Math 215 Spring 2023 Number Theory II

Diophantine Problems

Sankar Sitaraman – nature-lover.net/math

Math Dept, Howard University

2-15-2023

Outline

Definition of Diophantine Problems

A diophantine problem involves solving a polynomial equation with *integer coefficients* using integers.

Examples and Highlights:

1. **Fermat's Last Theorem** $x^n + y^n = z^n$

2.**Hilbert 10th problem**: When can a diophantine equation be solved? Is there a general algorithm?

Matiyasevich: It is impossible to find an algorithm to decide whether solution exists for a given polynomial.
Used Fibonacci numbers to construct counter-example.

Fermat's Last Theorem

Conjecture: *$x^n + y^n = z^n$ has no non-zero integer solutions if $n \geq 2$.*

1. Fermat said he had a solution, but it is doubtful.
2. For $n = 2$ we got complete solution, by looking at $(x + iy)(x - iy)$.
3. It is enough to look at $n = p$ where p is prime and $n = 4$.
4. Kummer proved it for all regular primes, i.e, odd p such that the class number of $\mathbb{Q}(\zeta_p)$ is not divisible by p. His idea was to look at divisibility of $x + \zeta_p y$ by prime ideals. Here we could have $\zeta_p = e^{2\pi i/p}$

Fermat's Last Theorem

For $n = 4$ Fermat did provide a proof of unsolvability of $x^4 + y^4 = z^2$ using descent. Note that this implies unsolvability of $x^4 + y^4 = z^4$.

1. Start with $a = x^2, b = y^2, c = z$ – this is a primitive Pythagorean triple.
2. Get $a = x^2 = st, b = y^2 = (s^2 - t^2)/2, c = z = (s^2 + t^2)/2$; s, t *odd* , $st = x^2 \implies s \equiv t \pmod 4$.
3. $2y^2 = s^2 - t^2 \implies s + t = 2u^2, s - t = 4v^2$. From this get $x^2 = u^4 - 4v^4$.
4. Repeat process with $A = x, B = 2v^2, C = u^2$
5. $A = ST, 2v^2 = (S^2 - T^2)/2, u^2 = (S^2 + T^2)/2 \implies S = X^2 + Y^2, T = X^2 - Y^2 \implies u^2 = X^4 + Y^4$.

Square triangular numbers

$$n^2 = \frac{m(m+1)}{2}$$

This can be written as

$$2n^2 = m^2 + m \implies 2n^2 = (m + (1/2))^2 - (1/4)$$

$$\implies 2n^2 = \frac{(2m+1)^2 - 1}{4} \implies 2(2n)^2 = (2m+1)^2 - 1.$$

So if m, n are solutions for original equation, $2m+1, 2n$ are solutions for

$$x^2 - 2y^2 = 1.$$

Converse is true also. Given a solution to this "Pell's equation" we get a square-triangular pair.

Solution for Pell gives Square triangular numbers

We saw that if m, n are square triangular numbers, $2m+1, 2n$ are solutions for

$$x^2 - 2y^2 = 1.$$

Given a solution to this "Pell's equation" we show that you get a square-triangular pair.
If $x^2 - 2y^2 = 1$, then x has to be odd and y has to be even. To see why y has to be even, look at equation mod 4.

So $m = (x-1)/2, n = y/2$ are also integers and clearly they are square-triangular,.

Pell's equation and Quadratic fields

$$x^2 - Dy^2 = 1 \implies (x - \sqrt{D}y)(x + \sqrt{D}y) = 1, D > 0$$

So there is a connection between the solutions of Pell's equation and the units of the ring $\mathbb{Z}[\sqrt{D}]$ in the quadratic extension generated by $\sqrt{D}$. For the moment let us assume that $D \not\equiv 1 \pmod 4$. (Otherwise the ring of algebraic integers is different from $\mathbb{Z}[\sqrt{D}]$).

FACT: A consequence of Dirichlet's theorem on units in number fields is that the unit group $U(\mathbb{Z}[\sqrt{D}])$ of $\mathbb{Z}[\sqrt{D}]$ is free of rank 1. In other words, the group is generated by one element $\alpha + \beta\sqrt{2}$, called the fundamental unit:

$$x + y\sqrt{2} \in U(\mathbb{Z}[\sqrt{D}]) \implies x + y\sqrt{2} = (\alpha + \sqrt{D}\beta)^k, k \in \mathbb{Z}.$$

Generating square triangular numbers

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

Starting with the solution $(3, 2)$ we can generate more solutions. If $x^2 - 2y^2 = 1$ then any power of LHS is also 1. In fact, we have:

FACT: Every solution to Pell's equation is given by

$$(3 + 2\sqrt{2})^k = x_k + y_k\sqrt{2},\ k = 1, 2, 3, ...$$

And so every square-triangular number can also be generated this way.

