

Fermat's Little Theorem and Euler's Theorem

Theorem: In any field, F , the non-zero elements, U , form a group under the field multiplication.

Proof:

0. U is closed under multiplication since if $x, y \in U$, then by definition $x \neq 0$ and $y \neq 0$. But then $xy \neq 0$ otherwise F would have zero divisors. So $xy \in U$.
1. The multiplication in F is associative since F is also a ring.
2. The identity element $1 \in F$ is in U since it's non-zero.
3. If $x \in U$ then by definition x is a unit and has a non-zero inverse which is also in U .

Hence, U is a group under the field multiplication.

In particular, the non-zero elements of \mathbb{Z}_p , p being a prime number, form a group. Thus, $\{1, 2, \dots, p - 1\}$ is a group of order $p - 1$ under multiplication modulo p .

Since the order of any element of the group must divide the order of the group, if $a \neq 0, a \in \mathbb{Z}_p$ then $a^{p-1} = 1$ in \mathbb{Z}_p .

Since \mathbb{Z}_p is isomorphic to the group of cosets:

$$\{p\mathbb{Z}, 1 + p\mathbb{Z}, 2 + p\mathbb{Z}, \dots, (p - 1) + p\mathbb{Z}\}.$$

This gives us: $a^{p-1} \equiv 1 \pmod{p}$.

Note: the notation $a^{p-1} \equiv 1 \pmod{p}$ read as " a^{p-1} is congruent to 1 modulo p ", is often used in place of $a^{p-1} = 1 \pmod{p}$.

Thus we have:

Little Theorem of Fermat: If $a \in \mathbb{Z}$ and p is prime not dividing a , then p divides $a^{p-1} - 1$, that is, $a^{p-1} \equiv 1 \pmod{p}$ for $a \not\equiv 0 \pmod{p}$.

Corollary: If $a \in \mathbb{Z}$, then $a^p \equiv a \pmod{p}$ for any prime p .

Proof: If $a \not\equiv 0 \pmod{p}$ then this follows from the previous theorem.

If $a \equiv 0 \pmod{p}$ then both sides are 0 modulo p .

Ex. Find the remainder of 8^{100} when divided by 13, i.e. find $8^{100} \pmod{13}$.

We know by the The Little Theorem of Fermat that when $p = 13$ and $a = 8$ we have: $8^{13-1} = 8^{12} \equiv 1 \pmod{13}$.

Thus: $(8^{12})^b \equiv 1 \pmod{13}$ for any integer b .

Write:

$$\begin{aligned} 8^{100} &= (8^{12})^8 (8^4) \equiv (1)^8 (8^4) \\ &\equiv 8^4 \equiv (-5)^4 \\ &\equiv (-25)^2 (-25)^2 \equiv (25)^2 (25)^2 \\ &\equiv (-1)^2 (-1)^2 \equiv 1 \pmod{13}. \end{aligned}$$

Ex. Show $2^{2023} + 1$ is not divisible by 11 (i.e. $2^{2023} + 1 \not\equiv 0 \pmod{11}$).

By Fermat's Theorem we know:

if $a = 2$ and $p = 11$, $2^{10} \equiv 1 \pmod{11}$.

$$\begin{aligned} 2^{2023} + 1 &= ((2^{10})^{202} \cdot 2^3) + 1 \\ &\equiv [(1^{202}) \cdot (2^3)] + 1 \\ &\equiv 8 + 1 \equiv 9 \pmod{11}. \end{aligned}$$

Thus the remainder when dividing $2^{2023} + 1$ by 11 is 9 and not 0.

Theorem: The set H_n of non-zero elements of \mathbb{Z}_n that are not zero divisors form a group under multiplication modulo n .

Def. Let $n \in \mathbb{Z}^+$ and let $\varphi(n)$ be the number of positive integers relatively prime to n . Note: $\varphi(1) = 1$.

Ex. Let $n = 18$ find $\varphi(n)$.

$\varphi(n)$ is the number of positive integers relatively prime to 18.

The positive integers relatively prime to 18 are:

$$1, 5, 7, 11, 13, 17.$$

So $\varphi(18) = 6$.

By an earlier theorem, $\varphi(n)$ is the number of non-zero elements of \mathbb{Z}_n that are not zero divisors.

Def. The function $\varphi: \mathbb{Z}^+ \rightarrow \mathbb{Z}^+$ is called the **Euler Phi Function**.

Euler's Theorem: If a is an integer relatively prime to n , then $a^{\varphi(n)} - 1$ is divisible by n , that is $a^{\varphi(n)} \equiv 1 \pmod{n}$.

