Section 17

Infinite Descent and Fermat's Conjecture

Week 12

In Section 16 we found all possible integer solutions to the equation $x^2 + y^2 = z^2$. What happens when we consider higher order equations? Apart from the trivial solution $x = y = z = 0$, or $x = z$, $y = 0$, the equation

$$x^n + y^n = z^n, \qquad n \geq 3,$$

has no solution. This fact was known for over 300 years as **Fermat's Last Theorem**, although Fermat only claimed that he could prove it, but if he ever did, he never showed it to the rest of the world. It was finally proved by Andrew Wiles in 1995. Fermat, however, did prove the easiest case of this result, that there is no non-trivial solution to the equation

$$x^4 + y^4 = z^4. \tag{17.1}$$

17.1 The Equation $x^4 + y^4 = z^2$

It is sufficient to prove that there is no non-trivial solution to $x^4 + y^4 = z^2$, for in that case, if, to the contrary, $x = a$, $y = b$, $z = c$ were a solution to (17.1), we would have

$$a^4 + b^4 = c^4 = (c^2)^2,$$

a contradiction.

Theorem 17.1 *There are no non-trivial solutions of*

$$x^4 + y^4 = z^2. \tag{17.2}$$

17.2 Infinite Descent

To prove Theorem 17.1 one assumes, to the contrary, that (17.2) has non-trivial solutions. By the Well Ordering Principle, it has a solution with a smallest value of z^2; let c^2 be this smallest value of z^2. Then one constructs a smaller number with the same properties, hence obtaining a contradiction. This method is also called the **method of infinite descent**, for if one did not at the start assume that c was as small as possible, one could have constructed an infinite sequence of positive integers $\{t_i\}$ with $c > t_1 > t_2 > \cdots$, which would have contradicted the Well Ordering Principle.

The same method can be used to show that other equations of this type do not have non-trivial solutions.

Example: Show that there are no nontrivial integer solutions to $x^3 + 5y^3 = 25z^3$.

Solution

Suppose to the contrary that there are nontrivial solutions to

$$x^3 + 5y^3 = 25z^3$$

and let $(x, y, z) = (a, b, c)$ be one for which c is as small as possible. Thus

$$a^3 + 5b^3 = 25c^3.$$

- First show that $(a, b) = 1$.

  Suppose p is prime and $p|a$, $p|b$. Then

  $$(\frac{a}{p})^3 + 5(\frac{b}{p})^3 = \frac{1}{p^3}(a^3 + 5b^3) = \frac{1}{p^3}25c^3$$

  is an integer. Now p and 5 being prime implies $p^3 \nmid 5^2$, so $p|c^3$ and thus $p|c$ (again because p is prime), so $c/p \in \mathbb{Z}^+$, that is,

  $$(\frac{a}{p})^3 + 5(\frac{b}{p})^3 = 25(\frac{c}{p})^3$$

  where $c/p \in \mathbb{Z}^+$. This equation has the same form as the given one, hence by the choice of c, $\frac{c}{p} \geq c$. This is impossible if p is prime and so a and b are relatively prime.

Since $5|(25c^3 - 5b^3)$, it follows that $5|a^3$, and since 5 is prime, $5|a$. Say $a = 5k$ for some k. Then

$$(5k)^3 + 5b^3 = 25c^3,$$
$$\text{i.e.} \quad 25k^3 + b^3 = 5c^3.$$

But then evidently $5|b^3$ and so $5|b$, which is a contradiction since $5|a$ and $(a, b) = 1$.

The method of infinite descent can also be used to show that the square root of an integer which is not a perfect square, is irrational.

Example: Show that $\sqrt{21}$ is irrational.

Solution

Assume to the contrary that $\sqrt{21}$ is rational, and write it as a fraction in lowest form, say

$$\sqrt{21} = \frac{a}{b},$$

where $(a, b) = 1$ (i.e. b is as small as possible). Squaring both sides we get

$$a^2 = 21b^2. \tag{17.3}$$

Thus $7|a^2$, and since 7 is prime it follows that $7|a$. Say $a = 7c$. Then (17.3) becomes

$$49c^2 = 21b^2, \quad \text{i.e.} \quad 7c^2 = 3b^2.$$

Thus $7|3b^2$ and so $7|b$ as 7 is prime and $(3, 7) = 1$. But now $7|a$ and $7|b$, contradicting $(a, b) = 1$. [Or, if we write $b = 7d$, we see that $\sqrt{21} = 7c/7d = c/d$, where $d < b$, contradicting b being as small as possible.]

