^4 + y^4 + z^4 = t^4$$

  has no nontrivial solutions.

More equations

- Euler (1769):

$$x^4 + y^4 + z^4 = t^4$$

  has no nontrivial solutions.
  (Elkies, 1998):

$$2682440^4 + 15365639^4 + 18796760^4 = 20615673^4$$

- Swinnerton-Dyer (2001):

$$x^4 + 2y^4 = z^4 + 4t^4$$

  has no nontrivial solutions.

More equations

- Euler (1769):

$$x^4 + y^4 + z^4 = t^4$$

has no nontrivial solutions.
(Elkies, 1998):

$$2682440^4 + 15365639^4 + 18796760^4 = 20615673^4$$

- Swinnerton-Dyer (2001):

$$x^4 + 2y^4 = z^4 + 4t^4$$

has no nontrivial solutions.
(Elsenhans/Jahnel, 2004):

$$484801^4 + 2 \cdot 1203120^4 = 1169407^4 + 4 \cdot 1157520^4$$

More equations

Sums of cubes (a problem of Mordell):

$$x^3 + y^3 + z^3 = k.$$

More equations

Sums of cubes (a problem of Mordell):

$$x^3 + y^3 + z^3 = k.$$

Sutherland-Booker 2020:

$$569936821221962380720^3 + (-569936821113563493509)^3$$

$$+(-472715493453327032)^3 = 3,$$

More equations

Sums of cubes (a problem of Mordell):

$$x^3 + y^3 + z^3 = k.$$

Sutherland-Booker 2020:

$$569936821221962380720^3 + (-569936821113563493509)^3$$

$$+(-472715493453327032)^3 = 3,$$

The only other solutions are $(1, 1, 1)$ and $(4, 4, -5)$.

More equations

Sums of cubes (a problem of Mordell):

$$x^3 + y^3 + z^3 = k.$$

Sutherland-Booker 2020:

$$569936821221962380720^3 + (-569936821113563493509)^3$$

$$+(-472715493453327032)^3 = 3,$$

The only other solutions are $(1,1,1)$ and $(4,4,-5)$.

We implemented these improvements on Charity Engine's global compute grid of 500,000 volunteer PCs and found new representations for several values of k, including $k = 3$ and $k = 42$.

Solving diophantine equations

Theorem (Legendre)

The equation

$$ax^2 + by^2 = cz^2, \quad a, b, c \in \mathbb{N}, \text{ squarefree, coprime}$$

is solvable in $\mathbb{Z}$ iff it is solvable modulo p, for all primes p.

First instance of the Hasse principle (local-global principle).

Proof

(1) $x^2 + y^2 = z^2$ is solvable: $(2mn, m^2 - n^2, m^2 + n^2)$

Proof

(1) $x^2 + y^2 = z^2$ is solvable: $(2mn, m^2 - n^2, m^2 + n^2)$

(2) If $p \mid c$ and (x_0, y_0, z_0) is a nontrivial solution then $x_0, y_0 \not\equiv 0 \pmod{p}$.

Proof

(1) $x^2 + y^2 = z^2$ is solvable: $(2mn, m^2 - n^2, m^2 + n^2)$

(2) If $p \mid c$ and (x_0, y_0, z_0) is a nontrivial solution then $x_0, y_0 \not\equiv 0 \pmod{p}$. Thus we can express

$$ax^2 + by^2 \equiv \frac{a}{y_0}(xy_0 + yx_0)(xy_0 - yx_0) \pmod{p}$$

$$ax^2 + by^2 - cz^2 \equiv L_p(x, y, z)M_p(x, y, z) \pmod{p}$$

with linear L_p and M_p, for all p.

Proof

(1) $x^2 + y^2 = z^2$ is solvable: $(2mn, m^2 - n^2, m^2 + n^2)$

(2) If $p \mid c$ and (x_0, y_0, z_0) is a nontrivial solution then $x_0, y_0 \not\equiv 0 \pmod{p}$. Thus we can express

$$ax^2 + by^2 \equiv \frac{a}{y_0}(xy_0 + yx_0)(xy_0 - yx_0) \pmod{p}$$

$$ax^2 + by^2 - cz^2 \equiv L_p(x, y, z)M_p(x, y, z) \pmod{p}$$

with linear L_p and M_p, for all p. Same holds for $p \mid abc$.

