# MATH10040
# Chapter 5:
# Fermat's 'Little' Theorem

## 1. Cancellation in arithmetic modulo $m$.

Recall that, in school algebra, if $a$ is a nonzero integer and if $ar = as$ then we deduce that $r = s$ (we 'cancel' the $a$s on both sides). The proof of this law is: divide both sides by $a$, or equivalently, multiply both sides by (the rational number) $1/a$.

In arithmetic modulo $m$ this argument does not work: even if $a \not\equiv 0$ we cannot generally 'divide by $a$'.

**Example 1.1.** $a = 10 \not\equiv 0 \pmod{12}$. *We have* $10 \cdot 5 \equiv 2 \equiv 10 \cdot 11 \pmod{12}$ *but* $5 \not\equiv 11 \pmod{12}$. *So we cannot divide by* 10*, or 'cancel'* 10*, in this congruence.*

However, if $(a, m) = 1$, we can essentially 'divide by $a$' in modulo $m$ arithmetic. (Observe that $(10, 12) = 2$.)

Recall that if $m \geq 1$ and if $(a, m) = 1$ then the congruence $ax \equiv 1 \pmod{m}$ is always solvable. (In practice, we can use Euclid's algorithm to find a solution $b$. Then the general solution is the *congruence class of $b$ modulo $m$*; i.e. the set $\{b + mt \mid t \in \mathbb{Z}\}$.)

**Lemma 1.2** (Cancellation in congruences)**.** *Suppose that* $(a, m) = 1$ *and* $ar \equiv as \pmod{m}$. *Then* $r \equiv s \pmod{m}$.

*Proof.* Since $(a, m) = 1$ there exists $b \in \mathbb{Z}$ satisfying $ab \equiv 1 \pmod{m}$. (The point, as we shall see, is that such a $b$ plays the role of $1/a$ or $a^{-1}$ in arithmetic modulo $m$.)

Now suppose that $ar \equiv as \pmod{m}$. Then $b(ar) \equiv b(as) \pmod{m}$. But $b(ar) = (ab) \cdot r \equiv 1 \cdot r \equiv r \pmod{m}$. Similarly $b(as) \equiv s \pmod{m}$. Thus $r \equiv s \pmod{m}$. □

## 2. The order of $a$ modulo $m$

We have seen that it is often useful, when calculating modulo $m$ with large powers of $a$, to find some $n \geq 1$ such that $a^n \equiv 1 \pmod{m}$ – i.e. to find a solution $b$ of $ax \equiv 1 \pmod{m}$ which is itself a power of $a$.

Can we always do this?

**Proposition 2.1.** *Suppose that* $(a, m) = 1$. *Then there exists an integer* $n$ *satisfying* $a^n \equiv 1 \pmod{m}$ *and* $1 \leq n \leq m$.

*Proof.* Consider the list of integers $a^0, a^1, \ldots, a^{m-1}, a^m$. There are $m+1$ integers in this list and each has remainder in the set $\{0, \ldots, m-1\}$. Since there are only $m$ possible remainders, some two of these $m+1$ numbers must have the same remainder on division by $m$.

Thus there exists $r, s$ with $0 \leq r < s \leq m$ such that $a^r$ and $a^s$ have the same remainder on division by $m$; i.e.

$$a^r \equiv a^s \pmod{m}.$$

Let $n = s - r$. So $s = r + n$. Therefore

$$a^r \equiv a^r \cdot a^n \pmod{m}.$$

Since $(a^r, m) = 1$, we can 'cancel' $a^r$ on both sides, by Lemma 1.2. Thus

$$a^n \equiv 1 \pmod{m}.$$

□

**Definition 2.2.** *Suppose that* $(a, m) = 1$. *The* order of $a$ modulo $m$ *is the smallest positive integer* $d$ *with the property that* $a^d \equiv 1 \pmod{m}$.

**Example 2.3.** *The order of* 3 *modulo* 80 *is* 4 *since* $3^4 = 81 \equiv 1 \pmod{80}$ *but* $3^1, 3^2, 3^3 \not\equiv 1 \pmod{80}$. *Here is a table of powers of* 3 *modulo* 80*:*

| $n$ | $R_{80}(3^n)$ |
|---|---|
| 0 | 1 |
| 1 | 3 |
| 2 | 9 |
| 3 | 27 |
| 4 | 1 |
| 5 | 3 |
| 6 | 9 |
| 7 | 27 |
| 8 | 1 |
| 9 | 3 |
| ⋮ | ⋮ |

*Notice that the numbers on the right repeat themselves in cycles of length* 4. *This is no coincidence.*

**Theorem 2.4.** *Suppose that* $(a, m) = 1$ *and let* $d \geq 1$ *be the order of* $a$ *modulo* $m$. *Then* $a^n \equiv 1 \pmod{m}$ *if and only if* $d|n$.

