Statistics of Diophantine equations

Peter Koymans
Institute for Theoretical Studies

ETH zürich

ITS Fellows Seminar

Zurich, 26 September 2023

Overview

Diophantine equations and factoring

Class groups

Pell's equation

Future work

Fermat's last theorem

Pierre de Fermat

The most well-known Diophantine equation is

$$X^n + Y^n = Z^n.$$

Fermat's last theorem

Pierre de Fermat

The most well-known Diophantine equation is

$$X^n + Y^n = Z^n.$$

Fermat handled the case $n = 4$, Euler treated $n = 3$ and Dirichlet covered $n = 5$.

Fermat's last theorem

Pierre de Fermat

The most well-known Diophantine equation is

$$X^n + Y^n = Z^n.$$

Fermat handled the case $n = 4$, Euler treated $n = 3$ and Dirichlet covered $n = 5$.

For odd n, Lamé (1847) factored the equation

$$Z^n = X^n + Y^n = (X + Y)(X + \zeta_n Y) \cdots (X + \zeta_n^{n-1} Y)$$

with ζ_n satisfying $\zeta_n^n = 1$.

Fermat's last theorem

Pierre de Fermat

The most well-known Diophantine equation is

$$X^n + Y^n = Z^n.$$

Fermat handled the case $n = 4$, Euler treated $n = 3$ and Dirichlet covered $n = 5$.

For odd n, Lamé (1847) factored the equation

$$Z^n = X^n + Y^n = (X + Y)(X + \zeta_n Y) \cdots (X + \zeta_n^{n-1} Y)$$

with ζ_n satisfying $\zeta_n^n = 1$.

These factors are essentially coprime. So by unique factorization each $X + \zeta_n^i Y$ must be an n-th power. But $X + \zeta_n^i Y = \alpha^n$ leads to a contradiction with some effort.

Fermat's last theorem

Pierre de Fermat

The most well-known Diophantine equation is

$$X^n + Y^n = Z^n.$$

Fermat handled the case $n = 4$, Euler treated $n = 3$ and Dirichlet covered $n = 5$.

For odd n, Lamé (1847) factored the equation

$$Z^n = X^n + Y^n = (X + Y)(X + \zeta_n Y) \cdots (X + \zeta_n^{n-1} Y)$$

with ζ_n satisfying $\zeta_n^n = 1$.

These factors are essentially coprime. So by unique factorization each $X + \zeta_n^i Y$ must be an n-th power. But $X + \zeta_n^i Y = \alpha^n$ leads to a contradiction with some effort.

We have proven Fermat's last theorem!

Unfortunately, not quite ...

Ernst Kummer

Consider the ring

$$\mathbb{Z}[\zeta_n] = \{a_0 + a_1\zeta_n + a_2\zeta_n^2 + \cdots + a_{n-1}\zeta_n^{n-1}\}.$$

We can formally add such expressions, and also multiply them using $\zeta_n^n = 1$.

Unfortunately, not quite ...

Ernst Kummer

Consider the ring

$$\mathbb{Z}[\zeta_n] = \{a_0 + a_1\zeta_n + a_2\zeta_n^2 + \cdots + a_{n-1}\zeta_n^{n-1}\}.$$

We can formally add such expressions, and also multiply them using $\zeta_n^n = 1$.

This ring has many similar properties as the usual integers $\mathbb{Z}$, except that it may lack unique factorization.

Unfortunately, not quite ...

Ernst Kummer

Consider the ring

$$\mathbb{Z}[\zeta_n] = \{a_0 + a_1\zeta_n + a_2\zeta_n^2 + \cdots + a_{n-1}\zeta_n^{n-1}\}.$$

We can formally add such expressions, and also multiply them using $\zeta_n^n = 1$.

This ring has many similar properties as the usual integers $\mathbb{Z}$, except that it may lack unique factorization.

The first prime number p for which $\mathbb{Z}[\zeta_p]$ does not have unique factorization is $p = 23$.

Unfortunately, not quite ...

Ernst Kummer

Consider the ring

$$\mathbb{Z}[\zeta_n] = \{a_0 + a_1\zeta_n + a_2\zeta_n^2 + \cdots + a_{n-1}\zeta_n^{n-1}\}.$$

We can formally add such expressions, and also multiply them using $\zeta_n^n = 1$.

This ring has many similar properties as the usual integers $\mathbb{Z}$, except that it may lack unique factorization.

The first prime number p for which $\mathbb{Z}[\zeta_p]$ does not have unique factorization is $p = 23$.

Kummer was able to rescue Lamé's proof by introducing ideals and studying the factorization properties of $\mathbb{Z}[\zeta_p]$.

Unfortunately, not quite ...

Ernst Kummer

Consider the ring

$$\mathbb{Z}[\zeta_n] = \{a_0 + a_1\zeta_n + a_2\zeta_n^2 + \cdots + a_{n-1}\zeta_n^{n-1}\}.$$

We can formally add such expressions, and also multiply them using $\zeta_n^n = 1$.

This ring has many similar properties as the usual integers $\mathbb{Z}$, except that it may lack unique factorization.

