Lecture 3

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

There are no nontrivial solutions to

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

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 $n = 3$

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

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

$$\Rightarrow q \equiv 0 \pmod 4, p \equiv 1 \pmod 2$$

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

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.

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

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

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

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

- 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

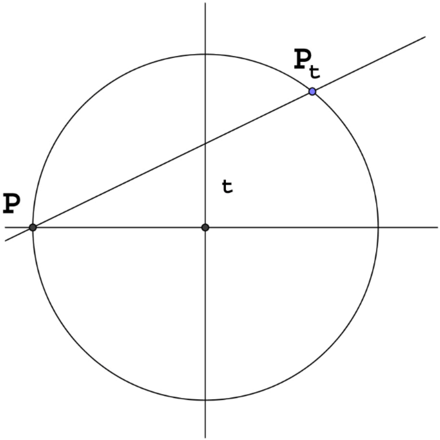
Basic invariant: dimension

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

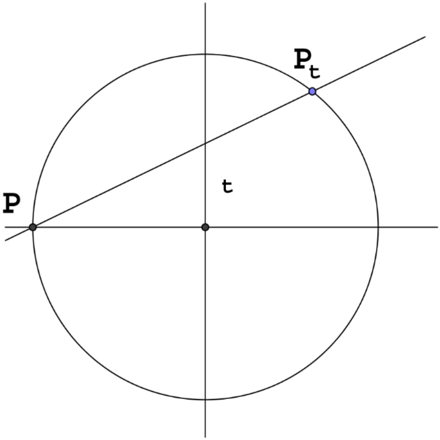
with $a, b, c \in \mathbb{Z}$, $abc \neq 0$, and $r \geq 2$.

- $r = 2$ – 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

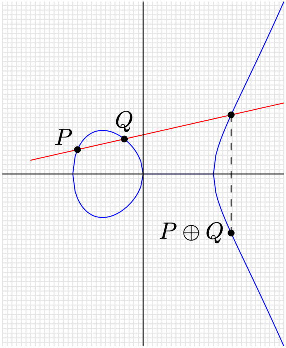


Conics: geometry



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

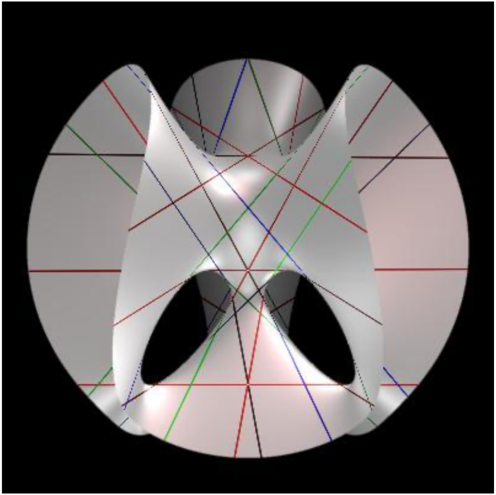
$$ax^r + by^r = cz^r + dt^r,$$

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

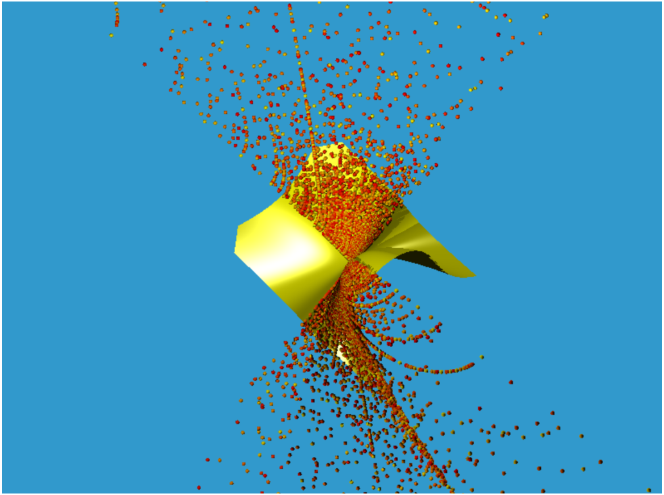
- $r = 2$ - no solutions or a dense set of solutions
- $r = 3$ - no solutions or a dense set of solutions
- $r \geq 4$ - ???