Proof: If a is relatively prime to n , then the coset $a + n\mathbb{Z}$ of $n\mathbb{Z}$ containing a contains an integer $b < n$ and relatively prime to n .

Using the fact that multiplication of cosets by multiplication modulo n of representatives is well defined, we have: $a^{\varphi(n)} \equiv b^{\varphi(n)} \pmod{n}$.

If H_n is the group of non-zero elements in \mathbb{Z}_n that are not 0 divisors then $|H_n| = \varphi(n)$, thus $b^{\varphi(n)} \equiv 1 \pmod{n}$.

Note: if $n = p$, then $\varphi(n) = n - 1$, thus we get Fermat's Theorem:

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

Ex. Show that $11^6 - 1$ is divisible by 18 using Euler's theorem.

Let $n = 18$. Then as we saw earlier, $\varphi(18) = 6$.

If we take any integer that is relatively prime to 18, 11 for example, then by Euler's theorem, $11^6 \equiv 1 \pmod{18}$.

$$\Rightarrow 11^6 - 1 \equiv 0 \pmod{18} \Rightarrow 11^6 - 1 \text{ is divisible by } 18.$$

Of course it's easy enough to compute 11^6 in \mathbb{Z}_{18} by:

$$11^2 \equiv 121 \pmod{18} \equiv 13 \pmod{18}$$

$$11^4 \equiv (11^2)(11^2) \pmod{18} \equiv 13^2 \pmod{18} \equiv 7 \pmod{18}$$

$$\begin{aligned} 11^6 &\equiv 11^4 \cdot 11^2 \pmod{18} \equiv (7 \cdot 13) \pmod{18} \\ &\equiv 1 \pmod{18}. \end{aligned}$$

Ex. Find $29^{6008} \pmod{18}$.

18 and 29 are relatively prime so by Euler's theorem

$$29^{\varphi(18)} = 29^6 \equiv 1 \pmod{18}.$$

Thus we have:

$$\begin{aligned} 29^{6008} &\equiv (29^6)^{1001} (29^2) \pmod{18} \\ &\equiv (1)^{1001} (29^2) \pmod{18} \\ &\equiv (11^2) \pmod{18} \quad \text{since } 29 \equiv 11 \pmod{18} \\ &\equiv (121) \pmod{18} \\ &\equiv 13 \pmod{18}. \end{aligned}$$

Solving $ax \equiv b \pmod{n}$

Theorem: Let n be a positive integer and let $a \in \mathbb{Z}_n$ be relative prime to n .
For each $b \in \mathbb{Z}_n$ the equation $ax = b$ has a unique solution in \mathbb{Z}_n .

Proof: a is a unit in \mathbb{Z}_n so $a^{-1}(ax) = a^{-1}b$.

$x = a^{-1}b$ is the only solution.

Corollary: If a and n are relatively prime integers, then for any integer b ,
 $ax \equiv b \pmod{n}$ has as solutions all integers in precisely
one residue class modulo n .

Theorem: Let n be a positive integer and let $a, b \in \mathbb{Z}_n$. Let $d = \text{GCD}(a, n)$.
The equation $ax = b$ has a solution in \mathbb{Z}_n if, and only if, d divides b .
When d divides b , the equation has exactly d solutions in \mathbb{Z}_n .

Proof: First let's show $ax = b$ in \mathbb{Z}_n has no solutions unless d divides b .

Suppose $s \in \mathbb{Z}_n$ is a solution.

Then $as - b = qn$ in \mathbb{Z} so, $b = as - qn$.

Since d divides both a and n , d must divide $as - qn = b$.

Thus a solution s can exist only if d divides b .

Suppose that d does divide b .

Let $a = a_1d$, $b = b_1d$, and $n = n_1d$.

Then the equation $as - b = qn$ in \mathbb{Z} can be written:

$$a_1ds - b_1d = qn_1d$$

$$d(a_1s - b_1) = d(qn_1).$$

So $(as - b)$ is a multiple of n if, and only if, $a_1s - b_1$ is a multiple of n_1 .

Thus, the solutions s of $ax = b$ in \mathbb{Z}_n are precisely the solutions of $a_1x = b_1$ in \mathbb{Z}_{n_1} .

Now let $s \in \mathbb{Z}_{n_1}$ be the unique solution of $a_1x = b_1$ in \mathbb{Z}_{n_1}

(since a_1 is relatively prime to n_1 , there is a unique solution by the previous theorem).

The numbers in \mathbb{Z}_n that reduce to $s \pmod{n_1}$ are those given by:

$$s, \quad s + n_1, \quad s + 2n_1, \quad s + n, \dots, \quad s + (d - 1)n_1.$$

Thus there are exactly d solutions.