The first prime number p for which $\mathbb{Z}[\zeta_p]$ does not have unique factorization is $p = 23$.

Kummer was able to rescue Lamé's proof by introducing ideals and studying the factorization properties of $\mathbb{Z}[\zeta_p]$.

He was able to prove Fermat's last theorem if p does not divide the "class number".

Unfortunately, not quite ...

Ernst Kummer

Consider the ring

$$\mathbb{Z}[\zeta_n] = \{a_0 + a_1\zeta_n + a_2\zeta_n^2 + \cdots + a_{n-1}\zeta_n^{n-1}\}.$$

We can formally add such expressions, and also multiply them using $\zeta_n^n = 1$.

This ring has many similar properties as the usual integers $\mathbb{Z}$, except that it may lack unique factorization.

The first prime number p for which $\mathbb{Z}[\zeta_p]$ does not have unique factorization is $p = 23$.

Kummer was able to rescue Lamé's proof by introducing ideals and studying the factorization properties of $\mathbb{Z}[\zeta_p]$.

He was able to prove Fermat's last theorem if p does not divide the "class number".

The class number measures unique factorization.

Example of failure of unique factorization

Definition

Let R be a commutative domain. An element $\pi \in R$ is called irreducible if all divisors d of π satisfy $d = u$ or $d = \pi u$ for some unit u.

Example of failure of unique factorization

Definition

Let R be a commutative domain. An element $\pi \in R$ is called irreducible if all divisors d of π satisfy $d = u$ or $d = \pi u$ for some unit u.

Example

The irreducible elements of $\mathbb{Z}$ are exactly $\pm p$ with p a prime.

Example of failure of unique factorization

Definition

Let R be a commutative domain. An element $\pi \in R$ is called irreducible if all divisors d of π satisfy $d = u$ or $d = \pi u$ for some unit u.

Example

The irreducible elements of $\mathbb{Z}$ are exactly $\pm p$ with p a prime.

Example

Consider the ring $\mathbb{Z}[\sqrt{-6}] = \{a + b\sqrt{-6} : a, b \in \mathbb{Z}\}$. Then we have the factorization

$$6 = -\sqrt{-6} \cdot \sqrt{-6} = 2 \cdot 3.$$

These are genuinely different factorizations, since one can check that 2, 3 and $\sqrt{-6}$ are all irreducible.

Example of failure of unique factorization

Definition

Let R be a commutative domain. An element $\pi \in R$ is called irreducible if all divisors d of π satisfy $d = u$ or $d = \pi u$ for some unit u.

Example

The irreducible elements of $\mathbb{Z}$ are exactly $\pm p$ with p a prime.

Example

Consider the ring $\mathbb{Z}[\sqrt{-6}] = \{a + b\sqrt{-6} : a, b \in \mathbb{Z}\}$. Then we have the factorization

$$6 = -\sqrt{-6} \cdot \sqrt{-6} = 2 \cdot 3.$$

These are genuinely different factorizations, since one can check that 2, 3 and $\sqrt{-6}$ are all irreducible.

The root cause of this problem is that the ideals

$$I = (2, \sqrt{-6}) \supsetneq 2\mathbb{Z}[\sqrt{-6}], \quad J = (3, \sqrt{-6}) \supsetneq 2\mathbb{Z}[\sqrt{-6}]$$

of $\mathbb{Z}[\sqrt{-6}]$ are not principal. If it were, we could use it to further factor 2, 3 and $\sqrt{-6}$.

Overview

Diophantine equations and factoring

Class groups

Pell's equation

Future work

Class groups

Definition

Let R be a commutative domain. Let $I, J \subseteq R$ be ideals. We write $I \sim J$ if there exist $\alpha, \beta \in R - \{0\}$ such that

$$I \cdot (\alpha) = J \cdot (\beta).$$

The class group $\mathrm{Cl}(R)$ of R is the set of equivalence classes under $\sim$.

Class groups

Definition

Let R be a commutative domain. Let $I, J \subseteq R$ be ideals. We write $I \sim J$ if there exist $\alpha, \beta \in R - \{0\}$ such that

$$I \cdot (\alpha) = J \cdot (\beta).$$

The class group $\mathrm{Cl}(R)$ of R is the set of equivalence classes under $\sim$.

For nice rings R (Dedekind domains), this is a commutative group. Furthermore, R is an UFD if and only if $\mathrm{Cl}(R)$ is trivial.

Class groups

Definition

Let R be a commutative domain. Let $I, J \subseteq R$ be ideals. We write $I \sim J$ if there exist $\alpha, \beta \in R - \{0\}$ such that

$$I \cdot (\alpha) = J \cdot (\beta).$$

The class group $\mathrm{Cl}(R)$ of R is the set of equivalence classes under $\sim$.

For nice rings R (Dedekind domains), this is a commutative group. Furthermore, R is an UFD if and only if $\mathrm{Cl}(R)$ is trivial.

Example

We have $\mathrm{Cl}(\mathbb{Z}) = \{0\}$ and $\mathrm{Cl}(\mathbb{Z}[\sqrt{-6}]) \cong \mathbb{Z}/2\mathbb{Z}$.

