XM452 Lecture Notes 7

Erdaifu Luo

9 April 2023

§32 Introduction to Diophantine Equations

§32.1 Background and Examples on Diophantine Equations

Fermat's equation was perhaps the most well known Diophantine equation. Fermat states that he had a proof for $n \geq 3$ there are no nonzero integral solutions ot the equation

$$x^n + y^n = z^n \quad (x, y, z \in \mathbb{Z}).$$

If Fermat's last theorem is true for integer $n = a$, then it is also true for all $n = a \cdot b$ where $b \in \mathbb{Z}$, because

$$x^{a \cdot b} + y^{a \cdot b} = z^{a \cdot b}$$

is the same as

$$\left(x^b\right)^a + \left(y^b\right)^a = \left(z^b\right)^a,$$

which by assumption has no non-zero integral solutions for x^b, y^b, z^b.

Now note that every integer $n > 2$ is either divisible by an odd prime or is a power of 2. Thus if Fermat's last theorem is ture for $n = 4$, and for all odd primes then it is true.

Fermat proved his theorem in the $n = 4$ case, then left the problem for proving

$$x^p + y^p = z^p$$

has no non-zero integral solutions for p any odd prime. Euler proved this for $p = 3$ but the whole theorem was not proven until 1994 when a proof was given by Andrew Wiles.

Fermat announced that

$$x^2 + 2 = y^3$$

only had $x = 5$ and $x = 3$ as a positive integer solution. Fermat's rival, John Wallis, said that

$$x^4 + 9 = y^2$$

has only $x = 2$, $y = 5$ as a positive integer solution, and what Fermat has proven is equivalent to that. In actuality, Wallis's result can be shown using simple algebra, whilst Fermat's was much deeper.

Solution to Wallis' equation.

$$x^4 + 9 = y^2.$$

Rewrite it as $y^2 - x^4 = 9$, and factor

$$\left(y + x^2\right)\left(y - x^2\right) = 9.$$

Assuming $x, y > 0$ are integers, it follows that $y + x^2 = \geq 2$. Thus, $y - x^2 > 0$.

There are only two possibilities of factoring $y + x^2 \geq 2$ as product of positive integers: $9 = 1 \cdot 9 + 3 \cdot 3$.

Therefore either

$$y + x^2 = 3 \text{ and } y \cdot x^2 = 3 \tag{1}$$

or

$$y + x^2 = 9 \text{ and } y \cdot x^2 = 1. \tag{2}$$

In (1), if $y + x^2 = 3$ and $y \cdot x^2 = 3$, x and y are positive integers. Then, $x = 1$ since $2^2 > 3$, but then $y \cdot x^2 \neq 3$.

Thus, testing (2), if $y \cdot x^2 = 1$ then $y = x^2 + 1$. Substituting in $y + x^2 = 9$ yields

$$\left(x^2 + 1\right) + x^2 = 9,$$

which after solving, we get $x = 2$.

This implies that $y = x^2 + 1 = 2^2 + 1 = 5$. So $x = 2$ and $y = 5$ are the only solutions to Wallis' equation. □

§33 Using Congruences to Solve Diophantine Equations

In this lecture, we will describe a method of proof that uses modular arithmetic.

We consider a family of famious Diophantine equations: the "Fermat-Pell equations":

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

and

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

for fixed values of d.

Example 33.1

$$x^2 - 7y^2 = -1$$

Now, suppose (x_0, y_0) is a solution. Then, of course, it is a solution mod 7, or

$$x_0^2 - 7y_0^2 \equiv 1 \pmod 7.$$

But $7_0^2 \equiv 0 \pmod 7$ so $x_0^2 \equiv -1 \pmod 7$.

But this is impossible, since we know by a previous theorem that there are no mod p square roots of -1 if $p \equiv 3 \pmod 4$.

So by "reducing mod 7" this equation, we see that there are no solutions to the equation

$$x^2 - 7x^2 \equiv -1$$

among the positive integers.

We now generalize this technique.

Theorem 33.2

Suppose that d is divisible by a prime p which is congruent to 3 mod 4, or that d is divisible by 4. Then the Fermat-Pell equation

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

has no solutions among the positive integers

Proof. Suppose (x_0, y_0) is a solution to $x^2 - dy^2 = -1$ and $p \equiv 3 \pmod 4$ and $p \mid d$ so that $d \equiv 0 \pmod p$.

