

**Math 104B, Number Theory, Winter 2003.**

**Lecture 25. Pythagorean Triples.**

If  $d$  is a positive integer which is not a perfect square then the equation  $x^2 - dy^2 = -1$  has solutions if and only if the smallest period of the continued fraction expansion of  $\sqrt{d}$  is odd. We saw that if  $d \equiv 0$  or  $3$  modulo  $4$ , then there are no solutions.

**Proposition 14.5.11** (Lagrange). If  $p$  is a prime such that  $p \equiv 1 \pmod{4}$  then the equation  $x^2 - py^2 = -1$  has a solution.

We can also study the equation  $x^2 - dy^2 = n$  for other values of  $n$ .

**Proposition 14.5.10.** If the equation  $x^2 - dy^2 = m$  has one solution, then it has infinitely many.

**Example 14.2.1.** The equation  $x^2 - 7y^2 = 3$  has no solutions.

We gave the proofs of these results from the book.

**Pythagorean Triples.** A **Pythagorean triple** is a list  $x, y, z$  of three integers satisfying  $x^2 + y^2 = z^2$ . It is **primitive** if the greatest common divisor  $(x, y, z) = 1$ . Any pythagorean triple is obtained by taking multiples of a primitive one.

**Theorem 14.3.2.** A primitive pythagorean triple  $x, y, z$  with  $y$  even is primitive if and only if it has the form

$$(*) \quad x = r^2 - s^2, \quad y = 2rs, \quad z = r^2 + s^2,$$

where  $r$  and  $s$  are relatively prime integers with  $rs$  even.

Note that any primitive Pythagorean triple either has  $x$  odd and  $y$  even or  $x$  even and  $y$  odd. This is by considering the equation  $x^2 + y^2 \equiv z^2 \pmod{4}$ .

**Proof 1.** We assume that  $x, y, z$  is a primitive pythagorean triple. We have just seen that  $x$  and  $z$  are odd, so we can write the equation in the form

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

Set  $d$  to be the greatest common divisor,

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

Then  $d$  divides  $(x+z)/2 + (x-z)/2 = x$  and  $(x+z)/2 - (x-z)/2 = z$ , so  $d$  divides  $(x, z)$ . But then  $(x, z) = 1$ , since the relationship  $x^2 + y^2 = z^2$  ensures that  $(x, z) = (x, y, z) = 1$ . Hence  $(x-z)/2$  and  $(x+z)/2$  are perfect squares, that is

$$\frac{x-z}{2} = s^2, \quad \frac{x+z}{2} = r^2, \quad \left(\frac{y}{2}\right)^2 = (rs)^2$$

1

and switching the sign of  $r$  if necessary to obtain the correct sign for  $y$ , we get (\*). If  $r$  and  $s$  are odd then  $x$ ,  $y$  and  $z$  are even which is a contradiction, and so  $rs$  is even. Since  $(x, y, z) = 1$ , we see that  $r$  and  $s$  are relatively prime.

Conversely, if  $r$  and  $s$  are relatively prime with  $rs$  even, then  $x, y, z$  given by (\*) is clearly a pythagorean triple. To see that it is primitive, if  $d$  divides  $x$ ,  $y$  and  $z$  then  $d|x + z = 2r^2$  and  $d|z - x = 2s^2$  so  $d|(2r^2, 2s^2) = 2(r^2, s^2) = 2$ . But one of  $r, s$  is even and the other is odd, so  $x$  is odd and  $d|x$  implies  $d = 1$ .

We give here the other proof in the book which is easier to generalize. This was not covered in the lecture.

First we make a note of a useful formula: if  $a = 2^k a'$  and  $b = 2^\ell b'$  where  $a'$  and  $b'$  are odd, then

$$(a - b, a + b) = \begin{cases} (a, b) & \text{if } k \neq \ell, \\ 2(a, b) & \text{if } k = \ell. \end{cases}$$

**Proof 2.** We notice that there is a one-to-one correspondence between primitive Pythagorean triples and rational points on the unit circle by the map

$$x, y, z \quad \rightarrow \quad \left( \frac{x}{z}, \frac{y}{z} \right).$$

Consider a line through  $(-1, 0)$  which intersects the unit circle center the origin in the rational point  $(u, v)$ . Then the slope of the line is rational, and can be written as  $s/r$  where  $r$  and  $s$  are relatively prime integers. Conversely, we will see that if the slope is rational then the intersection with the circle is a rational point. Indeed, the line has parametric equation

$$u = t - 1, \quad v = st,$$

So the equation  $u^2 + v^2 = 1$  becomes  $1 = (t - 1)^2 + ((s/r)t)^2 = t^2 - 2t + 1 + (s/r)^2 t^2$  which is equivalent to  $t^2(1 + (s/r)^2) - 2t = 0$  or

$$t((1 + (s/r)^2)t - 2) = 0.$$

One solution  $t = 0$  corresponds to the point  $(-1, 0)$  and the other one  $t = 2/(1 + (s/r)^2)$  gives the point

$$(u, v) = \left( \frac{r^2 - s^2}{r^2 + s^2}, \frac{2rs}{r^2 + s^2} \right).$$

Now we wish to recover a primitive triple  $x, y, z$  from this. We see that since  $r$  and  $s$  are relatively prime,

$$(r^2 - s^2, r^2 + s^2) = \begin{cases} 2 & rs \text{ odd,} \\ 1 & rs \text{ even.} \end{cases}$$

2

If  $rs$  is even then, the solution is given by (\*). If  $r$  and  $s$  are both odd, then we multiply up by  $(r^2 + s^2)/2$  instead of  $r^2 + s^2$  and set

$$\begin{aligned}x &= rs = \left(\frac{r+s}{2}\right)^2 - \left(\frac{r-s}{2}\right)^2 \\y &= \frac{r^2 - s^2}{2} = \frac{r-s}{2} \frac{r+s}{2}, \\z &= \frac{r^2 + s^2}{2} = \left(\frac{r+s}{2}\right)^2 + \left(\frac{r-s}{2}\right)^2\end{aligned}$$

The numbers  $m = (r+s)/2$  and  $n = (r-s)/2$  are relatively prime and by considering the fact that  $r^2 - s^2 \equiv 0$  modulo 8, we see that  $mn$  is even.