Class groups

Definition

Let R be a commutative domain. Let $I, J \subseteq R$ be ideals. We write $I \sim J$ if there exist $\alpha, \beta \in R - \{0\}$ such that

$$I \cdot (\alpha) = J \cdot (\beta).$$

The class group $\mathrm{Cl}(R)$ of R is the set of equivalence classes under $\sim$.

For nice rings R (Dedekind domains), this is a commutative group. Furthermore, R is an UFD if and only if $\mathrm{Cl}(R)$ is trivial.

Example

We have $\mathrm{Cl}(\mathbb{Z}) = \{0\}$ and $\mathrm{Cl}(\mathbb{Z}[\sqrt{-6}]) \cong \mathbb{Z}/2\mathbb{Z}$.

This definition also plays a key role in other areas of mathematics (Picard group, Jacobian etc.).

Why is the class group so important?

David Hilbert

Teiji Takagi

Number theorists are really interested in describing extensions (i.e. covers) of their favorite number ring (like $\mathbb{Z}$, $\mathbb{Z}[\zeta_n]$ or $\mathbb{Z}[\sqrt{-6}]$).

Why is the class group so important?

David Hilbert

Teiji Takagi

Number theorists are really interested in describing extensions (i.e. covers) of their favorite number ring (like $\mathbb{Z}$, $\mathbb{Z}[\zeta_n]$ or $\mathbb{Z}[\sqrt{-6}]$).

The crowning achievement of early 20th century number theory (Hilbert, Takagi) was class field theory. It describes all abelian extensions of R in terms of $\mathrm{Cl}(R)$.

Why is the class group so important?

David Hilbert

Teiji Takagi

Number theorists are really interested in describing extensions (i.e. covers) of their favorite number ring (like $\mathbb{Z}$, $\mathbb{Z}[\zeta_n]$ or $\mathbb{Z}[\sqrt{-6}]$).

The crowning achievement of early 20th century number theory (Hilbert, Takagi) was class field theory. It describes all abelian extensions of R in terms of $\mathrm{Cl}(R)$.

One of the main programs right now is the Langlands program, which aims to generalize class field theory to non-abelian extensions.

Why is the class group so important?

David Hilbert

Teiji Takagi

Number theorists are really interested in describing extensions (i.e. covers) of their favorite number ring (like $\mathbb{Z}$, $\mathbb{Z}[\zeta_n]$ or $\mathbb{Z}[\sqrt{-6}]$).

The crowning achievement of early 20th century number theory (Hilbert, Takagi) was class field theory. It describes all abelian extensions of R in terms of $\mathrm{Cl}(R)$.

One of the main programs right now is the Langlands program, which aims to generalize class field theory to non-abelian extensions.

Although Wiles' proof does not rely on factoring in any way, class field theory is essential to his whole approach!

Statistical questions

Statistical questions about class groups are *exceptionally difficult*.

Statistical questions

Statistical questions about class groups are *exceptionally difficult*.

Gauss already asked if there are infinitely many squarefree integers d such that $\mathrm{Cl}(\mathbb{Z}[\sqrt{d}]) = \{0\}$, i.e. $\mathbb{Z}[\sqrt{d}]$ is an UFD. Completely open!

Statistical questions

Statistical questions about class groups are *exceptionally difficult*.

Gauss already asked if there are infinitely many squarefree integers d such that $\mathrm{Cl}(\mathbb{Z}[\sqrt{d}]) = \{0\}$, i.e. $\mathbb{Z}[\sqrt{d}]$ is an UFD. Completely open!

If one numerically enumerates d such that 9 exactly divides $|\mathrm{Cl}(\mathbb{Z}[\sqrt{-d}])|$, then one sees that the group $\mathbb{Z}/3\mathbb{Z} \oplus \mathbb{Z}/3\mathbb{Z}$ is 8 times less likely than $\mathbb{Z}/9\mathbb{Z}$. Why?

Statistical questions

Statistical questions about class groups are *exceptionally difficult*.

Gauss already asked if there are infinitely many squarefree integers d such that $\mathrm{Cl}(\mathbb{Z}[\sqrt{d}]) = \{0\}$, i.e. $\mathbb{Z}[\sqrt{d}]$ is an UFD. Completely open!

If one numerically enumerates d such that 9 exactly divides $|\mathrm{Cl}(\mathbb{Z}[\sqrt{-d}])|$, then one sees that the group $\mathbb{Z}/3\mathbb{Z} \oplus \mathbb{Z}/3\mathbb{Z}$ is 8 times less likely than $\mathbb{Z}/9\mathbb{Z}$. Why?

Conjecture (Cohen–Lenstra, 1984)

Let p be an odd prime. Let A be a finite abelian group such that all elements have order p^k for some k. Then

$$\lim_{X\to\infty} \frac{|\{0 < d < X \text{ sqf.} : \mathrm{Cl}(\mathbb{Z}[\sqrt{-d}])[p^\infty] \cong A\}|}{|\{0 < d < X : \text{ sqf.}\}|} = \frac{\prod_{i=1}^{\infty}\left(1 - \frac{1}{p^i}\right)}{|\mathrm{Aut}(A)|}$$

Randomness

The weight $1/|\mathrm{Aut}(A)|$ may seem strange at first, but is very natural.