We derive a contradiction:

$$\begin{aligned} x_0^2 - dy^2 &\equiv -1 \pmod p \\ x_0^2 &\equiv -1 \pmod p \end{aligned}$$

which is impossible by the previous theorem mentioned above.

Similarily, if $4 \mid d$, then

$$x_0^2 \equiv x_0^2 - dy_0^2 \equiv -1 \pmod 4$$

which is impossible because every integer x has the property that $x^2 \equiv 0$ or $x^2 equiv 1 \pmod 4$.

Thus our assumption that $x^2 - dy^2 = -1$ has a solution led to a contradiction, which must be false. □

The main idea is that if x, y satisfy a Diophantine equation, then they must satisfy the corresponding mod n Diophantine equation for every n. This equation might be easier.

Example 33.3

$$x^2 - 5y^2 = 2$$

"Reduce mod 5"

$$x^2 \equiv x^2 - 5y^2 \equiv 2 \pmod 5$$

so

$$x^2 \equiv 2 \pmod 5.$$

But none of the numbers 0, 1, 2, 3, or 4 have square congruent to 2 mod 5, hence our original equation has no solutions.

§34 Pythagorean Triples

Recall a theorem we proved a long time ago stating that if $(a, b) = 1$, $a, b > 0$ and

$$ab = c^n$$

then there exists integers d, e such that $a = d^n$, $b = e^n$.

We will show how this theorem can be used to find ”Pythagorean Triples”. These are the sides of right triangles with integral lengths orin other words, postive integral solutions to

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

Of course, if x_0, y_0, z_0 is a solution, then so is kx_0, ky_0, kz_0 for any integer multiple k (similar triangles). So we will look only for ”primitive solutions”, solutions with $(x, y, z) = 1$.

Since $x^2+y^2 = z^2$, if x and y are both even, then so is z, which contradicts $(x, y, z) = 1$. So at most, one of x and y is even.

Moreover, if both x and y are odd, then

$$z^2 \equiv x^2 + y^2 \equiv 1 + 1 \equiv 2 \pmod 4.$$

Therefore, exactly one of x and y must be odd, the other even. Assume x is odd and y is even.

Theorem 34.1

There are infinitely many solutions to the equation

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

with $(x, y, z) = 1$, y evem, and $x, y, z > 0$.

Additionally, these are given by $x = u^2 - v^2$, $y = 2uv$, $z = u^2 + v^2$ where u and v are any relatively prime integers and one of u and v is even.

Proof. By the above reasoning we assume x is odd, y is even, so that

$$z^2 \equiv 1 + 0 \equiv 1 \pmod 4.$$

Thus z is odd. So, $z + x$, $z - x$ are both even. Moreover,

$$(z + x)(z - x) = z^2 - x^2 = y^2$$

and we can divide each factor y 2:

$$\frac{(z + x)}{2} \cdot \frac{(z - x)}{2} = \frac{y^2}{4}$$

since $z + x$, $z - x$, y are all divisible by 2.

Claim 34.2 —

$$\left(\frac{z + x}{2}, \frac{z - x}{2}\right) = 1.$$

Since $x^2 + y^2 = z^2$, we have that $z > x$. So $\frac{z+2}{2}$ and $\frac{z-x}{2}$ are positive, relatively prime ietegers whose product is y^2.

By the theorem mentioned in the beginning of the lecture, we can find u and v such that

$$\frac{z + x}{2} = u^2, \quad \frac{z - x}{2} = v^2$$

and thus

$$x = \frac{z + x}{2} - \frac{z - x}{2} = u^2 - v^2$$

and

$$y = 2\left(\frac{z+x}{2}\right)^{1/2}\left(\frac{z-x}{2}\right)^{1/2} = 2uv$$

with

$$z = \frac{z+x}{2} + \frac{z-x}{2} = u^2 + v^2.$$

This gives us the u and v stated in the theorem. We now go back and prove the claim:

Let $d = \left(\frac{z+x}{2}, \frac{z-x}{2}\right)$. So,

$$d \mid \frac{z+x}{2} + \frac{z-x}{2} = z$$

and

$$d \mid \frac{z+x}{2} - \frac{z-x}{2} = x.$$

Hence $d \mid (x, z)$. But $(x, z) = 1$. Therefore, $d = 1$, proving the claim. □

We now verify the converse: if $x = u^2 - v^2$, $y = 2uv$, $z = u^2 = v^2$ with u, v positive, relatively prime and one of u and v is even, then $x^2 + y^2 = z^2$ with $x, y, z > 0$ and $(x, y, z) = 1$.

