Theorem (Fermats Little Theorem)

Let p be a prime number, and let $a \in \mathbb{Z}$. Then either

$$p|a, \qquad \text{so that } a^i \equiv 0 \pmod{p} \text{ for all } i,$$

or

$$p \nmid a \qquad \text{and} \qquad a^{p-1} \equiv 1 \pmod{p}.$$

Note that this is not true if the modulus is not prime...

Example: $a^i \pmod{6}$

$\leftarrow i \rightarrow$

		2	3	4	5	6
	1	1	1	1	1	1
$\uparrow$	2	4	2	4	2	4
a	3	3	3	3	3	3
$\downarrow$	4	4	4	4	4	4
	5	1	5	1	5	1
	6	0	0	0	0	0

Theorem (Fermats Little Theorem)

Let p be a prime number, and let $a \in \mathbb{Z}$. Then either

$$p|a, \qquad \text{so that } a^i \equiv 0 \pmod{p} \text{ for all } i,$$

or

$$p \nmid a \qquad \text{and} \qquad a^{p-1} \equiv 1 \pmod{p}.$$

Note that this is not true if the modulus is not prime...

Example: $a^i \pmod{8}$

$\leftarrow i \rightarrow$

		2	3	4	5	6	7	8
	1	1	1	1	1	1	1	1
	2	4	0	0	0	0	0	0
$\uparrow$	3	1	3	1	3	1	3	1
a	4	0	0	0	0	0	0	0
$\downarrow$	5	1	5	1	5	1	5	1
	6	4	0	0	0	0	0	0
	7	1	7	1	7	1	7	1
	8	0	0	0	0	0	0	0

Theorem (Fermats Little Theorem)

Let p be a prime number, and let $a \in \mathbb{Z}$. Then either

$$p|a, \qquad \text{so that } a^i \equiv 0 \pmod{p} \text{ for all } i,$$

or

$$p \nmid a \qquad \text{and} \qquad a^{p-1} \equiv 1 \pmod{p}.$$

For what a and n are there solutions to

$$a^i \equiv 1 \pmod{n}?$$

1. If n is prime and $n \nmid a$, then $i = n - 1$ is a solution.
2. If $n|a$, then there is no solution.
3. If $\gcd(n, a) \neq 1$, then there is no solution:
   If $a^i \equiv 1 \pmod{n}$, then there is some $k \in \mathbb{Z}$ such that
   $$a^i - 1 = kn, \qquad \text{so } a(a^{i-1}) + (-k)n = 1.$$
   But we have $\gcd(n, a)$ divides every integer combination of n and a. $\lightning$

So what if $\gcd(a, n) = 1$, but n is not prime?

Are there solutions to $a^i \equiv 1 \pmod{n}$ when $\gcd(a, n) = 1$, but n is not prime?

Example: $a^i \pmod{6}$

$\leftarrow i \rightarrow$

a	2	3	4	5	6
1	**1**	**1**	**1**	**1**	**1**
2	4	2	4	2	4
3	3	3	3	3	3
4	4	4	4	4	4
5	**1**	**5**	**1**	**5**	**1**
6	0	0	0	0	0

Are there solutions to $a^i \equiv 1 \pmod{n}$ when $\gcd(a, n) = 1$, but n is not prime?

Example: $a^i \pmod{8}$

$\leftarrow i \rightarrow$

$\uparrow a \downarrow$	2	3	4	5	6	7	8
1	**1**	**1**	**1**	**1**	**1**	**1**	**1**
2	4	0	0	0	0	0	0
3	**1**	**3**	**1**	**3**	**1**	**3**	**1**
4	0	0	0	0	0	0	0
5	**1**	**5**	**1**	**5**	**1**	**5**	**1**
6	4	0	0	0	0	0	0
7	**1**	**7**	**1**	**7**	**1**	**7**	**1**
8	0	0	0	0	0	0	0

Are there solutions to $a^i \equiv 1 \pmod{n}$ when $\gcd(a, n) = 1$, but n is not prime?