Proof : Use method of descent.

Proof: Generating square triangular numbers

It is enough to show, given any solution (u, v), another solution $(s + t\sqrt{2})$ such that

$$(u + v\sqrt{2}) = (3 + 2\sqrt{2})(s + t\sqrt{2}),\ s < u.$$

Proof : First solve for s, t using above equation, just by comparing both sides. You get

$$s = 3u - 4v, t = -2u + 3v.$$

Next show s is positive using $u^2 = 1 + 2v^2$ and $s = 3u - 4v$.
Then show $t > 0$ using $v > 2u/3$ and $t = 3v - 2u$. To show $v > 2u/3$ use $u^2 = 1 + 2v^2$ and $u > 3$.
Finally show that $s < u$ using $u = 3s + 4t$ and $s > 0, t > 0$.

Solution for the negative Pell equation

The negative Pell equation (for $D = 2$) is

$$x^2 - 2y^2 = -1.$$

The solutions $x + \sqrt{2}y$ of this equation are also units in $\mathbb{Z}[\sqrt{2}]$!

This equation can be written as $2y^2 - x^2 = 1$. The smallest solution is $x = 1, y = 1$.

Now notice that $(1 + \sqrt{2})^2 = 1 + 2 + 2\sqrt{2} = 3 + 2\sqrt{2}$!
This is not a coincidence. The fundamental solution of the positive Pell's equation is a square of the fundamental solution of the negative Pell equation, if it exists. Unlike the positive equation, the negative equation need not have solution. We will prove existence of solutions to positive Pell's equation later.

Generating solution for the Pell equation

If $x^2 - 2y^2 = 1$ then any power of LHS is also 1. This is the idea that helps us generates solutions of positive Pell equation. We proved that all solutions can be generated this way, starting with fundamental unit. In the case of negative pell equation, only odd powers will work

Notice that, $x^2 - Dy^2 = -1 \implies Dy^2 = x^2 + 1$ and so D cannot be divisible by primes congruent to 3 mod 4.

Generating solutions using fundamental units

The following is based on a paper by Michel Waldschmidt.

As mentioned above, solutions to both positive and negative Pell's equation $x^2 - Dy^2 = \pm 1$ are units.
The norms of the units thus obtained are $+1$ and -1 respectively.

FACT: Any unit is a power of the fundamental unit.
The proof, based on Waldschmidt's, follows below.

Since the powers of unit of norm 1 cannot be of norm -1, this means that
if the fundamental unit is of norm $+1$ *then there is NO SOLUTION to the negative Pell equation*

Generating solutions using fundamental units

Proof of fundamental unit theorem (based on Waldschmidt's paper):

Let $a + b\sqrt{D}$ be the fundamental unit, i.e, lowest positive unit with non-zero coefficients a, b.

Remember, $a + b\sqrt{D}$ could be a solution of either positive OR negative Pell's equation.

(so the norm of unit could be $+1$ or -1).

contd: Generating solutions using fundamental units

Proof continued:

Let $x + y\sqrt{D}$ be any other positive solution. Then there is an $n \in \mathbb{Z}^+$ such that

$$(a + b\sqrt{D})^n \leq x + y\sqrt{D} < (a + b\sqrt{D})^{n+1}.$$

$$\implies 1 \leq (x + y\sqrt{D})(a + b\sqrt{D})^{-n} < (a + b\sqrt{D})$$

Easy to check that $(x + y\sqrt{D})(a + b\sqrt{D})^{-n}$ is a unit itself, but if it is smaller than fundamental unit, then
$(x + y\sqrt{D})(a + b\sqrt{D})^{-n} = 1$ and that means
$(x + y\sqrt{D}) = (a + b\sqrt{D})^n$!

Diophantine Approximation and Pell's Equation

"Diophantine" in general refers to finding *solution in integers.*
"Diophantine approximation" refers to finding integers close to irrational (or even transcendental) numbers.

Example: The decimal approximation of $u = \sqrt{2}$ is between 1 and 2 because $1 < u^2 < 4$.