The only nontrivial part of the converse is that $(x, y, z) = 1$. That is, $*u^2 - v^2, 2uv, u^2 + v^2) = 1$.

Let d equals the above. Suppose by ways of contradiction that $d > 1$. Then, there is a prime $p \mid d$ which threfore divides each of the previous terms.

Thus, $p \mid (u^2 + v^2) + 2uv$, or $p \mid (u + v)^2$ which implies $p \mid (u + v)$.

Similarily, $p \mid *u^2 + v^2 - 2uv$, or $p \mid (u - v)^2$ which implies $p \mid (u - v)$.

Thus, $p \mid (u + v) + (u - v)$ so that $p \mid 2u$. Similarily, $p \mid 2v$, and thus $p \mid (2u, 2v) = 2(u, v) = 2$ since $(u, v) = 1$. So $p = 2$. But since one of u and v is even while th other is odd, p cannot be 2. This contradiction implies $d = 1$.

§35 The Method of Descent (Fermat)

Proof. Suppose that x_0, y_0, z_0 is a solution. For example,

$$x_0^4 + y_0^4 = z_0^2$$

We show there are no solutions with x_0, y_0, $z_0 > 0$.

First show that there is a solution x_1, y_1, $z_1 > 0$ with $(x_1, y_1) = 1$. Let $d = (x_0, y_0)$. $d \mid x_0$ and $d \mid y_0$, so let $x_0 = d \cdot x_0$, $y_0 = d \cdot y_1$.

Thus,

$$d^4(x_1^4 + y_1^4) = z_0^2.$$

Therefore,

$$\left(\frac{z_0}{d^2}\right)^2 = x_1^4 + y_1^4$$

is an integer.

Let $z_1 = \frac{z_0}{d^2}$. This is rational as it is a ratio of integers, and it is a square root of an integer. By a prvious theorem, z_1 is an integer, and

$$x_1^4 + y_1^4 = z_1^2$$

is a solution to the original equation with x_1, y_1, $z_1 > 0$ and $(x_1, y_1) = 1$.

Now, show x_1, y_1, z_1 leads to another solution x_2, y_2, $z_2 > 0$ with $(x_2, y_2 = 1$ and $z_2 < z_1$.

This is the basic step in the **method of descent**. That is, we produce solutions in which a z term so small that it cannot possibly be a solution. This is how we arrive at a contradiction.

Note

$$\left(x_1^2\right)^2 + \left(y_1^2\right)^2 = z_1^2.$$

So therefore, x_1^2, y_1^2, z_1 is a Pythagorean triple. Also, if a prime p divides x_1^2 and y_1^2, then $p \mid x_1$, $p \mid y_1$.

However, $(x_1, y_1) = 1$. Thus, $(x_1^2, y_1^2) = 1$ and so x_1^2, y_1^2, z_1 is a primitive Pythagorean triple.

Recall that this implies exactly one of x_1^2 and y_1^2 is even. Assume y_1^2 is even and x_1^2 is odd. From last lecture, there exist integers u, $v > 0$ such that

$$x_1^2 = u^2 - v^2, \quad y_1^2 = 2uv, \quad z_1^2 = u^2 + v^2$$

Moreover, $(u, v) = 1$ and exactly one of u and v is even.

Thus, $x_1^2 v^2 = u^2$. Or, x_1, v, u is a Pythagorean triple. Since $(u, v) = 1$, it is primitive. Applying the theorem again, we find positive integers a, b such that $(a, b) = 1$ and x_1, u, v is a primitive Pythagorean triple with x_1 odd, and so v is even. Hence u is odd.

Therefore, if $d = (u, 2v)$, then d is odd. Since $d \mid 2v$, this implies that $d \mid v$. But $(u, v) = 1$ so $d = 1$ and u and $2v$ are relatively prime.

So we know

$$y_1^2 = 2uv = u(2v).$$

By a previous theorem, since $(u, 2v) = 1$, u and $2v$ are perfect squares.

Write

$$u = z_2^2, \quad 2v = c^2.$$

c must be even so let $c = 2d$.

Thus, $v = 2d^2$. So $v = 2ab$ implies

$$ab = \frac{v}{2} = \frac{c^2}{4} = d^2.$$

But $(a, b) = 1$ so both a and b are perfect squares. Write

$$a = x_2^2, b = y_2^2.$$

And note that $(a, b) = 1 \to (x_2, y_2) = 1$.