Example: $a^i \pmod{10}$

$\leftarrow i \rightarrow$

$\uparrow a \downarrow$	2	3	4	5	6	7	8	9	10
1	**1**	**1**	**1**	**1**	**1**	**1**	**1**	**1**	**1**
2	4	8	6	2	4	8	6	2	4
3	**9**	**7**	**1**	**3**	**9**	**7**	**1**	**3**	**9**
4	6	4	6	4	6	4	6	4	6
5	5	5	5	5	5	5	5	5	5
6	6	6	6	6	6	6	6	6	6
7	**9**	**3**	**1**	**7**	**9**	**3**	**1**	**7**	**9**
8	4	2	6	8	4	2	6	8	4
9	**1**	**9**	**1**	**9**	**1**	**9**	**1**	**9**	**1**
10	0	0	0	0	0	0	0	0	0

Big question:
Are there solutions to $a^i \equiv 1 \pmod{n}$ when $\gcd(a, n) = 1$?

How did we prove Fermat's little theorem for prime modulus?

Step 1: Show that the numbers

$$a,\ 2a,\ 3a,\ \ldots,\ (p-1)a$$

form the same set as

$$1,\ 2,\ \ldots,\ p-1 \qquad \text{modulo } p.$$

Step 2: Multiply all these numbers together to find

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

Step 3: Since $(p-1)!$ is relatively prime to p, we can cancel.

Big question:
Are there solutions to $a^i \equiv 1 \pmod{n}$ when $\gcd(a, n) = 1$?

Step 1 for prime modulus: Show that the numbers

$$a,\ 2a,\ 3a,\ \ldots,\ (p-1)a$$

form the same set as

$$1,\ 2,\ \ldots,\ p-1 \qquad \text{modulo } p.$$

Analog for composite modulus: Consider the set of numbers $1 \leqslant a \leqslant n-1$ that are relatively prime to n.

n	$\{1 \leqslant a \leqslant n-1 \mid \gcd(a,n) = 1\}$
2	$\{1\}$
3	$\{1,2\}$
4	$\{1,3\}$
5	$\{1,2,3,4\}$
6	$\{1,5\}$
7	$\{1,2,3,4,5,6\}$
8	$\{1,3,5,7\}$

Big question:
Are there solutions to $a^i \equiv 1 \pmod{n}$ when $\gcd(a, n) = 1$?

Step 1 for prime modulus: Show that the numbers

$$a,\ 2a,\ 3a,\ \ldots,\ (p-1)a$$

form the same set as

$$1,\ 2,\ \ldots,\ p-1 \qquad \text{modulo } p.$$

Analog for composite modulus: Consider the set of numbers $1 \leqslant a \leqslant n-1$ that are relatively prime to n.

mod 4:

×	1	3
1	1	3
3	3	1

mod 6:

×	1	5
1	1	5
5	5	1

mod 8:

×	1	3	5	7
1	1	3	5	7
3	3	1	7	5
5	5	7	1	3
7	7	5	3	1

You try: Compute the integers $1 \leqslant a \leqslant 11$ that are relatively prime to 10, and compute their multiplication table modulo 10.

Big question:
Are there solutions to $a^i \equiv 1 \pmod{n}$ when $\gcd(a, n) = 1$?

Step 1 for prime modulus: Show that the numbers
$$a,\ 2a,\ 3a,\ \ldots,\ (p-1)a$$
form the same set as
$$1,\ 2,\ \ldots,\ p-1 \qquad \text{modulo } p.$$

Lemma
Let $\Phi(n) = \{x_1, x_2, \ldots, x_m\}$ be the set of numbers between 1 and $n-1$ that are relatively prime to n. Then, for any integer a with $\gcd(a, n) = 1$, the numbers

$$x_1 a,\ x_2 a,\ x_3 a,\ \ldots,\ x_m a$$

form the same set as $\Phi(n)$ modulo n.

Proof: Suppose $x_k a \equiv x_\ell a \pmod{n}$. Since $\gcd(a, n) = 1$, we can cancel the a's. But the x_k's are all distinct $\pmod{n}$, so $k = \ell$. □

Step 1 ✓

Big question:
Are there solutions to $a^i \equiv 1 \pmod{n}$ when $\gcd(a, n) = 1$?