*Proof.* Recall that $a^d \equiv 1 \pmod{m}$ and $a^r \not\equiv 1 \pmod{m}$ if $1 \leq r < d$.

First suppose that $d|n$. Then $n = dt$ for some integer $t$ and hence

$$a^n = (a^d)^t \equiv 1^t \equiv 1 \pmod{m}.$$

Conversely, suppose that $a^n \equiv 1 \pmod{m}$. We must prove that $d|n$. By the division algorithm, $n = dt + r$ for some $t, r \in \mathbb{Z}$ with $0 \leq r < d$. We must prove that $r = 0$:

Now

$$a^n = (a^d)^t \cdot a^r \equiv 1 \cdot a^r \equiv a^r \pmod{m}$$

and hence

$$a^r \equiv 1 \pmod{m}.$$

Since $r < d$ this forces $r = 0$ by the minimality of $d$. □

**Corollary 2.5.** *Suppose that $(a, m) = 1$ and let $d \geq 1$ be the order of $a$ modulo $m$. Then for any integers $r$ and $s$*

$$a^r \equiv a^s \pmod{m} \quad \Longleftrightarrow \quad r \equiv s \pmod{d}.$$

*Proof.* We will assume, without loss of generality, that $r \leq s$.

Suppose that $s \equiv r \pmod{d}$. Then $s = r + dt$ for some $t \geq 0$. So

$$a^s = a^r \cdot (a^d)^t \equiv a^r \cdot 1 \equiv a^r \pmod{m}.$$

Conversely suppose that $a^r \equiv a^s \pmod{m}$. We must prove that $d|s - r$.

Let $n = s - r$. Then by Lemma 1.2 from $a^r \equiv a^r \cdot a^n \pmod{m}$ we deduce $1 \equiv a^n \pmod{m}$ and hence that $d|n$ by Theorem 2.4. □

**Remark 2.6.** *Note that the corollary says that the powers of a repeat modulo $m$ in cycles of length $d$. This is precisely what we observed of the powers of 3 modulo 80 (where $d = 4$ in that case).*

**Example 2.7.** *What is the order of 2 modulo 33?*

***Solution:*** *Let $d$ be the order of 2 modulo 33.*

*We have $2^5 = 32 \equiv -1 \pmod{33}$. Thus $2^{10} \equiv (-1)^2 \equiv 1 \pmod{33}$.*

*It follows from Theorem 2.4 that $d|10$. Thus $d = 1, 2, 5$ or $10$. But $2, 2^2, 2^5 \not\equiv 1 \pmod{33}$. Thus $d = 10$.*

*It follows, from Theorem 2.4 again, that*

$$2^n \equiv 1 \pmod{33} \quad \Longleftrightarrow \quad 10|n.$$

**Example 2.8.** *The order of 7 modulo 10 is 4. (Check this!)*

*The powers of 7 modulo 10 repeat in cycles of length 4:*

| $n$ | $R_{10}(7^n)$ |
|---|---|
| 0 | 1 |
| 1 | 7 |
| 2 | 9 |
| 3 | 3 |
| 4 | 1 |
| 5 | 7 |
| 6 | 9 |
| 7 | 3 |
| 8 | 1 |
| 9 | 7 |
| $\vdots$ | $\vdots$ |

***Q:*** *What is the last digit of* $7^{83}$*?*

***A:*** *Since* $83 \equiv 3 \pmod 4$, $7^{83} \equiv 7^3 \equiv 3 \pmod{10}$.

## 3. Fermat's Little Theorem

**Remark 3.1.** *Recall (Homework 5, problem 9 (b)) that if* $p$ *is a prime number then* $\binom{p}{m} \equiv 0 \pmod p$ *if* $1 \leq m \leq p-1$.

**Proposition 3.2.** *Let* $p$ *be a prime number. Then* $n^p \equiv n \pmod p$ *for all* $n \geq 1$.

*Proof.* We'll prove this by induction on $n$. The case $n = 1$ is clear since $1^p = 1$.

