Last time

Let
$$\Phi(n) = \{ \text{ integers } 1 \leqslant x \leqslant n-1 \text{ relatively prime to } n \},$$
and define $\phi(n) = |\Phi(n)|$. This is called Euler's phi function.

Example: Since $\Phi(8) = \{1, 3, 5, 7\}$, we have
$$\phi(8) = 4 = 2^2(2-1)\checkmark.$$

Example: For any prime p, $\boxed{\phi(p^k) = p^k - p^{k-1} = p^{k-1}(p-1)}$.

Theorem (Euler's formula)

For $n > 0$ and $a \in \mathbb{Z}$, either
$$\gcd(a, n) > 1, \qquad \text{so that } a^i \equiv 1 \pmod{p} \text{ has no solutions,}$$
or
$$\gcd(a, n) = 1 \qquad \text{and} \qquad a^{\phi(n)} \equiv 1 \pmod{n}.$$

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

Bijective proofs

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

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

Note
$$\phi(mn) = |\Phi(mn)|, \quad \phi(m) = |\Phi(m)|, \quad \text{and} \quad \phi(n) = |\Phi(n)|,$$
and so
$$\phi(m)\phi(n) = |\Phi(m) \times \Phi(n)|,$$
where $\Phi(m) \times \Phi(n) = \{(a, b) \mid a \in \Phi(m), b \in \Phi(n)\}$.

Example:
$$\Phi(4) = \{1, 3\}, \qquad \Phi(5) = \{1, 2, 3, 4\}$$
$$\Phi(4) \times \Phi(5) = \{(1,1), (1,2), (1,3), (1,4), (3,1), (3,2), (3,3), (3,4)\}$$
$$\Phi(20) = \{1,\ 3,\ 7,\ 9,\ 11,\ 13,\ 17,\ 19\}$$

Goal: Show $|\Phi(mn)| = |\Phi(m) \times \Phi(n)|$ by giving a bijection
$$\Phi(mn) \to \Phi(m) \times \Phi(n).$$

Theorem (Chinese Remainder Theorem)

Let m and n be integers satisfying $\gcd(m, n) = 1$, and let b and c be any integers. Then the simultaneous congruences

$$x \equiv b \pmod{m} \quad \textit{and} \quad x \equiv c \pmod{n}$$

have exactly one solution with $0 \leqslant x < mn$.

Q. How do you usually solve systems of linear equations?
One way: solve one equation for one variable, plug another equation, and simplify.

Example: Find an $0 \leqslant x < 4 \cdot 5$ that satisfies both

$$x \equiv 1 \pmod{4} \quad \text{and} \quad x \equiv 3 \pmod{5}.$$

Solution. Rewrite $x \equiv 1 \pmod{4}$ as $x = 1 + 4y$, and plug in:

$$3 \equiv_5 x = 1 + 4y, \quad \text{so} \quad 4y \equiv 2 \pmod{5}.$$

We know $4^4 \equiv 1 \pmod{5}$, so the inverse of 4 mod 5 is 4^3. Thus

$$y \equiv_5 4^3(4y) \equiv_5 4^3 \cdot 2 = 128 \equiv_5 3.$$

So $x = 1 + 4 \cdot 3 = \boxed{13}$.

Theorem (Chinese Remainder Theorem)

Let m and n be integers satisfying $\gcd(m, n) = 1$, and let b and c be any integers. Then the simultaneous congruences

$$x \equiv b \pmod{m} \quad \textit{and} \quad x \equiv c \pmod{n}$$

have exactly one solution with $0 \leqslant x < mn$.

Proof.

Rewrite $x \equiv b \pmod{m}$ as $x = b + ym$, and plug in:

$$c \equiv_n x \equiv_n b + ym. \quad \text{So} \quad ym \equiv (c - b) \pmod{n}.$$

Since $\gcd(m, n) = 1$, we can solve $ym \equiv (c - b) \pmod{n}$ uniquely with some $0 \leqslant y < n$. So we can solve uniquely for x. This gives us exactly one solution $b \leqslant x < b + mn$.

Since mn is an integer multiple of both m and n, reducing our solution modulo mn will fix x's value both mod m and mod n. □

Back to the ϕ function

Corollary

If $\gcd(m,n) = 1$, *then* $\phi(mn) = \phi(m)\phi(n)$.

Proof.

Define

$$f : \Phi(mn) \to \Phi(m) \times \Phi(n) \quad \text{defined by} \quad a \mapsto (b,c)$$

where $0 \leqslant b < m$ and $0 \leqslant c < n$ satisfy

$$b \equiv a \pmod{m} \text{ and } c \equiv a \pmod{n}\text{, so that } f(a) = (b,c). \qquad (*)$$

Well-defined: If $\gcd(a, mn) = 1$, then so $\gcd(a,m) = 1$ and $\gcd(a,n) = 1$. And if $a = qm + r$ with $0 \leqslant r < m$, then $1 = \gcd(a,m) = \gcd(r,m)$ (and similarly for n). ✓

Bijective: By the Chinese Remainder Theorem, there one and only one solution to the equations in $(*)$ between 1 and mn. So f^{-1} is well defined.

□

Theorem

Let $\phi(n)$ be the number of integers relatively prime to n (up to equivalence). Then $\phi(n)$ can be calculated by

1. *if p is prime, then $\phi(p^k) = p^k - p^{k-1} = p^{k-1}(p-1)$; and*
2. *if $\gcd(m,n) = 1$, then $\phi(mn) = \phi(m)\phi(n)$.*

Example: Compute $\phi(7000)$.

First

$$7000 = 7 \cdot (10)^3 = 2^3 5^3 7.$$

So

$$\phi(7000) = \phi(2^3)\phi(5^3)\phi(7) = (2^3 - 2^2)(5^3 - 5^2)(7-1).$$

In general:

1. Factor n into prime powers,
2. compute $\phi(p^k)$ for each maximal p power dividing n, and
3. multiply there together.

Example: Find some x satisfying $x^{12002} \equiv 9 \pmod{7000}$.

First question: Is x relatively prime to 7000?
Consider what it means that $x^{12002} \equiv 9 \pmod{7000}$:
This is equivalent to

$$x^{12002} - 9 = 7000k \quad \text{for some } k \in \mathbb{Z}, \quad \text{i.e. } 9 = x^{12002} - 7000k.$$

So since 9 is an integer combination of x and 7000, we must have $\gcd(x, 7000)|9$. But $\gcd(7000, 9) = 1$, so the only possibility is $\gcd(x, 7000) = 1$.
Yes, x relatively prime to 7000! So we can use $x^{\phi(n)} \equiv 1 \pmod{n}\ldots$

We just saw

$$\phi(7000) = (2^3 - 2^2)(5^3 - 5^2)(7 - 1) = \boxed{2400}.$$

So since

$$12002 = 5(2400) + 2, \quad \text{we have } x^{12002} = (x^{2400})^5 x^2.$$

So

$$9 \equiv_{7000} x^{12002} = (x^{2400})^5 x^2 \equiv_{7000} 1^5 x^2 = x^2.$$

At least 2 sol's: $x = 3$ and $x = -3 \equiv_{7000} 6997$. (There may be more.)