Proof

(1) $x^2 + y^2 = z^2$ is solvable: $(2mn, m^2 - n^2, m^2 + n^2)$

(2) If $p \mid c$ and (x_0, y_0, z_0) is a nontrivial solution then $x_0, y_0 \not\equiv 0 \pmod{p}$. Thus we can express

$$ax^2 + by^2 \equiv \frac{a}{y_0}(xy_0 + yx_0)(xy_0 - yx_0) \pmod{p}$$

$$ax^2 + by^2 - cz^2 \equiv L_p(x, y, z)M_p(x, y, z) \pmod{p}$$

with linear L_p and M_p, for all p. Same holds for $p \mid abc$.

(3) By the Chinese Remainder Theorem we find

$$ax^2 + by^2 - cz^2 \equiv L(x, y, z)M(x, y, z) \pmod{abc}$$

Proof

(4) Now consider the box

$$\mathcal{B} := \begin{cases} 0 \leq x < \sqrt{bc} \\ 0 \leq y < \sqrt{ac} \\ 0 \leq z < \sqrt{ab} \end{cases}$$

Proof

(4) Now consider the box

$$\mathcal{B} := \begin{cases} 0 \le x < \sqrt{bc} \\ 0 \le y < \sqrt{ac} \\ 0 \le z < \sqrt{ab} \end{cases}$$

Since $\gcd(a, b) = 1, \ldots,$ none of the $\sqrt{ab}, \sqrt{ac}, \sqrt{bc}$ is an integer. It follows that

$$\#\text{ lattice points in } \mathcal{B} > \sqrt{ab}\sqrt{ac}\sqrt{bc} = abc.$$

Proof

(4) Now consider the box

$$\mathcal{B} := \begin{cases} 0 \leq x < \sqrt{bc} \\ 0 \leq y < \sqrt{ac} \\ 0 \leq z < \sqrt{ab} \end{cases}$$

Since $\gcd(a, b) = 1$, ..., none of the $\sqrt{ab}, \sqrt{ac}, \sqrt{bc}$ is an integer. It follows that

$$\# \text{ lattice points in } \mathcal{B} > \sqrt{ab}\sqrt{ac}\sqrt{bc} = abc.$$

Thus there exist (x_1, y_1, z_1) and (x_2, y_2, z_2) such that

$$L(x_1, y_1, z_1) \equiv L(x_2, y_2, z_2) \pmod{abc}$$

Proof

(5) Put

$$x_0 = x_1 - x_2, \quad y_0 := y_1 - y_2, \quad z_0 := z_1 - z_2.$$

Proof

(5) Put

$$x_0 = x_1 - x_2, \quad y_0 := y_1 - y_2, \quad z_0 := z_1 - z_2.$$

We have

$$|x_0| \leq \sqrt{bc}, \quad |y_0| \leq \sqrt{ac}, \quad |z_0| \leq \sqrt{ab}$$

and

$$ax_0^2 + by_0^2 - cz_0^2 \equiv 0 \pmod{abc}.$$

Proof

At the same time

$$-abc < ax_0^2 + by_0^2 - cz_0^2 < 2abc.$$

Proof

At the same time

$$-abc < ax_0^2 + by_0^2 - cz_0^2 < 2abc.$$

Either

$$ax_0^2 + by_0^2 - cz_0^2 = 0 \quad \text{or} \quad ax_0^2 + by_0^2 - cz_0^2 = abc.$$

Proof

At the same time

$$-abc < ax_0^2 + by_0^2 - cz_0^2 < 2abc.$$

Either

$$ax_0^2 + by_0^2 - cz_0^2 = 0 \quad \text{or} \quad ax_0^2 + by_0^2 - cz_0^2 = abc.$$

In the second case,

$$a(x_0z_0 + by_0)^2 + b(y_0 - ax_0)^2 - c(z_0^2 - ab)^2 = 0$$

which is a nontrivial solution since $z_0^2 = ab$ is not possible by coprimality.

Reichard's equation

Application of Quadratic reciprocity: if p, q are odd primes then

$$\left(\frac{p}{q}\right) = \left(\frac{q}{p}\right) \cdot (-1)^{\frac{p-1}{2} \cdot \frac{q-1}{2}}$$

Reichard's equation

Application of Quadratic reciprocity: if p, q are odd primes then

$$\left(\frac{p}{q}\right) = \left(\frac{q}{p}\right) \cdot (-1)^{\frac{p-1}{2} \cdot \frac{q-1}{2}}$$

Theorem

The equation

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

is solvable modulo all primes, and in the reals, but not in $\mathbb{Z}$.