Quadric surface

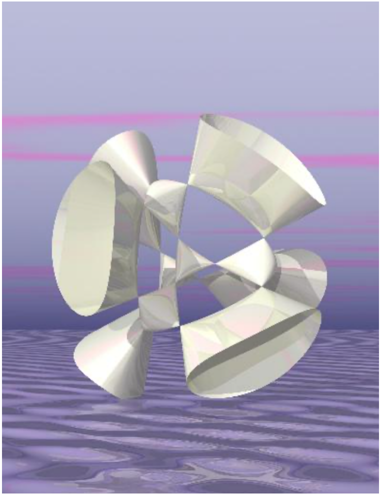
Cubic surface



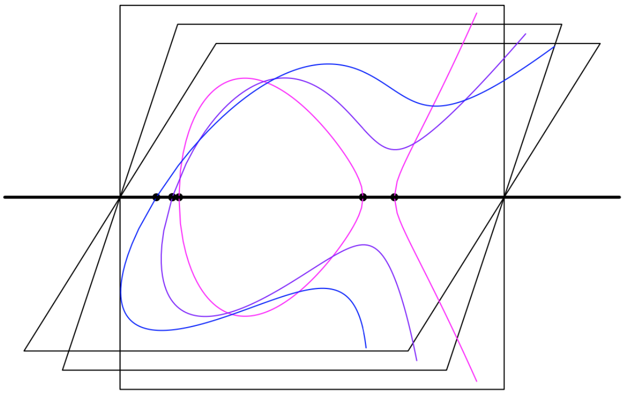
Cubic surface



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.

Reminder

Number theory studies systems of (homogeneous or inhomogeneous) equations with coefficients in $\mathbb{Z}, \mathbb{Q}$, or more general rings or fields. We will mostly focus on homogeneous equations. (Geometrically, on rational points on algebraic varieties.)

The simplest such systems consist of one equation, e.g.,

$$ax^2 + by^2 = cz^2, \quad x^3 + y^3 + z^3 = t^3, \quad \ldots$$

The corresponding varieties are called hypersurfaces.

$X_f \subset \mathbb{P}^n$ over $\mathbb{F}_q$

Consider

$$f(x_0, \ldots, x_n) = \sum_{|\mathbf{d}|=d} a_{\mathbf{d}}\, x^{\mathbf{d}},$$

in multi-index notation.

$X_f \subset \mathbb{P}^n$ over $\mathbb{F}_q$

Consider

$$f(x_0, \ldots, x_n) = \sum_{|\mathbf{d}|=d} a_{\mathbf{d}}\, x^{\mathbf{d}},$$

in multi-index notation.

Theorem [Chevalley-Warning (1936)]

If $d \leq n$ then $X(\mathbb{F}_q) \neq \emptyset$.

Proof

Step 1. $\delta-$function : $\sum_{x=1}^{p-1} x^d = \begin{cases} -1 \pmod{p} & \text{if } p-1 \mid d \\ 0 \pmod{p} & \text{if } p-1 \nmid d \end{cases}$

Proof

Step 1. $\delta -$ function : $\sum_{x=1}^{p-1} x^d = \begin{cases} -1 \pmod p & \text{if } p-1 \mid d \\ 0 \pmod p & \text{if } p-1 \nmid d \end{cases}$

Step 2. Let $\phi \in \mathbb{Z}[x_0, \ldots, x_n]$, with $\deg(\phi) \leq n(p-1)$. Then

$$\sum_{x_0,\ldots,x_n} \phi(x_0, \ldots, x_n) \equiv 0 \pmod p.$$

Proof

Step 1. $\delta -$ function : $\sum_{x=1}^{p-1} x^d = \begin{cases} -1 \pmod p & \text{if } p-1 \mid d \\ \ \ 0 \pmod p & \text{if } p-1 \nmid d \end{cases}$