Step 2: Multiply all these numbers together to find
$$(p-1)!a^{p-1} \equiv (p-1)! \pmod{p}.$$

Analog for composite modulus:
Let $a \in \mathbb{Z}$ with $\gcd(a, n) = 1$, and let $\{x_1, x_2, \ldots, x_m\}$ be the set of numbers between 1 and $n-1$ relatively prime to n.
Since
$$\{x_1, x_2, \ldots, x_m\} \equiv_n \{x_1 a, x_2 a, x_3 a, \ldots, x_m a\},$$
we have

$$x_1 x_2 \cdots x_m \equiv_n (x_1 a)(x_2 a) \cdots (a x_m) \equiv_n (x_1 x_2 \cdots x_m) a^m.$$

Step 2 ✓

Big question:
Are there solutions to $a^i \equiv 1 \pmod{n}$ when $\gcd(a, n) = 1$?

Step 3: Since $(p-1)!$ is relatively prime to p, we can cancel.

Analog for composite modulus:
Let $a \in \mathbb{Z}$ with $\gcd(a, n) = 1$, and let $\{x_1, x_2, \ldots, x_m\}$ be the set of numbers between 1 and $n-1$ relatively prime to n. So

$$a^m x \equiv x \pmod{n}, \quad \text{where } x = x_1 x_2 \cdots x_m.$$

Now, since x_j and n share no prime divisors, neither do x and n (by the fundamental theorem of arithmetic).
In other words, $\gcd(x, n) = 1$, so we can cancel:

$$a^m x \equiv x \pmod{n} \quad \text{implies} \quad a^m \equiv 1 \pmod{n}.$$

Step 3 ✓

Answer (Euler's formula): $a^i \equiv 1 \pmod{n}$ has a solution if and only if $\gcd(a, n) = 1$, in which case it is solved by

$$i = \#\{\text{ numbers between } 1 \text{ and } n-1 \text{ relatively prime to } n\ \}.$$

What is this value?

Euler's phi function

Let

$\Phi(n) = \{$ integers $1 \leqslant x \leqslant n-1$ relatively prime to n $\}$,

and define $\phi(n) = |\Phi(n)|$.

Examples:

n	$\{1 \leqslant a \leqslant n-1 \mid \gcd(a,n)=1\}$	$\phi(n)$
2	$\{1\}$	1
3	$\{1,2\}$	2
4	$\{1,3\}$	2
5	$\{1,2,3,4\}$	4
6	$\{1,5\}$	2
7	$\{1,2,3,4,5,6\}$	6
8	$\{1,3,5,7\}$	4

From your example: What is $\phi(10)$?

Example: For any prime p, $\boxed{\phi(p) = p-1}$ (all #s between 1 and $p-1$).

Euler's phi function

Let $\Phi(n) = \{$ integers $1 \leqslant x \leqslant n-1$ relatively prime to n $\}$,
and define $\phi(n) = |\Phi(n)|$.

Example: For any prime p, $\boxed{\phi(p) = p-1}$ (all #s between 1 and $p-1$).

Example: Computing $\phi(p^k)$ fo some $k \in \mathbb{Z}_{>0}$.
Aside: For sets, if $A \subseteq B$, then

$$|\{b \in B \mid b \notin B\}| = |B| - |A|.$$

Consider

$$B = \{ \text{ integers } 1 \leqslant x \leqslant p^k - 1 \}$$

and

$$A = \{b \in B \mid \gcd(b, p^k) > 1\} = \{b \in B \mid p \text{ divides } b\}$$
$$= \{ \text{ multiples of } p \text{ between } 1 \text{ and } p^k - 1 \}.$$

So $|B| = p^k - 1$ and $|A| = \lfloor (p^k-1)/p \rfloor = p^{k-1} - 1$. And therefore,

$$\phi(p^k) = |\Phi(p^k)| = |B| - |A| = (p^k - 1) - (p^{k-1} - 1) = \boxed{p^{k-1}(p-1)}.$$

Next time: $\phi(mn) = \phi(m)\phi(n)$ whenever $\gcd(m,n) = 1$.