Suppose the result has been proved for some $n \geq 1$. Then

$$\begin{aligned}(n+1)^p &= n^p + \binom{p}{1}n^{p-1} + \cdots + \binom{p}{m}n^m + \cdots + \binom{p}{p-1}n + 1 \\ &\quad \text{by the Binomial Theorem} \\ &\equiv n^p + 0 + \cdots + 0 + 1 \pmod p \text{ (see remark above)} \\ &\equiv n + 1 \pmod p \text{ by ind. hyp..}\end{aligned}$$

□

**Theorem 3.3** (Fermat's Little Theorem)**.** *Let* $p$ *be a prime and* $a$ *any integer not divisible by* $p$*. Then*

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

*Proof.* Replacing $a$, if necessary, by a positive number which is congruent to it modulo $p$, we can assume that $a \geq 1$. By Proposition 3.2, we have $a \cdot a^{p-1} \equiv a \cdot 1 \pmod p$. Since $(a, p) = 1$, we deduce that $a^{p-1} \equiv 1 \pmod p$ by Lemma 1.2. □

Combining Fermat's Little Theorem with Theorem 2.4 we deduce:

**Corollary 3.4.** *Suppose that $p$ is prime and that $p \not| a$. Let $d$ be the order of $a$ modulo $p$. Then $d|p-1$; i.e. $p \equiv 1 \pmod{d}$.*

**Example 3.5.** *Find the order of 10 modulo 29.*

***Solution:*** *Let $d$ be the order of 10 modulo 29.*

*29 is prime, so $d|29-1=28$. Thus $d = 1, 2, 4, 7, 14$ or 28.*

*We eliminate all but the last:*

$$10^2 = 4 \cdot 25 \equiv 4 \cdot (-4) \equiv -16 \pmod{29}: \quad d \neq 2.$$
$$10^3 \equiv 10 \cdot -16 \equiv -5 \cdot 32 \equiv -5 \cdot 3 \equiv -15 \pmod{29}.$$
$$10^4 \equiv 16^2 \equiv 32 \cdot 8 \equiv 3 \cdot 8 \equiv 24 \equiv -5 \pmod{29}: \quad d \neq 4$$
$$10^7 = 10^4 \cdot 10^3 \equiv -5 \cdot -15 \equiv 25 \cdot 3 \equiv -4 \cdot 3 \equiv -12 \pmod{29}: \quad d \neq 7.$$
$$10^{14} \equiv 12^2 \equiv 36 \cdot 4 \equiv 7 \cdot 4 \equiv 28 \equiv -1 \pmod{29}: \quad d \neq 14.$$

*Thus $d = 28$.*

*Thus*

$$29|10^{28} - 1 = \underbrace{99\cdots99}_{28}$$

*but*

$$29 \not| \underbrace{99\cdots99}_{n} \quad \text{if } n < 28.$$

**Example 3.6.** *Is $2^{32}+1 = 4294967297$ prime?*

***Solution:*** *If $2^{32}+1$ is not prime, then it is divisible by a prime $p < \lfloor\sqrt{2^{32}+1}\rfloor = 2^{16} = 65536$.*

*We can use Fermat's Little Theorem to eliminate most primes from consideration, as follows:*

*Let $p$ be a prime number dividing $2^{32}+1$. Then $2^{32} \equiv -1 \pmod{p}$ and hence*

$$2^{64} \equiv (-1)^2 \equiv 1 \pmod{p}.$$

*Let $d$ be the order of 2 modulo $p$. Then $d|64$. Thus $d = 2^r$ for some $r \leq 6$. But if $r < 6$ then $d|32$ and hence $2^{32} \equiv 1 \pmod{p}$, a contradiction. Thus $r = 6$ and $d = 64$.*

*It follows by Corollary 3.4 that $p \equiv 1 \pmod{64}$. Thus any prime divisor of $2^{32}+1$ must be of the form $64n+1$ for some $n \geq 1$. The first few such primes are:*

$$193, 449, 577, 641, \ldots$$

*We test each of these primes in turn and discover that $641|2^{32}+1$ (in fact $2^{32}+1 = 641 \cdot 6700417$, both factors are primes) to see that $2^{32}+1$ is not prime.*

**Example 3.7.** *Is* $2^{11} - 1 = 2047$ *prime?*

***Solution:*** *Let* $p$ *be a prime divisor of* $N = 2^{11} - 1$*. Then* $2^{11} \equiv 1 \pmod{p}$*. Thus the order of* 2 *modulo* $p$ *is* 11*. So* $p$ *is the form* $11n + 1$*. The smallest such prime is* $23 = 11 \cdot 2 + 1$*. Dividing, we find* $2047 = 23 \cdot 89$*. So it is composite.*

**Remark 3.8.** *Fermat's Little Theorem fails in general if the modulus is composite; i.e. If* $n$ *is composite and if* $(a, n) = 1$ *then it is not usually the case that* $a^{n-1} \equiv 1 \pmod{n}$*.*

