

## Fermat's 'little' theorem

### Fermat's 'little' Theorem.

**Fermat's 'little' Theorem.** Let  $p$  be any prime and let  $a \in \mathbf{Z}$  with  $a \not\equiv 0 \pmod{p}$ ; then  $a^{p-1} \equiv 1 \pmod{p}$ . [In words: if  $p$  is any prime number, and  $a$  is any integer *not* divisible by  $p$ , then  $a$  to the power of ( $p$  minus 1) leaves remainder 1 when divided by  $p$ .]

#### Numerical Examples.

1.  $p = 7, a = 2. a^{p-1} = 2^6 = 64 = 7 \times 9 + 1 \equiv 1 \pmod{7}$ .
2.  $p = 7, a = 9. a^{p-1} = 9^6 = 531,441 = 7 \times 75920 + 1 \equiv 1 \pmod{7}$ .

**Advice.** You should verify by hand some similar (small) examples for yourself, and you should use **Maple** to verify much larger examples.

**Note.** We didn't need to do the calculation in #2 because, since  $9 \equiv 2 \pmod{7}$ , it follows that  $9^6 \equiv 2^6 \pmod{7}$ , and since #1 already shows that  $2^6 \equiv 1 \pmod{7}$ , then  $9^6 \equiv 1 \pmod{7}$ .

This theorem of Fermat's (which he discovered, but couldn't prove) is one of the finest and *most important* theorems in all of Number Theory, and has many proofs. The proof that we see below is based on a very simple idea that suggests itself to someone who has looked closely at 'multiplication tables *modulo*  $p$ ' for a number of values of  $p$ .

Looking at the multiplication table *modulo* 7 one sees that:

$$4 \times 0, 4 \times 1, 4 \times 2, 4 \times 3, 4 \times 4, 4 \times 5, 4 \times 6 \equiv 0, 4, 1, 5, 2, 6, 3 \pmod{7},$$

from which we obtain - by multiplying the last 6 congruences together - the *single* congruence:

$$(4 \times 1) \times (4 \times 2) \times (4 \times 3) \times (4 \times 4) \times (4 \times 5) \times (4 \times 6) \equiv 4 \times 1 \times 5 \times 2 \times 6 \times 3 \pmod{7},$$

which successively simplifies to:

$$4^6 \times 6! \equiv 6! \pmod{7}, \quad 4^6 \times 6! - 6! \equiv 0 \pmod{7}, \quad 6!(4^6 - 1) \equiv 0 \pmod{7}.$$

From that last congruence we obtain *either*  $6! \equiv 0 \pmod{7}$  *or*  $(4^6 - 1) \equiv 0 \pmod{7}$ . But,  $6! \not\equiv 0 \pmod{7}$  [Why?], and thus  $(4^6 - 1) \equiv 0 \pmod{7}$ . Hence  $4^6 \equiv 1 \pmod{7}$ . (You should do some more numerical work like this yourself.)

The proof that is given below of Fermat's 'little' theorem uses precisely this idea (it is due to Euler), but it first of all requires this preliminary theorem, which shows that what you have seen above is a *general* phenomenon:

## Fermat's 'little' theorem

**Theorem 1.** Let  $p$  be any prime and  $a \in \mathbf{Z}$  with  $a \not\equiv 0 \pmod{p}$ , then:

$$a \times 0, a \times 1, a \times 2, \dots, a \times (p-1) \text{ in some order } \equiv 0, 1, 2, \dots, (p-1) \pmod{p}.$$

**Proof.** The integers  $a \times 0, a \times 1, a \times 2, \dots, a \times (p-1)$ , form  $p$  integers, and each of them is congruent  $\pmod{p}$  to some integer in the range 0 to  $(p-1)$ , and there are *exactly*  $p$  integers in that range. We will argue that *no two* of them are congruent to each other, and so it follows that one of them must be congruent to  $0 \pmod{p}$ , another of them to  $1 \pmod{p}$ , another of them to  $2 \pmod{p}$ ,  $\dots$ , and, finally, one of them to  $(p-1) \pmod{p}$ .

So, suppose that  $a \times c \equiv a \times b \pmod{p}$ , for some  $b, c \in \mathbf{Z}$  with  $0 \leq b < c \leq (p-1)$ . Then we would have  $a \times c - a \times b \equiv 0 \pmod{p}$ , and so have  $a \times (c-b) \equiv 0 \pmod{p}$ . But then (by the 'fundamental theorem for primes': 'if a prime  $p$  divides the product of two integers then it divides at least one of those two integers') we would have:

$$\text{either } a \equiv 0 \pmod{p} \text{ or } (c-b) \equiv 0 \pmod{p}.$$

The first of these *doesn't* happen since  $a \not\equiv 0 \pmod{p}$ , and the second *can't* happen because  $1 \leq c-b \leq p-1$  (and so  $(c-b)$  can't be divisible by  $p$ ). This proves the theorem.