Randomness

The weight $1/|\mathrm{Aut}(A)|$ may seem strange at first, but is very natural.

It essentially predicts that the class group is a random abelian group.

Randomness

The weight $1/|\mathrm{Aut}(A)|$ may seem strange at first, but is very natural.

It essentially predicts that the class group is a random abelian group.

Example (Random graphs)

Consider n labelled vertices. Among the set of all possible graphs with n labelled vertices, how many are isomorphic to a given graph $\mathcal{G}$? This is

$$\frac{n!}{|\mathrm{Aut}(\mathcal{G})|}.$$

Randomness

The weight $1/|\mathrm{Aut}(A)|$ may seem strange at first, but is very natural.

It essentially predicts that the class group is a random abelian group.

Example (Random graphs)

Consider n labelled vertices. Among the set of all possible graphs with n labelled vertices, how many are isomorphic to a given graph $\mathcal{G}$? This is

$$\frac{n!}{|\mathrm{Aut}(\mathcal{G})|}.$$

Indeed, let S_n act on the set of n labelled vertices. Then the orbit of $\mathcal{G}$ is the set of graphs isomorphic to $\mathcal{G}$, while the stabilizer is $\mathrm{Aut}(\mathcal{G})$. Now use the orbit–stabilizer theorem.

Randomness

The weight $1/|\mathrm{Aut}(A)|$ may seem strange at first, but is very natural.

It essentially predicts that the class group is a random abelian group.

Example (Random graphs)

Consider n labelled vertices. Among the set of all possible graphs with n labelled vertices, how many are isomorphic to a given graph $\mathcal{G}$? This is

$$\frac{n!}{|\mathrm{Aut}(\mathcal{G})|}.$$

Indeed, let S_n act on the set of n labelled vertices. Then the orbit of $\mathcal{G}$ is the set of graphs isomorphic to $\mathcal{G}$, while the stabilizer is $\mathrm{Aut}(\mathcal{G})$. Now use the orbit–stabilizer theorem.

One can do a similar story for "random abelian groups" (i.e. random multiplication tables), and this produces $c/\mathrm{Aut}(A)$ for c a constant.

Overview

Diophantine equations and factoring

Class groups

Pell's equation

Future work

Pell's equation

Pell's equation is

$$x^2 - dy^2 = \pm 1 \text{ to be solved in } x, y \in \mathbb{Z}.$$

Pell's equation

Pell's equation is

$$x^2 - dy^2 = \pm 1 \text{ to be solved in } x, y \in \mathbb{Z}.$$

Studied by Archimedes, Pythagoras, Bhaskara II, Brahmagupta, Fermat, Brouncker, Wallis, Euler, Lagrange, Legendre, Gauss, Dirichlet ...

Pell's equation

Pell's equation is

$$x^2 - dy^2 = \pm 1 \text{ to be solved in } x, y \in \mathbb{Z}.$$

Studied by Archimedes, Pythagoras, Bhaskara II, Brahmagupta, Fermat, Brouncker, Wallis, Euler, Lagrange, Legendre, Gauss, Dirichlet ...

Pythagoras proved that $\sqrt{2}$ is irrational, i.e. $x^2 - 2y^2 = 0$ has no solutions in $x, y \in \mathbb{Z}$.

Pell's equation

Pell's equation is

$$x^2 - dy^2 = \pm 1 \text{ to be solved in } x, y \in \mathbb{Z}.$$

Studied by Archimedes, Pythagoras, Bhaskara II, Brahmagupta, Fermat, Brouncker, Wallis, Euler, Lagrange, Legendre, Gauss, Dirichlet ...

Pythagoras proved that $\sqrt{2}$ is irrational, i.e. $x^2 - 2y^2 = 0$ has no solutions in $x, y \in \mathbb{Z}$.

The Pell equation is instead the "next best thing", namely $x^2 - 2y^2 = \pm 1$. It provides the best rational approximations to $\sqrt{2}$.

Pell's equation

Pell's equation is

$$x^2 - dy^2 = \pm 1 \text{ to be solved in } x, y \in \mathbb{Z}.$$

Studied by Archimedes, Pythagoras, Bhaskara II, Brahmagupta, Fermat, Brouncker, Wallis, Euler, Lagrange, Legendre, Gauss, Dirichlet ...

Pythagoras proved that $\sqrt{2}$ is irrational, i.e. $x^2 - 2y^2 = 0$ has no solutions in $x, y \in \mathbb{Z}$.

The Pell equation is instead the "next best thing", namely $x^2 - 2y^2 = \pm 1$. It provides the best rational approximations to $\sqrt{2}$.