Step 2. Let $\phi \in \mathbb{Z}[x_0, \ldots, x_n]$, with $\deg(\phi) \leq n(p-1)$. Then

$$\sum_{x_0,\ldots,x_n} \phi(x_0, \ldots, x_n) \equiv 0 \pmod p.$$

Proof: For monomials, we have

$$\sum_{x_0,\ldots,x_n} x_0^{d_0} \cdots x_n^{d_n} = \prod \Big(\sum x_j^{d_j}\Big), \quad \text{with} \quad d_0 + \ldots + d_n \leq n(p-1).$$

Proof

Step 1. $\delta-$ function : $\sum_{x=1}^{p-1} x^d = \begin{cases} -1 \pmod p & \text{if } p-1 \mid d \\ 0 \pmod p & \text{if } p-1 \nmid d \end{cases}$

Step 2. Let $\phi \in \mathbb{Z}[x_0, \ldots, x_n]$, with $\deg(\phi) \leq n(p-1)$. Then

$$\sum_{x_0,\ldots,x_n} \phi(x_0, \ldots, x_n) \equiv 0 \pmod p.$$

Proof: For monomials, we have

$$\sum_{x_0,\ldots,x_n} x_0^{d_0} \cdots x_n^{d_n} = \prod(\sum x_j^{d_j}), \quad \text{with} \quad d_0 + \ldots + d_n \leq n(p-1).$$

For some j, we have $0 \leq d_j < p-1$, and we apply Step 1.

Proof

Step 3. Let $f \in \mathbb{Z}[x_0, \ldots, x_n]$ with $\deg(f) \leq n$ then

$$N(f) := \#\{x \mid f(x) = 0\} \equiv 0 \pmod{p}.$$

Proof

Step 3. Let $f \in \mathbb{Z}[x_0, \dots, x_n]$ with $\deg(f) \leq n$ then

$$N(f) := \#\{x \mid f(x) = 0\} \equiv 0 \pmod{p}.$$

Proof: For $\phi(x) = 1 - f(x)^{p-1}$ we have $\deg(\phi) \leq \deg(f) \cdot (p-1)$.
Apply 2:

$$N(f) = \sum_{x_0, \dots, x_n} \phi(x).$$

Proof

Step 3. Let $f \in \mathbb{Z}[x_0, \ldots, x_n]$ with $\deg(f) \leq n$ then

$$N(f) := \#\{x \mid f(x) = 0\} \equiv 0 \pmod{p}.$$

Proof: For $\phi(x) = 1 - f(x)^{p-1}$ we have $\deg(\phi) \leq \deg(f) \cdot (p-1)$. Apply 2:

$$N(f) = \sum_{x_0, \ldots, x_n} \phi(x).$$

Step 4. The homogeneous equation $f(x) = 0$ has a trivial solution. It follows that

$$N(f) > 1 \quad \text{and} \quad X_f(\mathbb{F}_p) \neq \emptyset.$$

$X_f \subset \mathbb{P}^n$ over $\mathbb{Q}$

Theorem [Birch (1961)]

If

$$n \geq (\deg(f) - 1) \cdot 2^{\deg(f)},$$

and f is smooth, then X_f satisfies the local-global (Hasse) principle.

$X_f \subset \mathbb{P}^n$ over $\mathbb{Q}$

Theorem [Birch (1961)]

If

$$n \geq (\mathrm{deg}(f) - 1) \cdot 2^{\mathrm{deg}(f)},$$

and f is smooth, then X_f satisfies the local-global (Hasse) principle.

Moreover:

- asymptotic formulas

$X_f \subset \mathbb{P}^n$ over $\mathbb{Q}$

Theorem [Birch (1961)]

If

$$n \geq (\deg(f) - 1) \cdot 2^{\deg(f)},$$

and f is smooth, then X_f satisfies the local-global (Hasse) principle.

Moreover:

- asymptotic formulas
- better bounds for n for small $\deg(f)$

Heuristic

- Given: $f \in \mathbb{Z}[x_0, \ldots, x_n]$ homogeneous of degree $d = \deg(f)$.