Reichard's equation: proof

We may assume that $\gcd(x, y, z) = 1$. Recall that

$$\left(\frac{2}{17}\right) = 1.$$

Reichard's equation: proof

We may assume that $\gcd(x, y, z) = 1$. Recall that

$$\left(\frac{2}{17}\right) = 1.$$

For all primes p dividing z we have a congruence

$$x^4 \equiv 17y^4 \pmod{p}$$

i.e.,

$$\left(\frac{p}{17}\right) = 1 \quad \Rightarrow \quad \left(\frac{17}{p}\right) = 1.$$

Reichard's equation: proof

It follows that z is a square modulo 17,

$$z \equiv z_1^2 \pmod{17}.$$

Reichard's equation: proof

It follows that z is a square modulo 17,

$$z \equiv z_1^2 \pmod{17}.$$

Then

$$x^4 \equiv 2z_1^4 \pmod{17} \Rightarrow x^{16} \equiv 16 \cdot y^{16} \pmod{17}$$

Reichard's equation: proof

It follows that z is a square modulo 17,

$$z \equiv z_1^2 \pmod{17}.$$

Then

$$x^4 \equiv 2z_1^4 \pmod{17} \Rightarrow x^{16} \equiv 16 \cdot y^{16} \pmod{17}$$

This is a contradiction, as $1 \not\equiv -1 \pmod{17}$.

Diagonal cubics

Now consider similar equations of higher degree:

$$ax^3 + by^3 = cz^3.$$

- no local-global principle

Diagonal cubics

Now consider similar equations of higher degree:

$$ax^3 + by^3 = cz^3.$$

- no local-global principle
- no effective algorithm to decide solvability

Diagonal cubics

Now consider similar equations of higher degree:

$$ax^3 + by^3 = cz^3.$$

- no local-global principle
- no effective algorithm to decide solvability
- the set of solutions could be finite or infinite

Diagonal cubics

Now consider similar equations of higher degree:

$$ax^3 + by^3 = cz^3.$$

- no local-global principle
- no effective algorithm to decide solvability
- the set of solutions could be finite or infinite

Selmer's example:

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

is solvable modulo all primes and in $\mathbb{R}$ but not $\mathbb{Z}$.

Fermat's last theorem, for $n = 3$

Lemma (Euler 1768)

If $(a, b) = 1$ and $a^2 + 3b^2 = m^3$ then there exist $s, t \in \mathbb{Z}$ such that

$$a = s(s^2 - 9t^2) \quad b = 3t(s^2 - t^2).$$

Proof

We have

$$\underbrace{a^2 + 3b^2}_{\text{cube}} = \underbrace{(a + b\sqrt{-3})}_{\text{cube?}} \cdot \underbrace{(a - b\sqrt{-3})}_{\text{cube?}}$$

Proof

We have

$$\underbrace{a^2 + 3b^2}_{\text{cube}} = \underbrace{(a + b\sqrt{-3})}_{\text{cube?}} \cdot \underbrace{(a - b\sqrt{-3})}_{\text{cube?}}$$

If so, then put

$$a + b\sqrt{-3} = (s + t\sqrt{-3})^3.$$

Then

$$\underbrace{(s^2 - 9st^2)}_{a} + \underbrace{(3s^2t - 3t^2)}_{b}\sqrt{-3}$$

Issues

But is this true?

NO:

$$4 = 2 \cdot 2 = (1 + \sqrt{-3}) \cdot (1 - \sqrt{-3}).$$

Issues

But is this true?

NO:

$$4 = 2 \cdot 2 = (1 + \sqrt{-3}) \cdot (1 - \sqrt{-3}).$$

However, it is true for the ring

$$\mathbb{Z}[\frac{1 + \sqrt{-3}}{2}].$$

To understand this, we need theory – algebraic number theory.

