Fermat's Little Theorem

Fermat's little theorem is so called to distinguish it from the famous "Fermat's Last Theorem," a result which has intrigued mathematicians for over 300 years. Fermat's Last Theorem was only recently proved, with great difficulty, in 1994.[1] Before proving the little theorem, we need the following result on binomial coefficients.

Theorem: If p is a prime, then $\binom{p}{i}$ is divisible by p for $0 < i < p$. Otherwise put, $\binom{p}{i} \equiv 0 \mod p$ for $0 < i < p$.

For example, the 7th row of Pascal's triangle is 1 7 21 35 35 21 7 1. Here, $p = 7$ and the row itself consist of $\binom{7}{i}$ for $0 \le i \le 7$. Other than these, the numbers are $\binom{7}{i}$ for $0 < i < 7$, and we see that they are all divisible by 7, as predicted by the theorem.

The idea behind the proof is to notice that $\binom{p}{i} = \frac{p!}{i!(p-i)!}$. The numerator has a factor p and it cannot be canceled by any factor in the denominator. To prove the result mor formally for any prime p, we have

$$\binom{p}{i} = \frac{p!}{i!(p-i)!}$$

This shows that

$$i!(p-i)! \text{ divides } p! = p(p-1)!.$$

But $i!(p-i)!$ is relatively prime to p since all of its factors are smaller than p.[2] It follows that

$$i!(p-i)! \text{ divides } (p-1)!.$$

So

$$\binom{p}{i} = p \cdot \frac{(p-1)!}{i!(p-i)!}$$

This proves the result.

We can now state and prove Fermat's Little Theorem.

[1] See the Koshy text, pp 544–550.

[2] Here is where we use $0 < i < p$.

Theorem: (Fermat). If p is a prime and a is any number not divisible by p, then

$$a^{p-1} \equiv 1 \bmod p$$

For example, we know from this, without calculating, that $3^{22} \equiv 1 \bmod 23$.

It's more convenient to prove

$$a^p \equiv a \bmod p \text{ for all } a.$$

This clearly follows from the above congruence by multiplying it by a. And Fermat's little theorem follows from this congruence by canceling a which is allowed if p does not divide a.

The proof uses the binomial theorem. Clearly, $1^p \equiv 1 \bmod p$. Now

$$2^p = (1+1)^p = 1 + \binom{p}{1} + \binom{p}{2} + \cdots + \binom{p}{p-1} + 1 \equiv 1 + 0 + 0 + \cdots + 0 + 1 = 2 \bmod p.$$

Once we have $2^p \equiv 2 \bmod p$, we use the binomial theorem again to find 3^p:

$$3^p = (1+2)^p = 1+\binom{p}{1}2+\binom{p}{2}2^2+\cdots+\binom{p}{p-1}2^{p-1}+2^p \equiv 1+0+0+\cdots+0+2 = 3 \bmod p.$$

This process can be continued indefinitely to prove the result. (Technically, the result $a^p \equiv a \bmod p$ is found by induction on a.)

An important use of this result is the following:
Theorem: If a is not divisible by p, the inverse of a mod p is a^{p-2}.

This is clearly true since $1 \equiv a^{p-1} \equiv a \cdot a^{p-2} \bmod p$.

Why is this useful? If we want to find, say the inverse of 17 mod 101, this result says to find 17^{99}. It doesn't seem too useful to multiply 17 by itself 99 times, mod 101. Isn't it better to solve the congruence $17x \equiv 1 \bmod 101$? Perhaps so. But with large numbers, a computer can crunch out a power of a number mod another number in a very short time. For example, the program in the lab which does computing modulo a prime finds the inverse of a number very simply by repeated multiplications. In another section we shall show how this is done for large primes.

An interesting consequence of Fermat's little theorem is the following.
Theorem: Let p be a prime and let a be a number not divisible by p. Then if $r \equiv s \bmod (p-1)$ we have $a^r \equiv a^s \bmod p$. In brief, when we work mod p, exponents can be taken mod $(p-1)$.

We've seen this used in calculations. For example to find 2^{402} mod 11, we start with Fermat's theorem: $2^{10} \equiv 1 \bmod 11$. Raise to the 40th power to get $2^{400} \equiv 1 \bmod 11$. Now multiply by $2^2 = 4$ to get $2^{402} \equiv 4 \bmod 11$. In the language of the above theorem, $p = 11$, and so $p - 1 = 10$. We can thus take the exponent 402 mod 10 to get $2^{402} \equiv 2^2 \bmod 11$. Thus

$$402 \equiv 2 \bmod 10, \text{ so } 2^{402} \equiv 2^2 \bmod 11$$

The following is a useful corollary of Fermat's little theorem, which is used today in cryptography.

Theorem: . Suppose $n = pq$ where p and q are distinct primes, and a is not divisible by p or by q. Then

$$a^{(p-1)(q-1)} \equiv 1 \bmod n$$

To see this, we note that

$$a^{p-1} \equiv 1 \bmod p, \text{ and } a^{q-1} \equiv 1 \bmod q$$

Raise the first congruence to the $(q-1)$ power, and the second to the $(p-1)$ power. We then get

$$a^{(p-1)(q-1)} \equiv 1 \bmod p, \text{ and } a^{(p-1)(q-1)} \equiv 1 \bmod q$$

But this means that $a^{(p-1)(q-1)} - 1$ is divisible by p and by q, and so by $pq = n$. This is the result.

For example, taking primes 67 and 97, and computing $67 \cdot 97 = 6499$, and $66 \cdot 98 = 6468$, we get

$$a^{6468} \equiv 1 \bmod 6499$$

if a is not divisible by 67 or 97. In this case, we see that an inverse of a mod 6499 is $a^{6467} \bmod 6499$.

Note: Euler's ϕ function is defined as follows: If $n = p_1^{a_1} p_2^{a_2} \cdots p_k^{a_k}$ is the factorization of n into distinct prime powers, the

$$\phi(n) = p_1^{a_1-1} p_2^{a_2-1} \cdots p_k^{a_k-1} (p_1 - 1)(p_2 - 1) \cdots (p_k - 1)$$

The above result is a special case of Euler's Theorem (which we do not prove):

Theorem: If a and n are relatively prime, then $a^{\phi(n)} \equiv 1 \bmod n$.

Fermat's little theorem is a special case here, when n is a prime.