Solution x, y	Ratio x/y	Expansion of $\sqrt{2}$
$x = 1,\ y = 1$	1	1.4142135...
$x = 3,\ y = 2$	1.5	1.4142135...
$x = 7,\ y = 5$	1.4	1.4142135...
$x = 17,\ y = 12$	1.4166666...	1.4142135...
$x = 41,\ y = 29$	1.4137931...	1.4142135...
$x = 99,\ y = 70$	1.4142857...	1.4142135...

The riddle of Archimedes

Archimedes gave a two-part riddle. In the first part he asks to solve a linear system of seven equations in eight unknowns (to be solved in integer variables). The smallest solution vector has roughly seven digits in every entry.

The riddle of Archimedes

Archimedes gave a two-part riddle. In the first part he asks to solve a linear system of seven equations in eight unknowns (to be solved in integer variables). The smallest solution vector has roughly seven digits in every entry.

If one can solve this system, Archimedes says "thou wouldst not be called unskilled or ignorant of numbers, but not yet shalt thou be numbered among the wise."

The riddle of Archimedes

Archimedes gave a two-part riddle. In the first part he asks to solve a linear system of seven equations in eight unknowns (to be solved in integer variables). The smallest solution vector has roughly seven digits in every entry.

If one can solve this system, Archimedes says "thou wouldst not be called unskilled or ignorant of numbers, but not yet shalt thou be numbered among the wise."

He then asks to solve

$$x^2 - 609 \cdot 7766 y^2 = 1.$$

If one can solve this further equation, Archimedes says "thou shalt depart crowned with glory and knowing that thou hast been adjudged perfect in this species of wisdom."

The riddle of Archimedes

Archimedes gave a two-part riddle. In the first part he asks to solve a linear system of seven equations in eight unknowns (to be solved in integer variables). The smallest solution vector has roughly seven digits in every entry.

If one can solve this system, Archimedes says "thou wouldst not be called unskilled or ignorant of numbers, but not yet shalt thou be numbered among the wise."

He then asks to solve

$$x^2 - 609 \cdot 7766 y^2 = 1.$$

If one can solve this further equation, Archimedes says "thou shalt depart crowned with glory and knowing that thou hast been adjudged perfect in this species of wisdom."

The smallest solution after $x^2 = 1$, $y^2 = 0$ takes 50 pages to write down ($\approx 7.76 \times 10^{206544}$).

The positive Pell equation

Dirichlet proved that one can always non-trivially solve

$$x^2 - dy^2 = 1$$

in integers x, y (i.e. $x^2 = 1$ and $y^2 = 0$ being the trivial solution).

The positive Pell equation

Dirichlet proved that one can always non-trivially solve

$$x^2 - dy^2 = 1$$

in integers x, y (i.e. $x^2 = 1$ and $y^2 = 0$ being the trivial solution).

Archimedes seems to have already been aware of this, and the Indian mathematicians even provided an algorithm for solving this equation.

Example (Fermat's challenge to Brouncker and Wallis)

The smallest non-trivial solution to $x^2 - 61y^2 = 1$ is

The positive Pell equation

Dirichlet proved that one can always non-trivially solve

$$x^2 - dy^2 = 1$$

in integers x, y (i.e. $x^2 = 1$ and $y^2 = 0$ being the trivial solution).

Archimedes seems to have already been aware of this, and the Indian mathematicians even provided an algorithm for solving this equation.

Example (Fermat's challenge to Brouncker and Wallis)

The smallest non-trivial solution to $x^2 - 61y^2 = 1$ *is*

$$x = 1766319049, \quad y = 226153980.$$

The negative Pell equation

The negative Pell equation $x^2 - dy^2 = -1$ is more elusive.

The negative Pell equation

The negative Pell equation $x^2 - dy^2 = -1$ is more elusive.

To solve this equation, one certainly needs to be able to solve it modulo p for all primes p. But if p divides d, we get

$$x^2 \equiv -1 \bmod p.$$

The negative Pell equation

The negative Pell equation $x^2 - dy^2 = -1$ is more elusive.

To solve this equation, one certainly needs to be able to solve it modulo p for all primes p. But if p divides d, we get

$$x^2 \equiv -1 \bmod p.$$

This implies that $p \equiv 1 \bmod 4$ or $p = 2$. Define $\mathcal{D}$ to be the set of squarefree d for which $p \mid d$ implies $p \equiv 1 \bmod 4$ or $p = 2$.

The negative Pell equation

The negative Pell equation $x^2 - dy^2 = -1$ is more elusive.

To solve this equation, one certainly needs to be able to solve it modulo p for all primes p. But if p divides d, we get

$$x^2 \equiv -1 \bmod p.$$

This implies that $p \equiv 1 \bmod 4$ or $p = 2$. Define $\mathcal{D}$ to be the set of squarefree d for which $p \mid d$ implies $p \equiv 1 \bmod 4$ or $p = 2$.

Nagell (1930s) conjectured

$$\lim_{X \to \infty} \frac{\#\{d \leq X : d \in \mathcal{D}, x^2 - dy^2 = -1 \text{ sol.}\}}{\#\{d \leq X : d \in \mathcal{D}\}}$$

exists and lies in $(0, 1)$. The smallest $d \in \mathcal{D}$ for which the negative Pell equation is not soluble is $d = 34$.