Section 18

Sums of Squares

In Section 16 we found all integer solutions to the equation $x^2 + y^2 = z^2$ (thus all right triangles with integer lengths). Suppose we are given an integer c, and required to find a fundamental Pythagorean triangle with hypotenuse c. By Theorem 16.1, this will only be possible if c can be written as the sum of two squares, m^2 and n^2, such that m and n satisfy the conditions given in the theorem. So here is a good question: Which positive integers can be written as the sum of two squares?

Although it is not true that any square t^2 can be written as a sum of squares $r^2 + s^2 = t^2$, where $r, s > 0$ (for example 3^2 cannot be written in this way), we can still write t^2 as the sum of two squares if we relax the condition that $r, s > 0$, namely $t^2 = t^2 + 0^2$. So in this section we will allow one of r and s to be 0. Look at the numbers in Table 18.1.

1	2	[3]	4	5	[6]	[7]	8	9	10
[11]	[12]	13	[14]	[15]	16	17	18	[19]	20
[21]	[22]	[23]	[24]	25	26	[27]	[28]	29	[30]
[31]	32	[33]	34	[35]	36	37	[38]	[39]	40
41	[42]	[43]	[44]	45	[46]	[47]	[48]	49	50

Table 18.1: Sums of two squares

Those inside the rectangles cannot be written as the sum of two squares. What do they have in common, and how do they differ from the others?

Each $n \equiv 3 \pmod 4$ lies inside a rectangle, but many others do, too.

★ It is easy to prove that if $n \equiv 3 \pmod 4$, then n cannot be written as the sum of two squares – suppose $n = a^2 + b^2$ and consider the least residues of a and $b \pmod 4$. (See Assignment 2, 3(c).)

18.1 Numbers Representable as Sums of Two Squares

We will prove that the numbers which can be represented as the sum of two squares are precisely the following numbers:

Theorem 18.1 *The integer n can be written as the sum of two squares if and only if each prime p, where $p \equiv 3 \pmod 4$, occurs to an even power in the prime factorization of n.*

18.2 Proof of Necessity (Contrapositive)

Theorem 18.2 *If p is prime, $p \equiv 3 \pmod 4$, and p occurs to an odd power in the prime-power decomposition of n, then n cannot be written as the sum of two squares.*

Proof. Let p satisfy the hypothesis of the theorem. Then n can be written as $n = p^{2e+1}m$, where $e \geq 0$ and $(p, m) = 1$. Suppose to the contrary that $n = x^2 + y^2$ for some $x, y \in \mathbb{Z}^+$.

★ We will obtain a contradiction, namely that -1 is a quadratic residue of p, which it isn't, since $(-1/p) = -1$ if $p \equiv 3 \pmod 4$. (Theorem 11.5)

Let $(x, y) = d$ and say $d = p^k d_1$, where $k \geq 0$ and $\boxed{(d_1, p) = 1}$. Then $p^{2k}|x^2$ and $p^{2k}|y^2$, hence $p^{2k}|n$. Let $x_1 = x/p^k$, $y_1 = y/p^k$ and $n_1 = n/p^{2k}$. Then

$$n_1 = x_1^2 + y_1^2 \quad \text{and} \quad (x_1, y_1) = d_1. \tag{18.1}$$

★ We show that $p|n_1$.

- Since (a) $n = p^{2e+1}m$, (b) $(p, m) = 1$ and (c) $p^{2k}|n$, it follows that $p^{2k}|p^{2e+1}$. Therefore

(*i*) $2e + 1 \geq 2k$. Since $2e + 1$ is odd and $2k$ is even, $2e + 1 > 2k$.

From (a) and the definition of n_1,

$$n_1 = \frac{n}{p^{2k}} = p^{2e+1-2k}m.$$

Therefore

(*ii*) $p^{2e+1-2k}$ is a divisor of n_1.

Since $2e + 1 > 2k$, $2e + 1 - 2k \geq 1$, and then (*ii*) implies that $p|n_1$. Thus

$$n_1 \equiv 0 \pmod p.$$

Now if $p|x_1$, then by (18.1) $p|y_1$ and thus $p|d_1$. But $(d_1, p) = 1$, hence $p \nmid x_1$. Since p is prime, it follows that $(x_1, p) = 1$. Therefore the congruence

$$x_1 z \equiv y_1 \pmod{p}$$

(with z as the variable) has a solution. Say $z = u$ is a solution. Then

$$0 \equiv n_1 \equiv x_1^2 + y_1^2 \equiv x_1^2 + (x_1 u)^2 \equiv x_1^2(1 + u^2) \pmod{p}.$$

Since $(x_1, p) = 1$, we may divide the congruence $x_1^2(1 + u^2) \equiv 0 \pmod{p}$ by x_1^2 to get

$$1 + u^2 \equiv 0 \pmod{p},$$
$$\text{i.e.} \quad u^2 \equiv -1 \pmod{p}.$$

But then -1 is a quadratic residue of $p \equiv 3 \pmod{4}$, contrary to Theorem 11.5. ■

18.3 Proof of Sufficiency

We must prove that the converse of Theorem 18.2 also holds. We need several lemmas.

