Fermat's little theorem

Mathematics Explained and Clarified

1 Technical lemmas without proofs

Lemma 1 (Euclid's lemma)**.** *For any natural numbers a and b and a prime number p, if the product ab is divisible by p, then either a is divisible by p or b is divisible by p.*

Lemma 2. *For any natural numbers a and b and a prime number p, if both a and b are not divisible by p, then their product ab is not divisible by p either.*

Lemma 1 and Lemma 2 are trivially equivalent to each other. Sometimes, it is more convenient to use the statement in the form of Lemma 1 and sometimes in the form of Lemma 2.

Lemma 1 should be intuitively more or less obvious. It is a straightforward corollary of the fundamental theorem of arithmetic, which states that any natural number can be expressed as a product of prime numbers, and that this expression is unique up to the order of the prime divisors. Although it is sometimes proved without using the fundamental theorem of arithmetic as it is a simpler statement than the fundamental theorem of arithmetic. And, if proving Lemma 1 as a corollary of the fundamental theorem of arithmetic, we need to make sure that the fundamental theorem of arithmetic is proved without using Lemma 1 to avoid circular reasoning.

Lemma 3. *If $ab \equiv ac \pmod{p}$, where p is a prime number, and a is not divisible by p, then we can cancel a from both sides and get $b \equiv c \pmod{p}$.*

Lemma 3 is a straightforward corollary of Lemma 1.

The full proofs are given at the end in a separate section. Readers are encouraged to skip that section.

2 The main result

Theorem 1 (Fermat's little theorem)**.** *Let p be a prime number, and let n be a natural number not divisible by p. Then $n^{p-1} \equiv 1 \pmod{p}$.*

Proof. Consider the numbers n, $2n$, $\ldots$, $(p-1)n$.

First, by Lemma 2, none of these $p-1$ numbers is divisible by p. Indeed, for $1 \leq i \leq p-1$, i is not divisible by p because $i < p$. And n is not divisible by

p by the condition in the statement of the theorem. Therefore, by Lemma 2, in is not divisible by p.

Second, let us prove that these $p-1$ numbers all have different remainders when divided by p. Indeed, if in and jn have the same remainder, where $1 \leq i < j \leq p-1$, then $jn - in = (j-i)n$ is divisible by p, a contradiction with the previously proved fact.

So, these $p-1$ numbers all have different remainders when divided by p, and none of them has remainder 0. But there are only $p-1$ such possible remainders: 1, 2, ..., $p-1$. So, these $p-1$ numbers must have exactly these remainders, possibly in different order.

Then the product of these $p-1$ numbers must be congruent to the product of these $p-1$ remainders modulo p. So,

$$n \cdot 2n \cdot \ldots \cdot (p-1)n \equiv 1 \cdot 2 \cdot \ldots \cdot (p-1) \pmod{p}.$$

Therefore,

$$n^{p-1} \cdot 1 \cdot 2 \cdot \ldots \cdot (p-1) \equiv 1 \cdot 2 \cdot \ldots \cdot (p-1) \pmod{p}.$$

Since none of the numbers 1, 2, ..., $p-1$ is divisible by p (because they are all strictly smaller than p), applying Lemma 2 repeatedly $p-1$ times, we get that their product $1 \cdot 2 \cdot \ldots \cdot (p-1)$ is not divisible by p either. Now we can use Lemma 3 to cancel $1 \cdot 2 \cdot \ldots \cdot (p-1)$ on both sides of the congruency above. We get

$$n^{p-1} \equiv 1 \pmod{p},$$

which is exactly what we needed to prove. □

3 Proofs of the technical lemmas

Proof of Lemma 1 using the fundamental theorem of arithmetic. By the fundamental theorem of arithmetic, both a and b can be expressed as products of prime numbers: $a = q_1 \cdot \ldots \cdot q_n$ and $b = q'_1 \cdot \ldots \cdot q'_{n'}$, where all q_i and q'_i are prime numbers (not necessarily distinct).

Then the product ab can be expressed as $ab = q_1 \cdot \ldots \cdot q_n \cdot q'_1 \cdot \ldots \cdot q'_{n'}$. This is an expression of ab as a product of prime numbers. By the fundamental theorem of arithmentic, this expression is unique up to the order of the prime divisors.

Suppose that ab is divisible by p. Let us prove that p must be among q_i or q'_i. The fact that ab is divisible by p means that $ab = px$ for some natural number x. By the fundamental theorem of arithmetic, x can be expressed as a product of prime numbers: $x = r_1 \cdot \ldots \cdot r_k$, where all r_i are prime. Then $ab = px = p \cdot r_1 \cdot \ldots \cdot r_k$. This is also the expression of ab as a product of prime numbers. By the fundamental theorem of arithmetic, the expression of ab as a product of prime numbers must be unique up to the order of the prime divisors. Thus, the two lists of prime numbers $(q_1, \ldots, q_n, q'_1, \ldots, q'_{n'})$ and $(p, r_1, \ldots, r_k)$ are the same up to the order of the elements. Therefore, the first list must contain p, which means that p must be among q_i or q'_i.

Now, if p is among q_i, then a is divisible by p. And if p is among q'_i, then b is divisible by p. □

Proof of Lemma 3. By definition of congruency, $ab \equiv ac \pmod{p}$ means that $ab - ac$ is divisible by p. Notice that $ab - ac = a(b - c)$. Now it follows from Lemma 1 that either a is divisible by p or $b - c$ is divisible by p. But a is not divisible by p by the condition in the statement of the lemma. Therefore, $b-c$ is divisible by p. This is exactly equivalent to the congruency $b \equiv c \pmod{p}$. □