Heuristic

- Given: $f \in \mathbb{Z}[x_0, \ldots, x_n]$ homogeneous of degree $d = \deg(f)$.
- We have $|f(x)| = O(B^d)$, for $\|x\| := \max_j(|x_j|) \leq B$.

Heuristic

- Given: $f \in \mathbb{Z}[x_0, \ldots, x_n]$ homogeneous of degree $d = \deg(f)$.
- We have $|f(x)| = O(B^d)$, for $\|x\| := \max_j(|x_j|) \leq B$.
- May (?) assume that the probability of $f(x) = 0$ is B^{-d}.

Heuristic

- Given: $f \in \mathbb{Z}[x_0, \ldots, x_n]$ homogeneous of degree $d = \deg(f)$.
- We have $|f(x)| = O(B^d)$, for $\|x\| := \max_j(|x_j|) \leq B$.
- May (?) assume that the probability of $f(x) = 0$ is B^{-d}.
- There are B^{n+1} "events" with $\|x\| \leq B$.

Heuristic

- Given: $f \in \mathbb{Z}[x_0, \ldots, x_n]$ homogeneous of degree $d = \deg(f)$.
- We have $|f(x)| = O(B^d)$, for $\|x\| := \max_j(|x_j|) \leq B$.
- May (?) assume that the probability of $f(x) = 0$ is B^{-d}.
- There are B^{n+1} "events" with $\|x\| \leq B$.
- We expect B^{n+1-d} solutions with $\|x\| \leq B$.

Heuristic

- Given: $f \in \mathbb{Z}[x_0, \ldots, x_n]$ homogeneous of degree $d = \deg(f)$.
- We have $|f(x)| = O(B^d)$, for $\|x\| := \max_j(|x_j|) \leq B$.
- May (?) assume that the probability of $f(x) = 0$ is B^{-d}.
- There are B^{n+1} "events" with $\|x\| \leq B$.
- We expect B^{n+1-d} solutions with $\|x\| \leq B$.

Hope: reasonable at least when $n + 1 - d \geq 0$.

Circle method I

- δ-function:

$$\int_0^1 e^{2\pi i\alpha f(x)}d\alpha = \begin{cases} 1 & f(x)=0 \\ 0 & f(x)\neq 0 \end{cases}$$

Circle method I

- δ-function:

$$\int_0^1 e^{2\pi i \alpha f(x)} d\alpha = \begin{cases} 1 & f(x) = 0 \\ 0 & f(x) \neq 0 \end{cases}$$

- $N(f, B) := \#\{x \in \mathbb{Z}^{n+1} \mid f(x) = 0, \ \ \|x\| \leq B\}$

Circle method I

- δ-function:

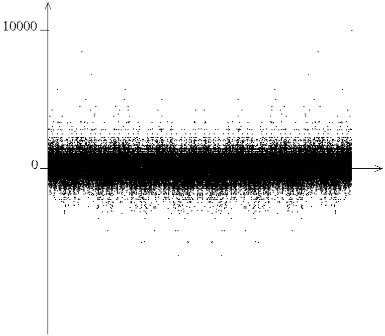
$$\int_0^1 e^{2\pi i\alpha f(x)} d\alpha = \begin{cases} 1 & f(x) = 0 \\ 0 & f(x) \neq 0 \end{cases}$$

- $N(f, B) := \#\{x \in \mathbb{Z}^{n+1} \mid f(x) = 0, \ \ \|x\| \leq B\}$
- $$N(f, B) := \sum_{\|x\| \leq B} \int_0^1 e^{2\pi i\alpha f(x)} d\alpha = \int_0^1 S(\alpha) d\alpha,$$

  where

$$S(\alpha) := \sum_{\|x\| \leq B} e^{2\pi i\alpha f(x)}$$

Circle method II: $S(\alpha)$



Circle method III

- major arcs $\mathfrak{M} := \bigcup_{(a,q)=1, q \le B^{\Delta}} \mathfrak{M}_{a,q}$, where

$$\mathfrak{M}_{a,q} := \{\alpha \,|\, |\alpha - \frac{a}{q}| \le B^{-d-\delta}\}.$$