We use a different proof to the one given in Dudley.

18.3.1 Some Lemmas

Lemma 18.1 *For any integers a, b, c, d,*

$$(a^2 + b^2)(c^2 + d^2) = (ac + bd)^2 + (ad - bc)^2.$$

Thus the product of the sum of two squares is also the sum of two squares.

Proof. Multiply both sides out. ■

Lemma 18.2 *If n is representable as the sum of two squares, then so is $k^2 n$.*

Proof. If $n = x^2 + y^2$, then $k^2 n = (kx)^2 + (ky)^2$. ■

Lemma 18.3 *Any integer n can be written in the form*

$$n = k^2 p_1 p_2 ... p_r,$$

where k is an integer and the p_i are distinct primes.

Proof.
Suppose n has distinct prime factors p_1, p_2, ..., p_r, p_{r+1}, ..., p_s, where we may assume the p_j have been arranged so that p_1, p_2, ..., p_r occur to odd powers and p_{r+1}, ..., p_s to even powers. (It is possible that $r = 0$ or $r = s$.) Thus we may write

$$\begin{aligned} n &= (p_1^{2e_1+1}p_2^{2e_2+1}...p_r^{2e_r+1})(p_{r+1}^{2e_{r+1}}...p_s^{2e_s}) \\ &= (p_1^{2e_1}p_2^{2e_2}...p_r^{2e_r}p_{r+1}^{2e_{r+1}}...p_s^{2e_s})(p_1p_2...p_r) \\ &= (p_1^{e_1}p_2^{e_2}...p_r^{e_r}p_{r+1}^{e_{r+1}}...p_s^{e_s})^2(p_1p_2...p_r) \\ &= k^2p_1p_2...p_r. \end{aligned}$$

■

Corollary 18.1 *If the prime-power decomposition of n contains no prime p, where $p \equiv 3 \pmod 4$, to an odd power, then*

$$n = k^2p_1p_2...p_r \quad \text{or} \quad n = 2k^2p_1p_2...p_r$$

for some k and r, where each p_i is congruent to $1 \pmod 4$.

Corollary 18.2 *To prove Theorem 18.1, it is now sufficient to prove that if p is a prime and $p \equiv 1 \pmod 4$, then p is representable as the sum of two squares.*

Proof. Consider the prime-power decomposition of n. If some prime congruent to $3 \pmod 4$ occurs to an odd power, then by Theorem 18.2 n is not representable as the sum of two squares. If no prime congruent to $3 \pmod 4$ occurs to an odd power, then by Corollary 18.1,

$$n = k^2p_1p_2...p_r \quad \text{or} \quad n = 2k^2p_1p_2...p_r$$

for some k and r, where each p_i is congruent to $1 \pmod 4$.
We know that $2 = 1^2 + 1^2$. If each p_i is the sum of two squares, we can apply Lemma 18.1 several times to show that $p_1p_2...p_r$ and $2p_1p_2...p_r$ are sums of two squares. Then by Lemma 18.2, $k^2p_1p_2...p_r$ and $2k^2p_1p_2...p_r$ are sums of two squares. ■

We still need to prove:

Theorem 18.3 If p is prime and $p \equiv 1 \pmod 4$, then p is representable as the sum of two squares.

★ We shall also show how to construct such a sum.

★ We need two more lemmas (the first one a by now familiar consequence of Wilson's Theorem (Theorem 6.2)) that will help us to actually *find* integers m and n such that $p = m^2 + n^2$.

