PROBLEM SET 14: FERMAT'S LITTLE THEOREM

Supplement:

(from Art of Problem Solving)

We are particularly interested in Proof 2 (Inverses).

Statement

If a is an integer, p is a prime number and a is not divisible by p, then $a^{p-1} \equiv 1 \pmod{p}$.

A frequently used corollary of Fermat's Little Theorem is $a^p \equiv a \pmod{p}$. As you can see, it is derived by multipling both sides of the theorem by a. The restated form is nice because we no longer need to restrict ourselves to integers a not divisible by p.

This theorem is a special case of Euler's Totient Theorem, which states that if a and n are integers, then $a^{\varphi(n)} \equiv 1 \pmod{n}$, where $\varphi(n)$ denotes Euler's totient function. In particular, $\varphi(p) = p - 1$ for prime numbers p. In turn, this is a special case of Lagrange's Theorem.

In contest problems, Fermat's Little Theorem is often used in conjunction with the Chinese Remainder Theorem to simplify tedious calculations.

Proof

We offer several proofs using different techniques to prove the statement $a^p \equiv a \pmod{p}$. If $\gcd(a, p) = 1$, then we can cancel a factor of a from both sides and retrieve the first version of the theorem.

Proof 1 (Induction)

The most straightforward way to prove this theorem is by by applying the induction principle. We fix p as a prime number. The base case, $1^p \equiv 1 \pmod{p}$, is obviously true. Suppose the statement $a^p \equiv a \pmod{p}$ is true. Then, by the binomial theorem,

$$(a+1)^p = a^p + \binom{p}{1}a^{p-1} + \binom{p}{2}a^{p-2} + \cdots + \binom{p}{p-1}a + 1.$$

Note that p divides into any binomial coefficient of the form $\binom{p}{k}$ for $1 \le k \le p-1$. This follows by the definition of the binomial coefficient as $\binom{p}{k} = \frac{p!}{k!(p-k)!}$; since p is prime, then p divides the numerator, but not the denominator.

Taken $\bmod p$, all of the middle terms disappear, and we end up with $(a+1)^p \equiv a^p + 1 \pmod{p}$. Since we also know that $a^p \equiv a \pmod{p}$, then $(a+1)^p \equiv a + 1 \pmod{p}$, as desired.

Proof 2 (Inverses)

Let $S = \{1, 2, 3, \cdots, p-1\}$. Then, we claim that the set $a \cdot S$, consisting of the product of the elements of S with a, taken modulo p, is simply a permutation of S. In other words,

$$S \equiv \{1a, 2a, \cdots, (p-1)a\} \pmod{p}.$$

Clearly none of the ia for $1 \le i \le p-1$ are divisible by p, so it suffices to show that all of the elements in $a \cdot S$ are distinct. Suppose that $ai \equiv aj \pmod{p}$ for $i \ne j$. Since $\gcd(a, p) = 1$, by the cancellation rule, that reduces to $i \equiv j \pmod{p}$, which is a contradiction.

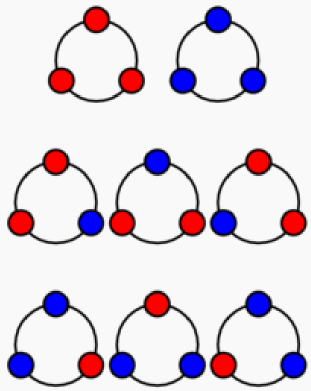
Thus, $\bmod p$, we have that the product of the elements of S is

$$1a \cdot 2a \cdots (p-1)a \equiv 1 \cdot 2 \cdots (p-1) \pmod{p}.$$

Cancelling the factors $1, 2, 3, \ldots, p-1$ from both sides, we are left with the statement $a^{p-1} \equiv 1 \pmod{p}$.

A similar version can be used to prove Euler's Totient Theorem, if we let $S = \{\text{natural numbers relatively prime to and less than } n\}$.

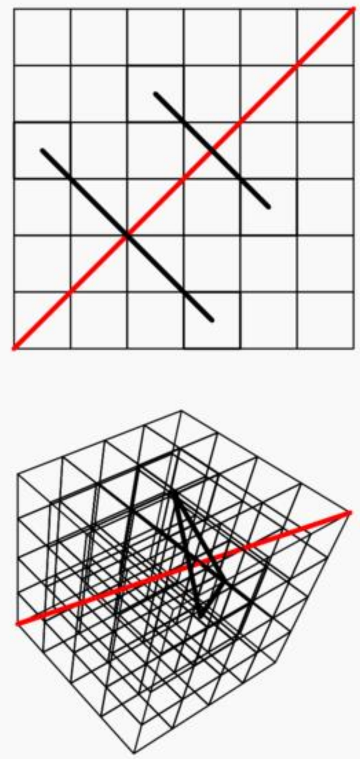
Proof 3 (Combinatorics)



An illustration of the case $p = 3, a = 2$.

Consider a necklace with p beads, each bead of which can be colored in a different ways. There are a^p ways to pick the colors of the beads. a of these are necklaces that consists of beads of the same color. Of the remaining necklaces, for each necklace, there are exactly $p - 1$ more necklaces that are rotationally equivalent to this necklace. It follows that $a^p - a$ must be divisible by p. Written in another way, $a^p \equiv a \pmod{p}$.

Proof 4 (Geometry)



For $p = 2, 3$ and $a = 6, 4$, respectively.

We imbed a hypercube of side length a in $\mathbb{R}^p$ (the p-th dimensional Euclidean space), such that the vertices of the hypercube are at $(\pm a/2, \pm a/2, \ldots, \pm a/2)$. A hypercube is essentially a cube, generalized to higher dimensions. This hypercube consists of a^p separate unit hypercubes, with centers consisting of the points

$$P(x_1, x_2, \ldots, x_n) = \left(a + \frac{1}{2} - x_1, a + \frac{1}{2} - x_2, \ldots, a + \frac{1}{2} - x_p\right),$$

where each x_i is an integer from 1 to a. Besides the a centers of the unit hypercubes in the main diagonal (from $(-a/2, -a/2, \ldots, -a/2)$ to $(a/2, a/2, \ldots, a/2)$), the transformation carrying

$$P(x_1, x_2, \ldots, x_n) \mapsto P(x_2, x_3, \ldots, x_n, x_1)$$

maps one unit hypercube to a distinct hypercube. Much like the combinatorial proof, this splits the non-main diagonal unit hypercubes into groups of size p, from which it follows that $a^p \equiv a \pmod{p}$. Thus, we have another way to visualize the above combinatorial proof, by imagining the described transformation to be, in a sense, a rotation about the main diagonal of the hypercube.