Circle method III

- major arcs $\mathfrak{M} := \bigcup_{(a,q)=1, q \le B^\Delta} \mathfrak{M}_{a,q}$, where

$$\mathfrak{M}_{a,q} := \{\alpha \,|\, |\alpha - \frac{a}{q}| \le B^{-d-\delta}\}.$$

- minor arcs: $\mathfrak{m} := [0,1] \setminus \mathfrak{M}$

Circle method III

- major arcs $\mathfrak{M} := \bigcup_{(a,q)=1, q \leq B^{\Delta}} \mathfrak{M}_{a,q}$, where

$$\mathfrak{M}_{a,q} := \{\alpha \,|\, |\alpha - \frac{a}{q}| \leq B^{-d-\delta}\}.$$

- minor arcs: $\mathfrak{m} := [0,1] \setminus \mathfrak{M}$
- **Goal:**

$$\int_{\mathfrak{m}} S(\alpha) d\alpha = O(B^{n+1-d-\epsilon}),$$

Circle method III

- major arcs $\mathfrak{M} := \bigcup_{(a,q)=1, q \leq B^{\Delta}} \mathfrak{M}_{a,q}$, where
$$\mathfrak{M}_{a,q} := \{\alpha \,|\, |\alpha - \frac{a}{q}| \leq B^{-d-\delta}\}.$$
- minor arcs: $\mathfrak{m} := [0,1] \setminus \mathfrak{M}$
- **Goal:**
$$\int_{\mathfrak{m}} S(\alpha) d\alpha = O(B^{n+1-d-\epsilon}),$$
$$\int_{\mathfrak{M}} S(\alpha) d\alpha \sim \prod_{p} \tau_p \cdot \tau_{\infty} \cdot B^{n+1-d} \quad \text{for} \quad B \to \infty$$

Circle method III

- major arcs $\mathfrak{M} := \bigcup_{(a,q)=1, q \le B^{\Delta}} \mathfrak{M}_{a,q}$, where

$$\mathfrak{M}_{a,q} := \{\alpha \,|\, |\alpha - \frac{a}{q}| \le B^{-d-\delta}\}.$$

- minor arcs: $\mathfrak{m} := [0,1] \setminus \mathfrak{M}$
- **Goal:**

$$\int_{\mathfrak{m}} S(\alpha) d\alpha = O(B^{n+1-d-\epsilon}),$$

$$\int_{\mathfrak{M}} S(\alpha) d\alpha \sim \prod_p \tau_p \cdot \tau_\infty \cdot B^{n+1-d} \quad \text{for} \quad B \to \infty$$

- Input: Weyl's bounds (1916), e.g, $|\sum_{1 \le x \le B} e^{2\pi i \alpha x^d}|$ "small" when $|\alpha - a/q|$ "large".

$X_f \subset \mathbb{P}^n$ over $\mathbb{C}(t)$

Theorem

If $d = \deg(f) \leq n$ then $X_f(\mathbb{C}(t)) \neq \emptyset$.

$X_f \subset \mathbb{P}^n$ over $\mathbb{C}(t)$

Theorem

If $d = \deg(f) \leq n$ then $X_f(\mathbb{C}(t)) \neq \emptyset$.

Proof: Insert $x_j = x_j(t) \in \mathbb{C}[t]$, of degree e, into

$$f = \sum_{|\mathbf{d}|=d} f_{\mathbf{d}} x^{\mathbf{d}} = 0.$$

This gives a system of $e \cdot d + \mathrm{const}$ equations in $e(n+1)$ variables.

$X_f \subset \mathbb{P}^n$ over $\mathbb{C}(t)$

Theorem

If $d = \deg(f) \leq n$ then $X_f(\mathbb{C}(t)) \neq \emptyset$.

Proof: Insert $x_j = x_j(t) \in \mathbb{C}[t]$, of degree e, into

$$f = \sum_{|\mathbf{d}|=d} f_{\mathbf{d}} x^{\mathbf{d}} = 0.$$

This gives a system of $e \cdot d + \mathrm{const}$ equations in $e(n+1)$ variables. This system is solvable for $e \gg 0$, provided $d \leq n$.