Fermat's last theorem, for $n = 3$

Assuming Euler's lemma, consider

$$x^3 + y^3 = z^3.$$

Fermat's last theorem, for $n = 3$

Assuming Euler's lemma, consider

$$x^3 + y^3 = z^3.$$

We may assume that

- x, y, z are pairwise coprime

Fermat's last theorem, for $n = 3$

Assuming Euler's lemma, consider

$$x^3 + y^3 = z^3.$$

We may assume that

- x, y, z are pairwise coprime
- $x \equiv 0 \pmod 2$ and $y, z \equiv 1 \pmod 2$

Fermat's last theorem, for $n = 3$

Assuming Euler's lemma, consider

$$x^3 + y^3 = z^3.$$

We may assume that

- x, y, z are pairwise coprime
- $x \equiv 0 \pmod 2$ and $y, z \equiv 1 \pmod 2$
- $|x|$ is minimal, $x = 2u$

Fermat's last theorem, for $n = 3$

Assuming Euler's lemma, consider

$$x^3 + y^3 = z^3.$$

We may assume that

- x, y, z are pairwise coprime
- $x \equiv 0 \pmod 2$ and $y, z \equiv 1 \pmod 2$
- $|x|$ is minimal, $x = 2u$
- $p := (z + y)/2$, $q := (z - y)/2$, both in $\mathbb{Z}$, $(p, q) = 1$, if one of them is even, the other is odd.

Fermat's last theorem, for $n = 3$

$$\begin{aligned} x^3 = z^3 - y^3 &= \left((p+q)^3 - (p-q)^3\right) \\ &= 6p^2q + 2q^3 = 2q(q^2 + 3p^2) \end{aligned}$$

Fermat's last theorem, for $n = 3$

$$x^3 = z^3 - y^3 = \left((p+q)^3 - (p-q)^3\right)$$
$$= 6p^2q + 2q^3 = 2q(q^2 + 3p^2)$$

$$\Rightarrow u^3 = \frac{q}{4}(\underbrace{q^2 + 2p^2}_{\text{odd}})$$
$$\Rightarrow q \equiv 0 \pmod 4, p \equiv 1 \pmod 2$$

$$(\frac{q}{4}, q^2 + 3p^2) = 1 \Leftrightarrow (q, \underbrace{3p^2}_{(q^2+3p^2)-q^2}) = 1 \Leftrightarrow q \not\equiv 0 \pmod 3$$

Fermat's last theorem, for $n = 3$

Case 1.

If $q \not\equiv 0 \pmod 3$ then $q/4$ and $q^2 + 3p^2$ are cubes, by Euler's lemma, we have

$$q = s(s^2 - 9t^2), \quad p = 3t(s^2 - t^2) \quad \text{odd.}$$

Fermat's last theorem, for $n = 3$

Case 1.

If $q \not\equiv 0 \pmod 3$ then $q/4$ and $q^2 + 3p^2$ are cubes, by Euler's lemma, we have

$$q = s(s^2 - 9t^2), \quad p = 3t(s^2 - t^2) \quad \text{odd}.$$

It follows that t is odd, s is even, $(s, t) = 1$.

Fermat's last theorem, for $n = 3$

Case 1.

If $q \not\equiv 0 \pmod 3$ then $q/4$ and $q^2 + 3p^2$ are cubes, by Euler's lemma, we have

$$q = s(s^2 - 9t^2), \quad p = 3t(s^2 - t^2) \quad \text{odd.}$$

It follows that t is odd, s is even, $(s, t) = 1$. Then $2q = 8q/4$ is also a cube. Thus

$$2s(s^2 - 9t^2) = 2s(s - 3t)(s + 3t) \quad \text{also cube.}$$

Fermat's last theorem, for $n = 3$

Case 1.

If $q \not\equiv 0 \pmod 3$ then $q/4$ and $q^2 + 3p^2$ are cubes, by Euler's lemma, we have

$$q = s(s^2 - 9t^2), \quad p = 3t(s^2 - t^2) \quad \text{odd.}$$

It follows that t is odd, s is even, $(s, t) = 1$. Then $2q = 8q/4$ is also a cube. Thus

$$2s(s^2 - 9t^2) = 2s(s - 3t)(s + 3t) \quad \text{also cube.}$$

Since $q \not\equiv 0 \pmod 3$, we have

$$(2s, s - 3t) = (2s, s + 3t) = (s - 3t, s + 3t) = 1.$$

Fermat's last theorem, for $n = 3$

Thus there exist x_1, y_1, z_1 such that

$$x_1^3 = 2s, \quad y_1^3 = -(s + 3t), \quad z_1^3 = (s - 3t)$$

which implies that

$$x_1^3 + y_1^3 = z_1^3, \quad x_1 \equiv 0 \pmod 2$$

Fermat's last theorem, for $n = 3$

Thus there exist x_1, y_1, z_1 such that

$$x_1^3 = 2s, \quad y_1^3 = -(s+3t), \quad z_1^3 = (s-3t)$$

which implies that

$$x_1^3 + y_1^3 = z_1^3, \quad x_1 \equiv 0 \pmod 2$$

But

$$x^3 = 2q(q^2+3p^2) \Rightarrow |\underbrace{q}_{s(s^2-9t^2)}| < |x^3/2|,$$

thus

$$|x_1|^3 = 2|s| < |x|^3,$$

which contradicts the assumption that x is minimal.