The decimal approximation of $10u = 10\sqrt{2}$ is between 14 and 15 because $198 < 10u^2 = 200 < 225$.
So that means $1.4 < u < 1.5$.

We can continue this way to get the approximation as precise as we want it.

Dirichlet's Theorem on Diophantine Approximation

You can frame the results above as saying

$$\forall k \in \mathbb{Z}, k \geq 0, \exists N \in \mathbb{Z} \text{ such that } \left| \frac{N}{10^k} - \sqrt{2} \right| < \frac{1}{10^k}$$

Proof: Divide both sides of $|N - 10^k u| < 1$ by 10^k.

Dirichlet's Theorem : *Given $\alpha \in \mathbb{R} - \mathbb{Q}$ there are infinitely many pairs of integers x, y such that*

$$|x - y\alpha| < \frac{1}{y} \text{ OR } \left| \frac{x}{y} - \alpha \right| < \frac{1}{y^2}.$$

Proof uses **Pigeonhole Principle** : If you put $n + 1$ things into n boxes, one of them will have two.

Pigeonhole Principle applications

Examples of application of Pigeonhole principle:

1. A one-one map from a set to itself is also onto.
2. The maximum of any finite set of numbers is greater than the average.
3. Bolzano-Weierstass theorem: Any infinite set of real numbers inside a bounded interval has a convergent subsequence
4. In any party of 6 people, there are either 3 who know each other or 3 who are strangers to each other.
5. A finite, closed subset of a group must be a subgroup. (actually any finite set with an operation that is closed, associative, and has identity AND satisifies cancellation property will do).

Proof of Dirichlet's Theorem

Main idea:

Let Y be any positive integer.
Look at $k\alpha$ where $k = 0, 1, 2, ..., Y$. There are $Y + 1$ of them.
Let $\{r\}$ denote the **fractional part** of any real number.

Then two of the $Y + 1$ numbers $\{k\alpha\}$ must be in the same interval among the Y intervals of length $1/Y$ given by $\left[\frac{k}{Y}, \frac{k+1}{Y}\right)$ where k goes from 0 to $Y - 1$.

You get infinitely many because, $x - y\alpha$ is never 0 (α is irrational!), and $1/y$ can get infinitely smaller, and so you need new pairs to get smaller values.

Proof of Dirichlet's Theorem - page 2

Production of desired $x - y\alpha$:

Let the two numbers $\{k\alpha\}$ that are in the same interval of length $1/Y$ be $\{n\alpha\}$ and $\{m\alpha\}$.

Now for any real number a, we can write $a = A + \{a\}$ where A is the integer part (greatest integer smaller than a).

Then $n\alpha = N + \{n\alpha\}$ and $m\alpha = M + \{m\alpha\}$ where N and M are their integer parts.

$$So \ \{n\alpha\} = n\alpha - N, \ \{m\alpha\} = m\alpha - M,$$

$$and \ \{n\alpha\} - \{m\alpha\} = M - N + (n - m)\alpha.$$

Proof of Dirichlet's Theorem - page 3

Conclusion of Proof:

Let the two numbers $\{k\alpha\}$ that are in the same interval of length $1/Y$ be $\{n\alpha\}$ and $\{m\alpha\}$. Assume WLOG $m > n$.
Now for any real number a, we can write $a = A + \{a\}$ where A is the integer part (greatest integer smaller than a).

Then $n\alpha = N + \{n\alpha\}$ and $m\alpha = M + \{m\alpha\}$ where N and M are their integer parts. So $\{n\alpha\} = n\alpha - N$, $\{m\alpha\} = m\alpha - M$, and

$$\textit{Define} \qquad \{n\alpha\} - \{m\alpha\} = M - N - (m-n)\alpha = x - y\alpha.$$

Easy to see: $y = m - n \leq Y$ and $|x - y\alpha| < 1/Y \leq 1/y$!

Dirichlet's Theorem and Pell's equation

Plan for proving existence of solutions to $x^2 - Dy^2 = 1$:

1. Among all the pairs x, y such that $|x - y\alpha| < 1/y$ find pairs such that $x^2 - Dy^2$ values are equal, say M. Since their norms are equal, their ratio will have norm 1. Need to show that the ratio is in $\mathbb{Z}[\sqrt{D}]$.
2. Among these pairs, find two such that the x values are congruent mod M and y values are also congruent mod M. For these, the ratio will be an integer.

Will use Pigeonhole principle in both of them.