Classification

- Low-degree (Fano varieties) – many rational points

Classification

- Low-degree (Fano varieties) – many rational points
- Intermediate

Classification

- Low-degree (Fano varieties) – many rational points
- Intermediate
- High-degree (varieties of general type) – few rational points

Main results

- Mordell's conjecture /Faltings' theorem: curves of general type have finitely many rational points. E.g., any (smooth) curve in $\mathbb{P}^2$, with equation

$$f_d(x_0, x_1, x_2) = 0, \quad d = \deg(f) \geq 4,$$

has only finitely many rational points.

Main results

- Mordell's conjecture /Faltings' theorem: curves of general type have finitely many rational points. E.g., any (smooth) curve in $\mathbb{P}^2$, with equation

$$f_d(x_0, x_1, x_2) = 0, \quad d = \deg(f) \geq 4,$$

has only finitely many rational points.

- Surfaces of low degree, e.g., cubic surfaces

$$x^3 + y^3 = x^3 + t^3$$

are understood, all have (potentially) dense sets of rational points.

Main results

- Mordell's conjecture /Faltings' theorem: curves of general type have finitely many rational points. E.g., any (smooth) curve in $\mathbb{P}^2$, with equation

$$f_d(x_0, x_1, x_2) = 0, \quad d = \deg(f) \geq 4,$$

  has only finitely many rational points.

- Surfaces of low degree, e.g., cubic surfaces

$$x^3 + y^3 = x^3 + t^3$$

  are understood, all have (potentially) dense sets of rational points.

- Fano threefolds (Harris, Bogomolov, T.): all have (potentially) dense sets of rational points, with the possible exception of

$$w^2 = f(x_0, x_1, x_2, x_3), \quad \deg(f) = 6.$$

Summary

- (nontrivial) solutions of homogeneous equations over fields F give F-rational points $X(F)$ on corresponding projective algebraic varieties X

Summary

- (nontrivial) solutions of homogeneous equations over fields F give F-rational points $X(F)$ on corresponding projective algebraic varieties X
- properties of the sets $X(F)$ reflect the geometric/algebraic complexity of X (e.g., dimension, degree) and the structure of F (e.g., topology, analytic structure)

Analytic structure

How does one pass from number theory to geometry?

Analytic structure

How does one pass from number theory to geometry? By viewing

$$\mathbb{Q} \hookrightarrow \mathbb{R}, \mathbb{C}.$$

Analytic structure

How does one pass from number theory to geometry? By viewing

$$\mathbb{Q} \hookrightarrow \mathbb{R}, \mathbb{C}.$$

Are there other possibilities?

Analytic structure

How does one pass from number theory to geometry? By viewing

$$\mathbb{Q} \hookrightarrow \mathbb{R}, \mathbb{C}.$$

Are there other possibilities? Indeed, there are: p-adic numbers!

Ordered abelian groups

$(\Gamma, +)$

Examples: $\Gamma = \mathbb{Z}, \mathbb{Q}, \mathbb{R}$

Ordered abelian groups

$(\Gamma, +)$

Examples: $\Gamma = \mathbb{Z}, \mathbb{Q}, \mathbb{R}$

$$\Gamma_\infty := \Gamma \cup \{\infty\}$$

$$\gamma + \infty = \infty + \infty = \infty \quad \forall \gamma \in \Gamma$$

Valuations

Let F be a field, e.g., $\mathbb{Q}$, $\mathbb{C}(t)$. A valuation with value group Γ is a map

$$\nu : F \to \Gamma_\infty$$

such that

- ν is a surjective homomorphism on $F^\times$, i.e., $\nu(xy) = \nu(x) + \nu(y)$ for all $x, y \in F^\times$.