Fermat's last theorem, for $n = 3$

Thus there exist x_1, y_1, z_1 such that

$$x_1^3 = 2s, \quad y_1^3 = -(s + 3t), \quad z_1^3 = (s - 3t)$$

which implies that

$$x_1^3 + y_1^3 = z_1^3, \quad x_1 \equiv 0 \pmod 2$$

But

$$x^3 = 2q(q^2 + 3p^2) \Rightarrow |\underbrace{q}_{s(s^2-9t^2)}| < |x^3/2|,$$

thus

$$|x_1|^3 = 2|s| < |x|^3,$$

which contradicts the assumption that x is minimal. This is an instance of infinite descent.

Fermat's last theorem, for $n = 3$

Case 2.

$$q = 3r, \quad r \equiv 0 \pmod 4$$

Fermat's last theorem, for $n = 3$

Case 2.

$$q = 3r, \quad r \equiv 0 \pmod 4$$

Then

$$u^3 = \frac{3}{4}r(9r^2 + 3p^2) = \frac{9}{4}r(3r^2 + p^2)$$

Fermat's last theorem, for $n = 3$

Case 2.

$$q = 3r, \quad r \equiv 0 \pmod 4)$$

Then

$$u^3 = \frac{3}{4}r(9r^2 + 3p^2) = \frac{9}{4}r(3r^2 + p^2)$$

We have

$$(\frac{9}{4}r, (3r^2 + p^2)) = 1,$$

and both are cubes.

Fermat's last theorem, for $n = 3$

Case 2.

$$q = 3r, \quad r \equiv 0 \pmod 4)$$

Then

$$u^3 = \frac{3}{4}r(9r^2 + 3p^2) = \frac{9}{4}r(3r^2 + p^2)$$

We have

$$(\frac{9}{4}r, (3r^2 + p^2)) = 1,$$

and both are cubes. By Euler's lemma

$$p = s(s^2 - 9t^2), \quad r = 3t(s^2 - t^2)$$

with t even and s odd.

Fermat's last theorem, for $n = 3$

Thus

$$\frac{8}{27} \cdot \frac{9}{4} \cdot r = \frac{2}{3} r = 2t(s^2 - t^2) \qquad\qquad 2t(s+t)(s-t)$$

and the factors are coprime, thus all cubes.

Fermat's last theorem, for $n = 3$

Thus

$$\frac{8}{27} \cdot \frac{9}{4} \cdot r = \frac{2}{3} r = 2t(s^2 - t^2) \qquad\qquad 2t(s+t)(s-t)$$

and the factors are coprime, thus all cubes.

As before, there exist x_1, y_1, z_1 such that

$$x_1^3 = 2t, \quad y_1^3 = s - t, \quad z_1^3 = s + t$$

with

$$x_1^3 + y_1^3 = z_1^3$$

and

$$|x_1|^3 < 2|t| \leq \frac{2}{3}|r| = \frac{2}{9}|q| < 2|q| < |x|^3,$$

contradiction.

Diophantine equations

Let $f \in \mathbb{Z}[t, x_1, \ldots, x_n]$. Consider

$$f(t, x_1, \ldots, x_n) = 0,$$

either as an equation in the unknowns $t, x_1, \ldots, x_n$ or as an algebraic family of equations in $x_1, \ldots x_n$ parametrized by $t \in \mathbb{Z}$.
Examples:

- $x^2 + r(t)y^2 = q(t)z^2$, with $r, q \in \mathbb{Z}[t]$
- $x^3 + y^3 = tz^3$
- $x^3 + y^3 + z^3 = t$ (e.g., $t = 3$)

Hilbert's problems, Paris 1900

10.