If we replace a, b, and u by x_2^2, y_2^2 and z_2^2, then the equation

$$u = a^2 + b^2$$

becomes

$$x_2^4 + y_2^4 = z_2^2.$$

Thus it is a solution to the original Diophantine equation.

Moreover, $(x_2, y_2) = 1$, so it only reamins to prove $z_2 < z_1$. This is because

$$0 < z_2 \leq z_2^4 = u^2 < u^2 = v^2 = z_1.$$

This completes the **descent part** of the theorem.

To complete the proof, apply the descent argument again to produce solutions x_3, y_3, z_3 all positive, such that $(x_3, y_3) = 1$ and $0 < z_3 < z_2 < z_1$.

Continuing, we produce an infinite sequence of positive integers

$$0 < \cdots < z_4 < z_3 < z_2 < z_1.$$

But this is impossible, as there are a finite number of positive integers, giving us our desired contradiction. □

§36 The Method of Ascent

A variation of the method of descent is the method of ascent. Consider the equation in 4 variables:

$$x^2 + y^2 + z^2 = w^2. \tag{1}$$

Where x, y, z, $w > 0$ and $(x, y, z, w) = 1$. Geometrically, finding integral solutions of this equation is equivalent to finding a rectangular box with integral sides and diagonal.

Let's find solutions to the equation where x and y form two parts of a Pythagorean triple, say, $x^2 + y^2 = t^2$. Then,

$$t^2 + z^2 = x^2 + y^2 + z^2 = w^2. \tag{2}$$

Thus, (t, z, w) is also a Pythagorean triple. So we actually look for solutions to (1) that satisfy

$$x^2 + y^2 = t^2, \quad t^2 + z^2 = w^2$$
$$(x, y, z) = (t, z, w) = 1, \quad x, y, t, z, w > 0.$$

We try using descent, since x, y, t is a primitive Pythagorean triple, t is odd, and exactly one of x and y is even. Say x is odd and y is even. Similarily, t is odd, and so z must be even.

By our theorem about Pythagorean triples, we know that there are integers r, s, u, and $v > 0$ with $(r, s) = 1 = (u, v)$, exactly one of r and s is odd and

$$x = r^2 - s^2, \quad , y = 2rs, \quad t = r^2 + s^2$$
$$t = u^2 - v^2, \quad y = 2uv, \quad t = u^2 + v^2.$$

Look at parts involving t:

$$t = r^2 + s^2 = u^2 - v^2.$$

So $r^2 + s^2 + v^2 = u^2$. Also, $(r, s, v, u) = 1$ because $(r, s) = 1$, and

$$0 < u \leq u^2 < u^2 + v^2 = w.$$

So we have gone from one solution to (1), (x, y, z, w) to another (r, s, v, u) with $0 < u < w$.

Thus, we have "descended". However, we assumed our original solution satisfied equation (2), where we don't know if that's true about our "descended" solution. So we don't have a contradiction this way.

However, we can "ascend" as well, or go backwards.

Consider the solution $1^2 + 2^2 + 2^2 = 3^2$. Put $u = 3$ (so it is odd). Now v must be even, so let $v = 2$. Since $r > s$ we let $r = 2$ and $s = 1$.

This yields $x = 3$, $y = 4$, $t = 5$, $z = 12$, $w = 13$ by the above procedure. They satisfy the equation:

$$x^2 + y^2 + z^2 = w^2$$
$$3^2 + 4^2 + 12^2 = 13^2$$

Now we let $u = 13$, Again, v is then even, so we put $v = 12$ (we couldn't choose $v = 4$ because $(r, s) = (12, 3) \neq 1$).

Since $r > s$, we have $r = 4$, $s = 3$. Plug in and we get

$$x = 7, y = 24, t = 25, z = 312, w = 313.$$

Which is another solution to (2) which gives another solution to (1).

Keep going in this "ascending manner" and we see (1) has infinitely many solutions. As observed before, the solution to (2) as shown above geometrically describes a rectangular box with integral edges and with a diagonal on a face. So, we have proven there are infinitely many such boxes.

This method of ascent can also show that if $d > 0$, then if there is one solution to the Fermat-Pell equation

$$x^2 - dy^2 = 1, \quad x, y > 0$$

then there are infinitely many solutions. Moreover, if there is one solution to the equation

$$x^2 - dy^2 = -1, \quad x, y > 0$$

then there are infinitely many solutions.