The negative Pell equation

The negative Pell equation $x^2 - dy^2 = -1$ is more elusive.

To solve this equation, one certainly needs to be able to solve it modulo p for all primes p. But if p divides d, we get

$$x^2 \equiv -1 \bmod p.$$

This implies that $p \equiv 1 \bmod 4$ or $p = 2$. Define $\mathcal{D}$ to be the set of squarefree d for which $p \mid d$ implies $p \equiv 1 \bmod 4$ or $p = 2$.

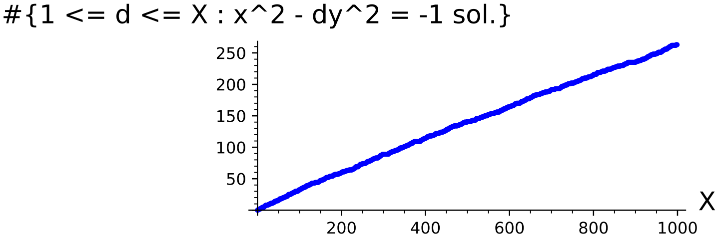
Nagell (1930s) conjectured

$$\lim_{X \to \infty} \frac{\#\{d \leq X : d \in \mathcal{D}, x^2 - dy^2 = -1 \text{ sol.}\}}{\#\{d \leq X : d \in \mathcal{D}\}}$$

exists and lies in $(0, 1)$. The smallest $d \in \mathcal{D}$ for which the negative Pell equation is not soluble is $d = 34$.

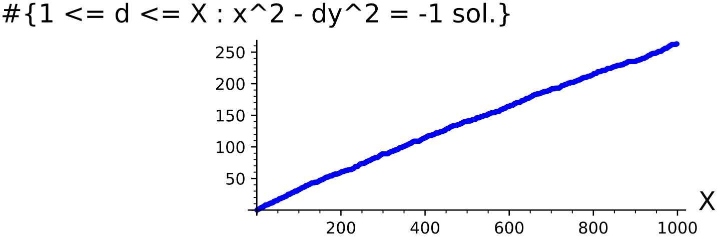
Stevenhagen (1995) predicted a precise value for the limit.

Proof of Stevenhagen's conjecture



Frequency of negative Pell solubility

Proof of Stevenhagen's conjecture



Frequency of negative Pell solubility

Theorem (K.–Pagano, 2022)

Stevenhagen's conjecture is true.

Translating to class groups

Consider the ring $\mathbb{Z}[\sqrt{d}]$. There is an automorphism $\sigma : \mathbb{Z}[\sqrt{d}] \to \mathbb{Z}[\sqrt{d}]$ given by $x + y\sqrt{d} \mapsto x - y\sqrt{d}$. Let $N(\alpha) = \alpha\sigma(\alpha)$. Note that

$$x^2 - dy^2 = \pm 1 \Leftrightarrow N(x + y\sqrt{d}) = \pm 1.$$

Translating to class groups

Consider the ring $\mathbb{Z}[\sqrt{d}]$. There is an automorphism $\sigma : \mathbb{Z}[\sqrt{d}] \to \mathbb{Z}[\sqrt{d}]$ given by $x + y\sqrt{d} \mapsto x - y\sqrt{d}$. Let $N(\alpha) = \alpha\sigma(\alpha)$. Note that

$$x^2 - dy^2 = \pm 1 \Leftrightarrow N(x + y\sqrt{d}) = \pm 1.$$

The norm map is multiplicative, i.e. $N(\alpha\beta) = N(\alpha)N(\beta)$, thus sends units to units. The only units of $\mathbb{Z}$ are ± 1.

Translating to class groups

Consider the ring $\mathbb{Z}[\sqrt{d}]$. There is an automorphism $\sigma : \mathbb{Z}[\sqrt{d}] \to \mathbb{Z}[\sqrt{d}]$ given by $x + y\sqrt{d} \mapsto x - y\sqrt{d}$. Let $N(\alpha) = \alpha\sigma(\alpha)$. Note that

$$x^2 - dy^2 = \pm 1 \Leftrightarrow N(x + y\sqrt{d}) = \pm 1.$$

The norm map is multiplicative, i.e. $N(\alpha\beta) = N(\alpha)N(\beta)$, thus sends units to units. The only units of $\mathbb{Z}$ are ± 1.

Conversely, if the norm is a unit, then the element itself is a unit. Thus negative Pell is soluble if and only if there is a unit of negative norm.

Translating to class groups

Consider the ring $\mathbb{Z}[\sqrt{d}]$. There is an automorphism $\sigma : \mathbb{Z}[\sqrt{d}] \to \mathbb{Z}[\sqrt{d}]$ given by $x + y\sqrt{d} \mapsto x - y\sqrt{d}$. Let $N(\alpha) = \alpha\sigma(\alpha)$. Note that

$$x^2 - dy^2 = \pm 1 \Leftrightarrow N(x + y\sqrt{d}) = \pm 1.$$

The norm map is multiplicative, i.e. $N(\alpha\beta) = N(\alpha)N(\beta)$, thus sends units to units. The only units of $\mathbb{Z}$ are ± 1.