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 (1970), Matiyasevich-Robinson (1975)

Theorem

The set of $t \in \mathbb{Z}$ such that $f(t, \ldots, x_n) = 0$ is solvable is not decidable, i.e., there is no algorithm to decide whether or not a diophantine equation is solvable in integers.

Matiyasevich (1970), Matiyasevich-Robinson (1975)

Theorem

The set of $t \in \mathbb{Z}$ such that $f(t, \ldots, x_n) = 0$ is solvable is not decidable, i.e., there is no algorithm to decide whether or not a diophantine equation is solvable in integers.

Theorem

There exists an $f \in \mathbb{Z}[t_1, t_2, x_0, \ldots, x_n]$, with $n \leq 13$, such that $f(a, n, z_0, \cdots, z_n) = 0$ for some $z_0, \cdots, z_n \in \mathbb{N}$ iff $a \in \mathcal{D}_n$, where $\mathcal{D}_0, \mathcal{D}_1, \cdots$ is a list of all recursively enumerable $\mathcal{D}_j \subset \mathbb{N}$.

Conjecture: $n \leq 3$.

Matiyasevich (1970), Matiyasevich-Robinson (1975)

The solubility of diophantine equations is not decidable.

Matiyasevich (1970), Matiyasevich-Robinson (1975)

The solubility of diophantine equations is not decidable.

There is a single equation

$$F(t, x_1, \ldots, x_n) = 0$$

with coefficients in $\mathbb{Z}$, which is equivalent to all of (formal mathematics): the statement $\#t$ is provable if and only if the above equation is solvable in $x_1, \ldots, x_n \in \mathbb{Z}$.

G. Chaitin (1993)

Theorem

The set of $t \in \mathbb{Z}$ such that $f_t = 0$ has infinitely many primitive solutions is algorithmically random.

Abstract: *One normally thinks that everything that is true is true for a reason. I've found mathematical truths that are true for no reason at all. These mathematical truths are beyond the power of mathematical reasoning because they are accidental and random. Using software written in Mathematica that runs on an IBM RS/6000 workstation, I constructed a perverse 200-page algebraic equation with a parameter t and 17,000 unknowns. For each whole-number value of the parameter t, we ask whether this equation has a finite or an infinite number of whole number solutions. The answers escape the power of mathematical reason because they are completely random and accidental.*

Points

- Basic rings: R

$$\mathbb{F}_p = \mathbb{Z}/p\mathbb{Z}, \mathbb{Z} \quad \text{or} \quad \mathbb{C}[t] \ldots$$

Points

- Basic rings: R

$$\mathbb{F}_p = \mathbb{Z}/p\mathbb{Z}, \mathbb{Z} \quad \text{or} \quad \mathbb{C}[t]...$$

- Basic geometric objects: $\mathbb{A}^n$ and $\mathbb{P}^n = \left(\mathbb{A}^{n+1} \setminus 0\right)/\mathbb{G}_m$

Points

- Basic rings: R

$$\mathbb{F}_p = \mathbb{Z}/p\mathbb{Z}, \mathbb{Z} \quad \text{or} \quad \mathbb{C}[t]...$$

- Basic geometric objects: $\mathbb{A}^n$ and $\mathbb{P}^n = \left(\mathbb{A}^{n+1} \setminus 0\right)/\mathbb{G}_m$
- Varieties: $X^{\text{affine}} \subset \mathbb{A}^n$ (system of polynomial equations with coefficients in R), resp. $X^{\text{projective}} \subset \mathbb{P}^n$ (system of homogeneous polynomial equations with coefficients in R)

Points

- Basic rings: R

$$\mathbb{F}_p = \mathbb{Z}/p\mathbb{Z}, \mathbb{Z} \quad \text{or} \quad \mathbb{C}[t]...$$

- Basic geometric objects: $\mathbb{A}^n$ and $\mathbb{P}^n = \left(\mathbb{A}^{n+1} \setminus 0\right)/\mathbb{G}_m$
- Varieties: $X^{\text{affine}} \subset \mathbb{A}^n$ (system of polynomial equations with coefficients in R), resp. $X^{\text{projective}} \subset \mathbb{P}^n$ (system of homogeneous polynomial equations with coefficients in R)
- R-valued points: $X^{\text{affine}}(R)$, resp. $X^{\text{projective}}(R)$. Note

$$X^{\text{projective}}(\mathbb{Z}) = X^{\text{projective}}(\mathbb{Q}).$$

Points

- Basic rings: R

$$\mathbb{F}_p = \mathbb{Z}/p\mathbb{Z}, \mathbb{Z} \quad \text{or} \quad \mathbb{C}[t]...$$