18.3.2 A result based on Wilson's Theorem

Lemma 18.4 *If p is prime and $p \equiv 1 \pmod 4$, then*

$$\left[\left(\frac{p-1}{2}\right)!\right]^2 \equiv -1 \pmod p.$$

Proof. Let $p = 4k + 1$ for some integer k. By Wilson's Theorem (Theorem 6.2),

$$(p-1)! \equiv (4k)! \equiv -1 \pmod p.$$

But

$$\begin{aligned} 4k &\equiv p-1 \equiv -1 \pmod p \\ 4k-1 &\equiv p-2 \equiv -2 \pmod p \\ &\vdots \\ 2k+1 &\equiv p-2k \equiv -2k \pmod p. \end{aligned}$$

Hence we have

$$\begin{aligned} -1 \equiv (p-1)! &\equiv 4k(4k-1)\cdots(2k+1)(2k)\cdots(2)(1) \pmod p \\ &\equiv (-1)(-2)\cdots(-2k)(2k)\cdots(2)(1) \pmod p \\ &\equiv (-1)^{2k}[(2k)\cdots(2)(1)]^2 \pmod p \\ &\equiv [(2k)!]^2 \equiv \left[\left(\frac{p-1}{2}\right)!\right]^2 \pmod p. \end{aligned}$$

■

18.3.3 Thue's Lemma

The next lemma is due to the Norwegian mathematician Axel Thue and relies on Dirichlet's pigeonhole principle.

Recall that $\lceil x \rceil$ (the ceiling function) is the smallest integer not less than x. If x is an integer, then $\lceil x \rceil = x$. If x is not an integer, then $\lceil x \rceil > x$.

- **Pigeonhole Principle.** If n objects (pigeons) are placed into m boxes (pigeonholes), where $m < n$, then some box will contain at least two objects.

Example

Consider the set $S = \{(x, y) : x \in \{0, 1\},\ y \in \{0, 1\}\}$. There are two ways to choose x and two ways to choose y to construct elements of S, so $|S| = 2 \times 2 = 4$ and, indeed, $S = \{(0, 0), (0, 1), (1, 0), (1, 1)\}$.

For each $(x, y) \in S$, consider the integer $5x - y$. There are four of them. Think of them as the pigeons. There are three least residues (mod 3). Think of them as the pigeonholes.

So two of the integers $5x - y$ must have the same least residue (mod 3). The numbers are 0, -1, 5 and 4, and we see that $-1 \equiv 5 \equiv 2 \pmod 3$.

Lemma 18.5 (Thue's Lemma) *Let p be a prime and a an integer such that $(a, p) = 1$. Then the congruence (in two variables x and y)*

$$ax \equiv y \pmod p$$

is satisfied by $x = x_0$, $y = y_0$, where

$$0 < |x_0| < \sqrt{p} \quad \textit{and} \quad 0 < |y_0| < \sqrt{p}.$$

Proof.
Let $k = \lceil \sqrt{p} \rceil$. Because p is prime, $\sqrt{p}$ is not an integer, and so $k = \lceil \sqrt{p} \rceil > \sqrt{p} > k - 1$. Therefore $k^2 > p$. Consider the set

$$S = \{(x, y) : x \in \{0, 1, ..., k-1\},\ y \in \{0, 1, ..., k-1\}\}.$$

There are k possible values for x and k possible values for y, so $|S| = k^2 > p$. For each $(x, y) \in S$, consider the integer $ax - y$. There are $k^2 > p$ of them. By the pigeonhole principle at least two of these integers have the same least residue (mod p), so are congruent (mod p); say $ax_1 - y_1 \equiv ax_2 - y_2 \pmod p$, where

$$x_1 \neq x_2 \quad \text{or} \quad y_1 \neq y_2. \tag{18.2}$$

Then

$$ax_1 - ax_2 \equiv a(x_1 - x_2) \equiv y_1 - y_2 \pmod p.$$

Let $x_0 = x_1 - x_2$ and $y_0 = y_1 - y_2$. Then x_0 and y_0 satisfy the congruence $ax \equiv y \pmod p$. Also,

$$-(k-1) \leq x_0 \leq k-1 \quad \text{and} \quad -(k-1) \leq y_0 \leq k-1,$$

i.e.

$$|x_0| \leq k-1 \quad \text{and} \quad |y_0| \leq k-1. \tag{18.3}$$

- If $x_0 = 0$, then the congruence $ax_0 \equiv y_0 \pmod p$ and (18.3) imply that $y_0 = 0$.
- If $y_0 = 0$, then $ax_0 \equiv 0 \pmod p$, and since $(a, p) = 1$, we can cancel a to get $x_0 \equiv 0 \pmod p$. Again (18.3) implies that $x_0 = 0$.

In each case we obtain a contradiction to (18.2). Hence, as required,

$$0 < |x_0| \leq k - 1 < \sqrt{p} \quad \text{and} \quad 0 < |y_0| \leq k - 1 < \sqrt{p}. \qquad \blacksquare$$