Valuations

Let F be a field, e.g., $\mathbb{Q}$, $\mathbb{C}(t)$. A valuation with value group Γ is a map

$$\nu : F \to \Gamma_\infty$$

such that

- ν is a surjective homomorphism on $F^\times$, i.e., $\nu(xy) = \nu(x) + \nu(y)$ for all $x, y \in F^\times$.
- the triangle inequality holds:

$$\nu(x+y) \geq \min(\nu(x), \nu(y)), \quad \forall x, y,$$

- $$\nu(0) = \infty.$$

Valuations: Example $F = \mathbb{Q}$

$$\nu_p : \mathbb{Z} \setminus 0 \hookrightarrow \mathbb{R}, \quad n = p^{\nu_p(n)} \cdot n', \quad \text{with } (n', p) = 1$$

$$\nu_p : \mathbb{Q} \hookrightarrow \mathbb{R} \cup \{\infty\}$$

$$\nu_p(\frac{a}{b}) = \nu_p(a) - \nu_p(b),$$

$$\Gamma = \mathbb{Z}.$$

Valuations: Example $F = \mathbb{C}(x)$

$$\nu : \mathbb{C}[x] \setminus 0 \hookrightarrow \mathbb{Z},$$

$$f = \sum_{n=0}^{N} a_n x^n$$

Valuations: Example $F = \mathbb{C}(x)$

$$\nu : \mathbb{C}[x] \setminus 0 \hookrightarrow \mathbb{Z},$$

$$f = \sum_{n=0}^{N} a_n x^n$$

$$\nu(f) = \min\{n | a_n \neq 0\}$$

$$\nu(\frac{f}{g}) = \nu(f) - \nu(g)$$

$$\Gamma = \mathbb{Z}.$$

Valuations: Example $F = \mathbb{C}(x, y)$

$$\nu : \mathbb{C}[x, y] \setminus 0 \hookrightarrow \mathbb{R},$$

$$f(x, y) = \sum_{n,m \geq 0} a_{n,m} x^n y^m$$

Valuations: Example $F = \mathbb{C}(x, y)$

$$\nu : \mathbb{C}[x, y] \setminus 0 \hookrightarrow \mathbb{R},$$

$$f(x, y) = \sum_{n,m \geq 0} a_{n,m} x^n y^m$$

$$\nu(f) = \min\{n + \sqrt{5}m \,|\, a_{nm} \neq 0\}$$

$$\nu(\frac{f}{g}) = \nu(f) - \nu(g)$$

$$\Gamma = \{n + \sqrt{5}m \mid n, m \in \mathbb{Z}\} \subset \mathbb{R}.$$

Valuations: $\mathbb{Q}$

Recall the usual absolute value:

$$|x| := \begin{cases} x & x \geq 0 \\ -x & x < 0 \end{cases}$$

Valuations: $\mathbb{Q}$

Recall the usual absolute value:

$$|x| := \begin{cases} x & x \geq 0 \\ -x & x < 0 \end{cases}$$

Are there others?

Valuations: $\mathbb{Q}$

Recall the usual absolute value:

$$|x| := \begin{cases} x & x \geq 0 \\ -x & x < 0 \end{cases}$$

Are there others?

For $F = \mathbb{Q}$ consider

$$|x|_p := p^{-\nu_p(x)}.$$

We have

$$|x+y|_p \leq \max\{|x|_p, |y|_p\}, \quad |0|_p = 0.$$

The inequality is stronger!

Valuations

Theorem (Ostrovski)

Up to equivalence, these are the only valuations on $\mathbb{Q}$.

Valuations

Theorem (Ostrovski)

Up to equivalence, these are the only valuations on $\mathbb{Q}$.

Product formula

$$\prod_p |x|_p \cdot |x| = 1, \text{ for all } x \in \mathbb{Q}^\times.$$

Topology

Let F be a field, with absolute value $|\cdot|$.