- Basic geometric objects: $\mathbb{A}^n$ and $\mathbb{P}^n = \left(\mathbb{A}^{n+1} \setminus 0\right)/\mathbb{G}_m$
- Varieties: $X^{\text{affine}} \subset \mathbb{A}^n$ (system of polynomial equations with coefficients in R), resp. $X^{\text{projective}} \subset \mathbb{P}^n$ (system of homogeneous polynomial equations with coefficients in R)
- R-valued points: $X^{\text{affine}}(R)$, resp. $X^{\text{projective}}(R)$. Note

$$X^{\text{projective}}(\mathbb{Z}) = X^{\text{projective}}(\mathbb{Q}).$$

- for now: work projectively
- first nontrivial variety: $X_f := \{f(x) = 0\} \subset \mathbb{P}^n$, a hypersurface

Dimension 1

Basic invariant: dimension

$$ax^r + by^r + cz^r = 0,$$

with $a, b, c \in \mathbb{Z}$, $abc \neq 0$, and $r \geq 2$.

Dimension 1

Basic invariant: dimension

$$ax^r + by^r + cz^r = 0,$$

with $a, b, c \in \mathbb{Z}$, $abc \neq 0$, and $r \geq 2$.

- $r = 2$ – no solutions or infinitely many solutions

Dimension 1

Basic invariant: dimension

$$ax^r + by^r + cz^r = 0,$$

with $a, b, c \in \mathbb{Z}$, $abc \neq 0$, and $r \geq 2$.

- $r = 2$ – no solutions or infinitely many solutions
- $r = 3$ – none, finitely many or infinitely many solutions

Dimension 1

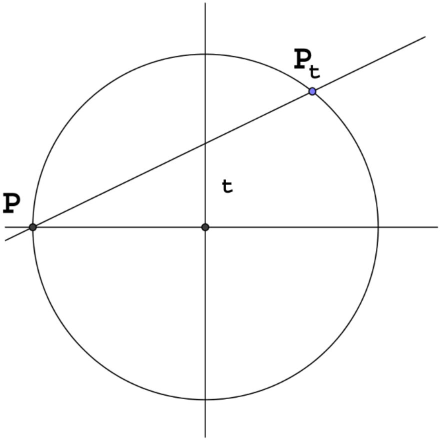
Basic invariant: dimension

$$ax^r + by^r + cz^r = 0,$$

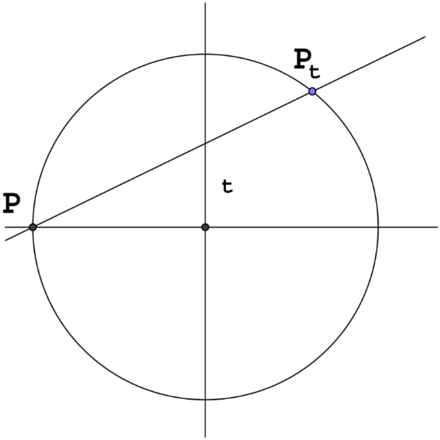
with $a, b, c \in \mathbb{Z}$, $abc \neq 0$, and $r \geq 2$.

- $r = 2$ – no solutions or infinitely many solutions
- $r = 3$ – none, finitely many or infinitely many solutions
- $r \geq 4$ – at most finitely many solutions

Conics: geometry

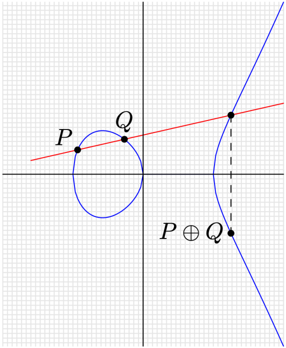


Conics: geometry



This is how one derives formulas for Pythagorean triples.

Cubic equations: geometry



This is how one adds rational points.

Dimension 2

$$ax^r + by^r = cz^r + dt^r,$$

with $a, b, c, d \in \mathbb{Z}$, $abcd \neq 0$, and $r \geq 2$.

- $r = 2$ - no solutions or a dense set of solutions

Dimension 2

$$ax^r + by^r = cz^r + dt^r,$$

with $a, b, c, d \in \mathbb{Z}$, $abcd \neq 0$, and $r \geq 2$.