*For example, take* $n = 9$ *and* $a = 2$*. Then*

$$2^3 \equiv -1 \pmod{9} \Longrightarrow 2^6 \equiv 1 \pmod{9} \Longrightarrow 2^8 \equiv 2^2 \not\equiv 1 \pmod{9}.$$

*There is however, an extension of Fermat's Little Theorem, due to Euler, which applies to composite as well as prime moduli:*

*There is a function* $\phi : \mathbb{N} \to \mathbb{N}$ *(the 'Euler phi-function') with the property that* $\phi(p) = p - 1$ *when* $p$ *is prime and for all* $m > 1$ *and* $a$ *with* $(a, m) = 1$ *we have*

$$a^{\phi(m)} \equiv 1 \pmod{m}.$$

*In fact* $\phi(9) = 6$*. So Euler's Theorem tells us that* $a^6 \equiv 1 \pmod{9}$ *if* $3 \not| a$*.*

*In practice,* $\phi$ *can be calculated from the following two facts:*

(1) *If* $p$ *is a prime number, then* $\phi(p^n) = p^{n-1}(p - 1)$*.*

(2) *If* $(n, m) = 1$ *then* $\phi(nm) = \phi(n) \cdot \phi(m)$*.*

*For example,* $\phi(100) = \phi(4)\phi(25) = (2 \cdot (2-1)) \cdot (5 \cdot (5-1)) = 2 \cdot 5 \cdot 4 = 40$*.*

**Example 3.9.** ***Testing for primality***

*Fermat's Little Theorem is the basis for testing whether a number is prime or not. If* $p > 2$ *is a prime number, Fermat's Theorem tells us that* $2^{p-1} \equiv 1 \pmod{p}$*. It follows that if* $n$ *is any odd number and if* $2^{n-1} \not\equiv 1 \pmod{n}$ *then* $n$ must be composite*. In this way, we can often determine that a number is composite* without finding any factors*. Indeed, there are examples of very large numbers which are known to be composite using this test, but for which factors cannot be found with existing computational methods.*

*As a toy example: Suppose that we want to determine that* 527 *is composite* without factoring*. Easy (but tedious) calculations show that* $2^{40} \equiv 1 \pmod{527}$*. Since* $526 = 40 \cdot 13 + 6$ *this gives*

$$2^{256} \equiv (2^{40})^{13} \cdot 2^6 \equiv 2^6 \equiv 64 \not\equiv 1 \pmod{257}.$$

*So* 257 *is composite. (In fact* $257 = 17 \cdot 31$*.)*

**Example 3.10.** *Use Fermat's Little Theorem to prove that* $385|n^{60}-1$ *if* $5,7,11 \not| n$.

***Solution:*** *Note that* $385 = 5 \cdot 7 \cdot 11$. *We wish to prove that if* $5,7,11 \not| n$ *then*

$$n^{60} \equiv 1 \pmod{385}.$$

*Since* $5,7,11$ *are pairwise relatively prime this is equivalent to showing that*

$$n^{60} \equiv 1 \pmod{5} \text{ and } n^{60} \equiv 1 \pmod{7} \text{ and } n^{60} \equiv 1 \pmod{11}$$

*By Fermat's Little Theorem,* $n^4 \equiv 1 \pmod{5}$, *and since* $4|60$ *it follows that* $n^{60} \equiv 1 \pmod{5}$.

*Similarly, by Fermat's Little Theorem,* $n^6 \equiv 1 \pmod{7}$, *and since* $6|60$ *it follows that* $n^{60} \equiv 1 \pmod{7}$.

*Finally, by Fermat's Little Theorem,* $n^{10} \equiv 1 \pmod{11}$, *and since* $10|60$ *it follows that* $n^{60} \equiv 1 \pmod{11}$.

Using the same idea as in this last example we prove the following:

**Lemma 3.11.** *Let* $p,q$ *be two (distinct) odd primes. Suppose that* $p,q \not| a$. *Then*

$$a^{\frac{(p-1)(q-1)}{2}} \equiv 1 \pmod{pq}.$$

*Proof.* Let $m := \frac{(p-1)(q-1)}{2}$.

Since $(p,q) = 1$ we just need to prove that

$$a^m \equiv 1 \pmod{p} \text{ and } a^m \equiv 1 \pmod{q}.$$

Since $q$ is odd, $q-1$ is even and hence $\frac{q-1}{2} \in \mathbb{Z}$. Thus $p-1|\frac{(p-1)(q-1)}{2} = m$. But $a^{p-1} \equiv 1 \pmod{p}$ by Fermat. Hence $a^m \equiv 1 \pmod{p}$.

Similarly (exchanging the roles of $p$ and $q$) $a^m \equiv 1 \pmod{q}$. □