Conversely, if the norm is a unit, then the element itself is a unit. Thus negative Pell is soluble if and only if there is a unit of negative norm.

Negative Pell equation can thus be solved if and only if there is a unit of norm -1.

Translating to class groups II

Recall that the negative Pell equation is soluble if and only if there is a unit of norm -1.

Translating to class groups II

Recall that the negative Pell equation is soluble if and only if there is a unit of norm -1.

This is equivalent to the ideal $(\sqrt{d})$ admitting a totally positive generator, i.e. $(\sqrt{d}) = (\alpha)$ with $\alpha > 0$ and $\sigma(\alpha) > 0$.

Translating to class groups II

Recall that the negative Pell equation is soluble if and only if there is a unit of norm -1.

This is equivalent to the ideal $(\sqrt{d})$ admitting a totally positive generator, i.e. $(\sqrt{d}) = (\alpha)$ with $\alpha > 0$ and $\sigma(\alpha) > 0$.

Rephrase this as an equality between the narrow class group (ideals modulo principal ideals with a totally positive generator) and the ordinary class group (ideals modulo principal ideals).

Translating to class groups II

Recall that the negative Pell equation is soluble if and only if there is a unit of norm -1.

This is equivalent to the ideal $(\sqrt{d})$ admitting a totally positive generator, i.e. $(\sqrt{d}) = (\alpha)$ with $\alpha > 0$ and $\sigma(\alpha) > 0$.

Rephrase this as an equality between the narrow class group (ideals modulo principal ideals with a totally positive generator) and the ordinary class group (ideals modulo principal ideals).

Obtain the statistics of the joint distribution of the 2-Sylow subgroup of the narrow class group and ordinary class group (in the style of Cohen–Lenstra).

Translating to class groups II

Recall that the negative Pell equation is soluble if and only if there is a unit of norm -1.

This is equivalent to the ideal $(\sqrt{d})$ admitting a totally positive generator, i.e. $(\sqrt{d}) = (\alpha)$ with $\alpha > 0$ and $\sigma(\alpha) > 0$.

Rephrase this as an equality between the narrow class group (ideals modulo principal ideals with a totally positive generator) and the ordinary class group (ideals modulo principal ideals).

Obtain the statistics of the joint distribution of the 2-Sylow subgroup of the narrow class group and ordinary class group (in the style of Cohen–Lenstra).

We only need to consider the 2-Sylow since $(\sqrt{d})$ has order 2 in the narrow class group. This is the only part of the class group that is well-understood by a recent breakthrough of A. Smith.

Overview

Future work

I am working on applying the techniques from Stevenhagen's conjecture to obtain statistics for other Diophantine equations.

Future work

I am working on applying the techniques from Stevenhagen's conjecture to obtain statistics for other Diophantine equations.

One question is: how many integers $|n| \leq X$ are such that

$$x^3 + y^3 = n$$

has a solution in rational integers x, y?

Future work

I am working on applying the techniques from Stevenhagen's conjecture to obtain statistics for other Diophantine equations.

One question is: how many integers $|n| \leq X$ are such that

$$x^3 + y^3 = n$$

has a solution in rational integers x, y?

Note: it is not hard to show that there are $\leq CX^{2/3}$ integers n for which there is a solution $x, y \in \mathbb{Z}$, for some absolute constant $C > 0$.

Future work

I am working on applying the techniques from Stevenhagen's conjecture to obtain statistics for other Diophantine equations.

One question is: how many integers $|n| \leq X$ are such that

$$x^3 + y^3 = n$$

has a solution in rational integers x, y?

Note: it is not hard to show that there are $\leq CX^{2/3}$ integers n for which there is a solution $x, y \in \mathbb{Z}$, for some absolute constant $C > 0$.

Example

For $n = 6$ one can use the factorization $x^3 + y^3 = (x+y)(x^2 - xy + y^2)$ to show that there are no integer solutions. However, we have

$$6 = \left(\frac{17}{21}\right)^3 + \left(\frac{37}{21}\right)^3.$$

Results

Alpöge–Bhargava–Shnidman showed that at least $2/21$ of integers are sums of cubes and at least $1/6$ are not sums of cubes.

Results

Alpöge–Bhargava–Shnidman showed that at least $2/21$ of integers are sums of cubes and at least $1/6$ are not sums of cubes.

Together with A. Smith I am working on improving these bounds (conjecturally, the limit should be $1/2$).

Results

Alpöge–Bhargava–Shnidman showed that at least $2/21$ of integers are sums of cubes and at least $1/6$ are not sums of cubes.

Together with A. Smith I am working on improving these bounds (conjecturally, the limit should be $1/2$).

Key tool: obtain distribution of Selmer group of $x^3 + y^3 = n$. This is the analogue of the class group for elliptic curves.

Chowla's conjecture

Sarvadaman Chowla

Kannan Soundararajan

Conjecture (Generalized Riemann hypothesis)

All non-trivial zeroes of $L(s, \chi)$ *lie on* $s = 1/2 + it$.