Topology

Let F be a field, with absolute value $|\cdot|$. It induces a metric

$$d(x, y) := |x - y|.$$

Topology

Let F be a field, with absolute value $|\cdot|$. It induces a metric

$$d(x, y) := |x - y|.$$

Properties:

- $d(x, y) \geq 0$
- $d(x, y) = d(y, x)$
- $d(x, z) \leq d(x, y) + d(y, z)$ – triangle inequality

Topology

Let F be a field, with absolute value $|\cdot|$. It induces a metric

$$d(x, y) := |x - y|.$$

Properties:

- $d(x, y) \geq 0$
- $d(x, y) = d(y, x)$
- $d(x, z) \leq d(x, y) + d(y, z)$ – triangle inequality

This defines the structure of a metric space, F is a topological field.

Topology

For $F = \mathbb{Q}$ and $d = |\cdot|_p$ we have the stronger inequality

$$d(x,z) \leq \max\{d(x,y), d(y,z)\},$$

the corresponding space is called ultra-metric.

Topology

For $F = \mathbb{Q}$ and $d = |\cdot|_p$ we have the stronger inequality

$$d(x,z) \leq \max\{d(x,y), d(y,z)\},$$

the corresponding space is called ultra-metric.
We have the notions of intervals or balls:

$$\mathcal{B}(a,r) := \{x \in F \mid d(x,a) < r\} \subset \overline{\mathcal{B}}(a,r) := \{x \in F \mid d(x,a) \leq r\},$$

Topology: $\mathbb{Q}$

Let $F = \mathbb{Q}$ and $|\cdot| = |\cdot|_p$. Then

$$\overline{\mathcal{B}}(0,1) = \mathcal{B}(0,1) \cup \mathcal{B}(1,1) \cup \ldots \cup \mathcal{B}(p-1,1),$$

so that $\bar{\mathcal{B}}$ are open and closed.

Topology: $\mathbb{Q}$

Let $F = \mathbb{Q}$ and $|\cdot| = |\cdot|_p$. Then

$$\overline{\mathcal{B}}(0,1) = \mathcal{B}(0,1) \cup \mathcal{B}(1,1) \cup \ldots \cup \mathcal{B}(p-1,1),$$

so that $\bar{\mathcal{B}}$ are open and closed.

Example: Show that in $\mathbb{Q}$, $|\cdot|_5$ one has

$$\mathcal{B}(1,1) = \mathcal{B}(1,\frac{1}{2}) = \overline{\mathcal{B}}(1,\frac{1}{5})$$

Topology

For ultrametric absolute values, we have

- $b \in \mathcal{B}(a, r) \Rightarrow \mathcal{B}(a, r) = \mathcal{B}(b, r)$

Topology

For ultrametric absolute values, we have

- $b \in \mathcal{B}(a, r) \Rightarrow \mathcal{B}(a, r) = \mathcal{B}(b, r) \quad$ (same for $\bar{\mathcal{B}}$)

Topology

For ultrametric absolute values, we have

- $b \in \mathcal{B}(a,r) \Rightarrow \mathcal{B}(a,r) = \mathcal{B}(b,r)$ (same for $\bar{\mathcal{B}}$)
- $a, b \in F, r, s \in \mathbb{R}_{\geq 0} \Rightarrow$ If

$$\mathcal{B}(a,r) \cap \mathcal{B}(b,s) \neq \emptyset$$

then either

$$\mathcal{B}(a,r) \subseteq \mathcal{B}(b,s) \quad \text{or} \quad \mathcal{B}(a,r) \supseteq \mathcal{B}(b,s).$$

Valuation theory

$$\begin{aligned} \mathcal{O}_\nu &:= \overline{\mathcal{B}}(0,1) && \text{valuation ring} \\ \mathfrak{m}_\nu &:= \mathcal{B}(0,1) && \text{valuation ideal} \\ k_\nu &:= \mathcal{O}_\nu / \mathfrak{m}_\nu && \text{residue field} \end{aligned}$$

Valuation theory

$F = \mathbb{Q}$, $|\cdot|_p$. In this case

$$\mathcal{O}_\nu = \mathbb{Z}_{(p)} := \{\frac{a}{b},\ p \nmid b\}$$
$$\mathfrak{m}_\nu = p\mathbb{Z}_{(p)}$$
$$k_\nu = \mathbb{F}_p = \mathbb{Z}/p\mathbb{Z}$$

to be continued ...