New Zealand Mathematical Olympiad Committee

Primes that are Sums of Two Squares

Arkadii Slinko

1 Introduction

These notes give a number of number theoretic applications of the Pigeonhole Principle. In particular we prove Fermat's theorem on primes of the form $4n + 1$.

2 Congruences

First a short summary of some facts about congruences. An excellent reference for this section's results is Richard Courant and Herbert Robbins' *What is Mathematics?* (Section 2, Supplement to Chapter 1).

Let m be an integer. We write

$$a \equiv b \pmod{m},$$

and say that a is congruent to b modulo m, if a and b have the same remainder on division by m. Equivalently, $a \equiv b \bmod m$ if and only if $a - b$ is divisible by m. The following facts about congruences will be used without explicit mention, and can be easily proved:

1. If $a \equiv b \bmod m$ and $c \equiv d \bmod m$, then $a + c \equiv b + d \bmod m$.
2. If $a \equiv b \bmod m$ and $c \equiv d \bmod m$, then $ac \equiv bd \bmod m$.

Lemma 1. *Let p be a prime. Then for every positive integer a such that $0 < a < p$ there exists a unique positive integer b such that $ab \equiv 1 \bmod p$ and $0 < b < p$.*

The number b will be called the inverse of a modulo p.

Proof. Let us consider the numbers

$$1 \cdot a,\ 2 \cdot a,\ \ldots\ , (p-1) \cdot a$$

or rather their remainders on division by p. These remainders must be all different. For if

$$i \cdot a \equiv j \cdot a \pmod{p}$$

for some integers $1 \le i < j \le p-1$ and j, then $i \cdot a - j \cdot a = (i-j)a$ must be divisible by p, which is impossible as $i - j$ and a are both smaller than p.

Therefore (Pigeonhole Principle!) one of these remainders must be 1. Thus $k \cdot a \equiv 1 \bmod p$ for some integer k such that $0 < k < p-1$, and we can set $b = k$. Suppose that this inverse is not unique; that is, that there is another positive integer c such that $0 < c < p$ and $ac \equiv 1 \bmod p$. Then we can consider the product bac, for which we will have

$$bac = (ba)c \equiv 1 \cdot c = c \pmod{p},$$
$$bac = b(ac) \equiv b \cdot 1 = b \pmod{p}.$$

Hence $b \equiv c \bmod p$, which implies $b = c$. □

Theorem 2 (Wilson)**.** *Let p be a prime. Then*

$$(p-1)! \equiv -1 \bmod p.$$

Proof. Modulo p, the residues 1 and $p-1$ are their own inverses. We claim there are no other such residues. Indeed, if $x^2 \equiv 1 \bmod p$, for some $0 < x < p$, then $x^2 - 1 \equiv 0 \bmod p$. That is, $x^2 - 1 = (x-1)(x+1)$ is divisible by p, which means either $x-1$ or $x+1$ is divisible by p. Thus $x = 1$ or $x = p-1$.

This means that all numbers $2, 3, \ldots, p-2$ can be split into pairs so that in each pair the integers are mutual inverses. Hence

$$(p-2)! \equiv 1 \pmod{p}.$$

So

$$(p-1)! = (p-2)!(p-1) \equiv p - 1 \equiv -1 \pmod{p}.$$

and Wilson's theorem follows. □

3 Fermat's theorem

Lemma 3. *Let $n > 1$ be a positive integer. Then for every positive integer u there exist integers x, y,not both zero, such that $0 \le |x| \le \sqrt{n}$ and $0 \le |y| \le \sqrt{n}$ and $xu \equiv y \bmod n$.*

Proof. Let $k = \lfloor \sqrt{n} \rfloor$ be the integer part of $\sqrt{n}$. Then $k^2 \le n < (k+1)^2$. Let us consider the $(k+1)^2$ integers

$$xu - y,$$

where both x and y take values from the set $\{0, 1, 2, \ldots, k\}$. As $n < (k+1)^2$, we have more such differences than remainders on dividing by n. Thus, by the Pigeonhole Principle, two such differences are congruent modulo n; that is,

$$x_1 u - y_1 \equiv x_2 u - y_2 \pmod{n}$$

for some x_1, x_2, y_1, y_2, where either $x_1 \ne x_2$ or $y_1 \ne y_2$. Hence

$$(x_1 - x_2)u \equiv y_1 - y_2,$$

and $x = x_1 - x_2$ and $y = y_1 - y_2$ satisfy the conditions of the lemma. □

Theorem 4 (Fermat)**.** *Let $p = 4n + 1$ be a prime. Then there exist positive integers x and y such that $x^2 + y^2 = p$.*

Proof. We will prove, first, that $u^2 \equiv -1 \bmod p$ for $u = ((p-1)/2)!$. We note that

$$\begin{array}{rcl} p-1 & \equiv & -1 \pmod{p}, \\ p-2 & \equiv & -2 \pmod{p}, \\ & \ldots & \\ (p-1)/2 + 1 & \equiv & -(p-1)/2 \pmod{p} \end{array}$$

where we have $(p-1)/2 = 2n$, i.e. an even number, of such pairs. Multiplying them all, we get

$$\frac{(p-1)!}{((p-1)/2)!} \equiv (-1)^{2n}(((p-1)/2)!) = (((p-1)/2)!) \pmod{p}.$$

Since, by Wilson's theorem

$$(p-1)! \equiv -1 \pmod{p},$$

this implies

$$-1 \equiv (p-1)! \equiv (((p-1)/2)!)^2 = u^2 \pmod{p}.$$

Now we will use Lemma 3, to find two integers x, y such that

1. $0 \le |x| \le \sqrt{p}$ and $0 \le |y| \le \sqrt{p}$; and,

2. $xu \equiv y \bmod p$.

Since $\sqrt{p}$ is not a whole number, the inequalities in the first property are strict; that is, $0 \leq |x| < \sqrt{p}$ and $0 \leq |y| < \sqrt{p}$. So $x^2 < p$ and $y^2 < p$, and hence

$$0 < x^2 + y^2 < 2p.$$

From the second property, we get that $y^2 \equiv x^2u^2 \equiv -x^2 \bmod p$, so

$$x^2 + y^2 \equiv 0 \bmod p$$

Combining these gives $x^2 + y^2 = p$, which proves the theorem. □

4 Problems

1. Given n pairwise coprime positive integers which are greater than 1 but smaller than $(2n-1)^2$, prove that at least one of them is prime.

January 24, 2009

http://www.mathsolympiad.org.nz