Chowla's conjecture

Sarvadaman Chowla

Kannan Soundararajan

Conjecture (Generalized Riemann hypothesis)

All non-trivial zeroes of $L(s, \chi)$ *lie on* $s = 1/2 + it$.

Conjecture (Chowla's conjecture)

We have $L(\frac{1}{2}, \chi) \neq 0$ *for all primitive Dirichlet characters* χ.

Chowla's conjecture

Sarvadaman Chowla

Kannan Soundararajan

Conjecture (Generalized Riemann hypothesis)

All non-trivial zeroes of $L(s, \chi)$ *lie on* $s = 1/2 + it$.

Conjecture (Chowla's conjecture)

We have $L(\frac{1}{2}, \chi) \neq 0$ *for all primitive Dirichlet characters* χ.

Important results towards Chowla's conjecture are due to Soundararajan and Özlük–Snyder.

Chowla's conjecture

Sarvadaman Chowla

Kannan Soundararajan

Conjecture (Generalized Riemann hypothesis)

All non-trivial zeroes of $L(s,\chi)$ lie on $s = 1/2 + it$.

Conjecture (Chowla's conjecture)

We have $L(\frac{1}{2},\chi) \neq 0$ for all primitive Dirichlet characters χ.

Important results towards Chowla's conjecture are due to Soundararajan and Özlük–Snyder.

There has also been great interest in the function field case of this conjecture.

Function fields

Theorem (W. Li (2018))

Let q be an odd prime power. There are infinitely many monic, squarefree polynomials $D \in \mathbb{F}_q[t]$ such that $L(\frac{1}{2}, \chi_D) = 0$.

Function fields

Theorem (W. Li (2018))

Let q be an odd prime power. There are infinitely many monic, squarefree polynomials $D \in \mathbb{F}_q[t]$ such that $L(\frac{1}{2}, \chi_D) = 0$.

However, 100% non-vanishing is still expected. This is currently not known for any single family of L-functions.

Function fields

Theorem (W. Li (2018))

Let q be an odd prime power. There are infinitely many monic, squarefree polynomials $D \in \mathbb{F}_q[t]$ such that $L(\frac{1}{2}, \chi_D) = 0$.

However, 100% non-vanishing is still expected. This is currently not known for any single family of L-functions.

The Özlük–Snyder result is known unconditionally over function fields (Bui–Florea).

Function fields

Theorem (W. Li (2018))

Let q be an odd prime power. There are infinitely many monic, squarefree polynomials $D \in \mathbb{F}_q[t]$ such that $L(\frac{1}{2}, \chi_D) = 0$.

However, 100% non-vanishing is still expected. This is currently not known for any single family of L-functions.

The Özlük–Snyder result is known unconditionally over function fields (Bui–Florea).

Many other families have also been studied but no 100% non-vanishing result is known.

Function fields

Theorem (W. Li (2018))

Let q be an odd prime power. There are infinitely many monic, squarefree polynomials $D \in \mathbb{F}_q[t]$ such that $L(\frac{1}{2}, \chi_D) = 0$.

However, 100% non-vanishing is still expected. This is currently not known for any single family of L-functions.

The Özlük–Snyder result is known unconditionally over function fields (Bui–Florea).

Many other families have also been studied but no 100% non-vanishing result is known.

Theorem (K.–Pagano–Shusterman)

We have $L(\frac{1}{2}, \chi_D) \neq 0$ for 100% of the monic squarefree polynomials D.

Proof sketch

By a result of Grothendieck we have $L(\frac{1}{2}, \chi_D) \neq 0$ if and only if there exists an embedding

$$\mathbb{Q}_2/\mathbb{Z}_2 \hookrightarrow \mathrm{Jac}(C_D)(\overline{\mathbb{F}_q})[2^\infty][\mathrm{Frob}_q^2 - q],$$

where C_D is the curve $y^2 = D$.

Proof sketch

By a result of Grothendieck we have $L(\frac{1}{2}, \chi_D) \neq 0$ if and only if there exists an embedding

$$\mathbb{Q}_2/\mathbb{Z}_2 \hookrightarrow \mathrm{Jac}(C_D)(\overline{\mathbb{F}_q})[2^\infty][\mathrm{Frob}_q^2 - q],$$

where C_D is the curve $y^2 = D$.

The Jacobian can be viewed as a function field analogue of the class group.

Proof sketch

By a result of Grothendieck we have $L(\frac{1}{2}, \chi_D) \neq 0$ if and only if there exists an embedding

$$\mathbb{Q}_2/\mathbb{Z}_2 \hookrightarrow \mathrm{Jac}(C_D)(\overline{\mathbb{F}_q})[2^\infty][\mathrm{Frob}_q^2 - q],$$

where C_D is the curve $y^2 = D$.

The Jacobian can be viewed as a function field analogue of the class group.

A suitable adaptation of our methods for Stevenhagen's conjecture allow one to obtain the distribution of this Jacobian, from which the theorem follows.

Questions?

Thank you for your attention!