

## Math 445 Number Theory

September 22, 2004

*Proposition:* If  $(x, y) = 1$  and  $xy = c^2$ , then  $x = u^2, y = v^2$  for some integers  $u, v$ .

Basic idea: write their prime factorizations  $x = p_1^{k_1} \cdots p_r^{k_r}$ ,  $y = p_{r+1}^{k_{r+1}} \cdots p_s^{k_s}$ . Since  $(x, y) = 1$  their factorizations have no primes in common. Since

$c^2 = xy = p_1^{k_1} \cdots p_r^{k_r} p_{r+1}^{k_{r+1}} \cdots p_s^{k_s}$ , this is its prime decomposition. Since  $c^2$  is a square, all of the exponents are even,  $k_i = 2t_i$ . So  $x = (p_1^{t_1} \cdots p_r^{t_r})^2$  and  $y = (p_{r+1}^{t_{r+1}} \cdots p_s^{t_s})^2$  are both squares.

Since  $a^2 + b^2 = c^2$  implies  $a = 2uv$ ,  $b = u^2 - v^2$ ,  $c = u^2 + v^2$ , it is straightforward to see that any even number  $a = 2(n)(1)$ , or any odd number  $b = (n+1)^2 - n^2 = 2n+1$ , can occur on the left side of a Pythagorean triple  $a^2 + b^2 = c^2$ . Which numbers can occur on the right-hand side,  $c = u^2 + v^2$ , is a more involved question. [Certainly, 3 cannot be expressed as a sum of squares...] Answering this question will lead us to some more interesting number theory! After noting that  $(a^2 + b^2)(c^2 + d^2) = (ac + bd)^2 + (ad - bc)^2 = (ad + bc)^2 + (ac - bd)^2$ , a more pointed question to ask might be: *which primes  $p$  can be expressed as  $p = u^2 + v^2$ ?* A bit of experimentation quickly leads us to the

*Conjecture:* A prime  $p$  is a sum of two squares  $\Leftrightarrow (p = 2 \text{ or } p \equiv 1 \pmod{4})$ .

This is certainly true for  $2 = 1^2 + 1^2$ , and so what we need to show is (1) if  $p \equiv 1 \pmod{4}$  is prime, then  $p = u^2 + v^2$ , and (2) if  $p \equiv 3 \pmod{4}$  is prime, then  $p = u^2 + v^2$  is impossible. Forgetting that we have already proved (2) [ $u^2, v^2 \equiv 0 \text{ or } 1 \pmod{4}$ , so the sum can't be  $\equiv 3$ ], it turns out that what is really relevant to the discussion is under what circumstances the equation  $x^2 \equiv -1 \pmod{p}$  has a solution! But first, we need:

*Wilson's Theorem:* If  $p$  is prime, then  $(p-1)! \equiv -1 \pmod{p}$ .

The idea: every  $k = 1, 2, \dots, p-1$  has an inverse, mod  $p$ . For everyone except 1 and  $p-1$ , it is not  $k$  (but is unique), so every factor in  $2 \cdot 3 \cdots (p-2)$  can be paired up with its inverse. So by reordering things,  $2 \cdot 3 \cdots (p-2)$  is a product of 1's, mod  $p$ , so is 1. Then  $(p-1)! \equiv 1 \cdot (p-1) \equiv p-1 \equiv -1 \pmod{p}$ , as desired.

This in turn allows us to show that

*Theorem:* If  $p$  is prime, the equation  $x^2 \equiv -1 \pmod{p}$  has a solution  $\Leftrightarrow p = 2 \text{ or } p \equiv 1 \pmod{4}$ .

Checking this for  $p = 2$  is quick ( $x = 1$  works), and so we need to show that (1) if  $p \equiv 1 \pmod{4}$  then  $x^2 \equiv -1 \pmod{p}$  has a solution, and (2) if  $p \equiv 3 \pmod{4}$  then  $x^2 \equiv -1 \pmod{p}$  has no solution.

To see the first, since  $p-1 = 4k$  for some  $k$ , we have, by Wilson's Theorem, that  $1 \cdot 2 \cdots (4k-1)(4k) \equiv -1 \pmod{p}$ . But, mod  $p$ ,  $1 \cdot 2 \cdots (4k-1)(4k) = 1 \cdot 2 \cdots (2k)(2k+1) \cdots (4k-1)(4k) = 1 \cdot 2 \cdots (2k)(p-2k)(p-(2k-1)) \cdots (p-2)(p-1) \equiv 1 \cdot 2 \cdots (2k)(-2k)(-(2k-1)) \cdots (-2)(-1) = (2k)!(2k)!(-1)^{2k} = ((2k)!)^2 = x^2$ , where  $x = (2k)!$ . so  $x^2 \equiv -1 \pmod{p}$  has a solution.

The second half we will do next time.