**Note.**  $p$  being *prime* is really *crucial*.

$2 \times 0, 2 \times 1, 2 \times 2, 2 \times 3 \equiv 0, 2, 0, 2 \pmod{4}$ .  
 $2 \times 0, 2 \times 1, 2 \times 2, 2 \times 3, 2 \times 4, 2 \times 5 \equiv 0, 2, 4, 0, 2, 4 \pmod{6}$ .  
*etc.*

At the same time also note that *sometimes* you can get things *like*:

$4 \times 0, 4 \times 1, 4 \times 2, 4 \times 3, \dots, 4 \times 7, 4 \times 8 \equiv 0, 4, 8, 3, 7, 2, 6, 1, 5 \pmod{9}$ .  
 $7 \times 0, 7 \times 1, 7 \times 2, 7 \times 3, 7 \times 4, \dots, 7 \times 8, 7 \times 9 \equiv 0, 7, 4, 1, 8, 5, 2, 9, 6, 3 \pmod{10}$ .

In fact, in general, the following is true (and may be proved like above): Let  $n$  be any natural number (prime or otherwise), and  $a \in \mathbf{Z}$  with  $\gcd(a, n) = 1$ , then:

$$a \times 0, a \times 1, a \times 2, \dots, a \times (n-1) \text{ in some order } \equiv 0, 1, 2, \dots, (n-1) \pmod{n}.$$

Before proceeding to the proof of Fermat's 'little' theorem there is one important point which has to be made concerning the 'fundamental property of the primes.' Recall that the fundamental property tells us that if a prime number  $p$  divides the product of *two* integers  $a$  and  $b$  then  $p$  must divide at *least one* of these two integers. However, it follows immediately (and this is something that we *need* in the following proof of Fermat's 'little' theorem) that whenever a prime  $p$  divides a product of *any* number of integers, then  $p$  must divide *at least one* of those integers. So, *if*  $p$  is prime and  $p|a_1 a_2 \dots a_n$ , where  $a_1, a_2, \dots, a_n \in \mathbf{Z}$ , then  $p|a_1$  or  $p|a_2$  or  $\dots$  or  $p|a_n$ .

## Fermat's 'little' theorem

That this is true follows easily from the single case of the product of *two* integers. The idea is a simple one: suppose that  $p$  is prime and that  $p|A.B.C$  where  $A, B, C \in \mathbf{Z}$ . Then just rewrite the product of the *three* integers  $A, B$  and  $C$  as a product of *two* integers, namely  $(A.B)$  and  $C$ . Then, from  $p|A.B.C$  we get  $p|(A.B).C$ . But then either  $p|(A.B)$  or  $p|C$ . But if  $p|(A.B)$  then  $p|A$  or  $p|B$ , and thus  $p|A$  or  $p|B$  or  $p|C$ . In a similar fashion the above result can be argued for a product of four, five, ... integers.

**Proof of Fermat's 'little' theorem.** Since  $p$  is prime and  $a \in \mathbf{Z}$  with  $a \not\equiv 0 \pmod{p}$ , then

$$a \times 0, a \times 1, a \times 2, \dots, a \times (p-1) \underset{\text{in some order}}{\equiv} 0, 1, 2, \dots, (p-1) \pmod{p},$$

and since  $a \times 0 \equiv 0 \pmod{p}$ , then the product of  $a \times 1, a \times 2, \dots$  and  $a \times (p-1)$  is congruent *mod*  $p$  to the product of  $1, 2, \dots$  and  $(p-1)$ . That is:

$$(a \times 1) \times (a \times 2) \times (a \times 3) \times \dots \times (a \times (p-1)) \equiv 1 \times 2 \times 3 \times \dots \times (p-1) \pmod{p}.$$

But then we have:

$$\begin{aligned} a^{p-1} \times (p-1)! &\equiv (p-1)! \pmod{p}, \\ \therefore a^{p-1} \times (p-1)! - (p-1)! &\equiv 0 \pmod{p}, \\ \therefore (p-1)! \times (a^{p-1} - 1) &\equiv 0 \pmod{p} \quad \dots (i) \end{aligned}$$

From (i) we get: either  $(p-1)! \equiv 0 \pmod{p}$  or  $a^{p-1} - 1 \equiv 0 \pmod{p}$ . But  $(p-1)!$  is the product of the  $(p-1)$  integers  $1, 2, 3, \dots, (p-1)$ , and if  $(p-1)!$  were divisible by  $p$  it would follow that at least one of those integers was divisible by  $p$ . But none of those integers is divisible by  $p$ , and thus  $a^{p-1} - 1 \equiv 0 \pmod{p}$ . Hence  $a^{p-1} \equiv 1 \pmod{p}$ .