- $r = 2$ - no solutions or a dense set of solutions
- $r = 3$ - no solutions or a dense set of solutions

Dimension 2

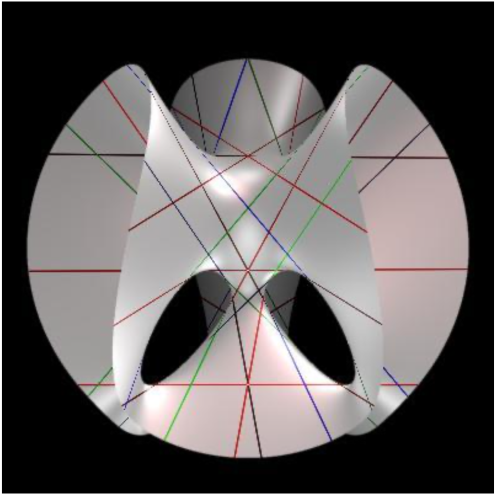
$$ax^r + by^r = cz^r + dt^r,$$

with $a, b, c, d \in \mathbb{Z}$, $abcd \neq 0$, and $r \geq 2$.

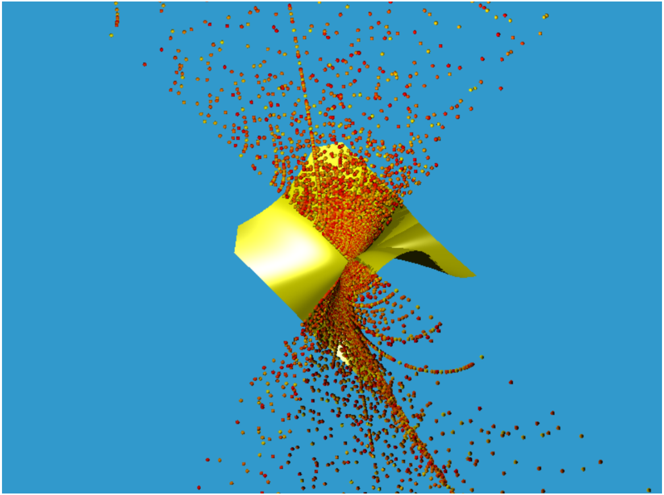
- $r = 2$ - no solutions or a dense set of solutions
- $r = 3$ - no solutions or a dense set of solutions
- $r \geq 4$ - ???

Quadric surface

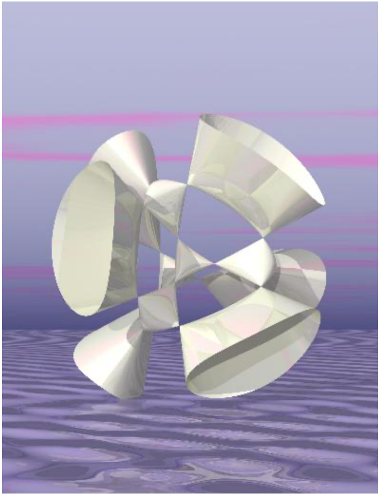
Cubic surface



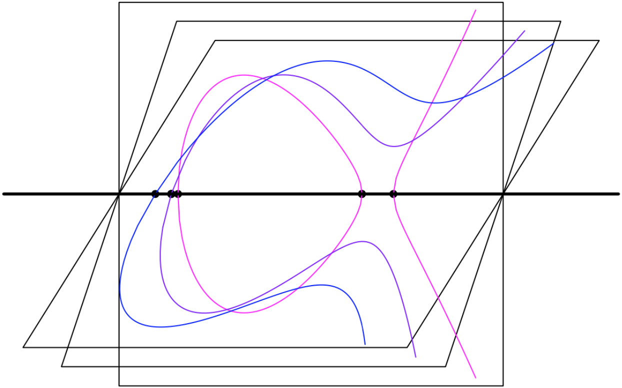
Cubic surface



Quartic surface



Quartic surface - sliced



Quartic surface - sliced

Consider

$$ax^4 + by^4 + cz^4 + dt^4 = 0$$

Assume that $abcd$ is a square in $\mathbb{Q}$ and

$$a + b + c + d = 0$$

but no two of the coefficients sum to zero. Then $\mathbb{Q}$-rational points are dense.

Special case of a general theorem of Bogomolov-T., worked out by Logan, McKinnon, van Luijk in 2010.