Corollary: Let $d = GCD(a, n)$, $a, n \in \mathbb{Z}^+$. The congruence $ax \equiv b \pmod{n}$ has a solution if, and only if, d divides b . When this is the case, the solutions are the integers in exactly d distinct residue classes modulo n .

Ex. Find all solutions of $155x \equiv 16 \pmod{65}$.

$GCD(155, 65) = 5$ and 5 does not divide 16 so there are no solutions in \mathbb{Z}_{65} .

Ex. Find all integer solutions of $155x \equiv 75 \pmod{65}$.

$GCD(155, 65) = 5$ and 5 does divide 75 so there are 5 solutions in \mathbb{Z}_{65} .

Start by dividing the equation and the 65 by 5.

$$31x \equiv 15 \pmod{13}$$

$$\text{also } 15 \pmod{13} \equiv 2 \pmod{13}$$

$$\text{so } 31x \equiv 2 \pmod{13}.$$

$$\text{now } 13x \equiv 0 \pmod{13} \quad (\text{for any } x \in \mathbb{Z})$$

$$\text{So solve: } (31 \pmod{13})x \equiv 2 \pmod{13}$$

$$5x \equiv 2 \pmod{13}.$$

The multiplicative inverse of 5 in \mathbb{Z}_{13} is 8 because:

$$(8)(5) \pmod{13} \equiv 40 \pmod{13} \equiv 1 \pmod{13}.$$

$$\text{So, } 8(5x) \equiv 8(2) \pmod{13}$$

$$x \equiv 16 \pmod{13}$$

$$x \equiv 3 \pmod{13}.$$

So $3 + 65\mathbb{Z} = \{\dots, -127, -62, 3, 68, 133, \dots\}$ are all solutions of $155x \equiv 75 \pmod{65}$.

The other integer solutions are gotten by:

$$\left(3 + \left(\frac{65}{5}\right)\right) + 65\mathbb{Z} = 16 + 65\mathbb{Z} = \{\dots, -144, -49, 16, 81, \dots\}$$

$$\left(3 + 2\left(\frac{65}{5}\right)\right) + 65\mathbb{Z} = 29 + 65\mathbb{Z} = \{\dots, -101, -36, 29, 94, \dots\}$$

$$\left(3 + 3\left(\frac{65}{5}\right)\right) + 65\mathbb{Z} = 42 + 65\mathbb{Z} = \{\dots, -88, -23, 42, 107, \dots\}$$

$$\left(3 + 4\left(\frac{65}{5}\right)\right) + 65\mathbb{Z} = 55 + 65\mathbb{Z} = \{\dots, -75, -10, 55, 120, \dots\}.$$

The 5 solutions in \mathbb{Z}_{65} are 3, 16, 29, 42, and 55.

Ex. Find all solutions in \mathbb{Z} to $20x \equiv 28 \pmod{32}$.

In this case $a = 20$, $b = 28$, and $n = 32$.

$d = \text{GCD}(20, 32) = 4$ and 4 divides 28, so there are 4 cosets in the solution.

Start by dividing the equation and the 32 by 4:

$$20x \equiv 28 \pmod{32}$$

$$5x \equiv 7 \pmod{8}.$$

The multiplicative inverse of 5 in \mathbb{Z}_8 is 5 so multiply the equation by 5:

$$(5)5x \equiv (5)7 \pmod{8}$$

$$x \equiv 35 \pmod{8}$$

$$x \equiv 3 \pmod{8}.$$

So $3 + 32\mathbb{Z} = \{\dots, -61, -29, 3, 35, 67, \dots\}$ are all solutions of $20x \equiv 28 \pmod{32}$.

The other integer solutions are given by:

$$3 + \frac{m}{d} + 32\mathbb{Z} = 3 + 8 + 32\mathbb{Z} = 11 + 32\mathbb{Z} = \{\dots, -53, -21, 11, 43, 75, \dots\}$$

$$3 + \frac{2m}{d} + 32\mathbb{Z} = 3 + 16 + 32\mathbb{Z} = 19 + 32\mathbb{Z} = \{\dots, -45, -13, 19, 51, 83, \dots\}$$

$$3 + \frac{3m}{d} + 32\mathbb{Z} = 3 + 24 + 32\mathbb{Z} = 27 + 32\mathbb{Z} = \{\dots, -37, -5, 27, 59, 91, \dots\}.$$

The 4 solutions in \mathbb{Z}_{32} are given by $\{3, 11, 19, 27\}$.