First example: Euler's Phi funtion.

Theorem (11.1 Euler's Phi funtion formula)

(a) If p is a prime and $k \geq 1$, then

$$\phi(p^k) = p^k - p^{k-1} = p^k\left(1 - \frac{1}{p}\right)$$

(b) If $\gcd(m,n) = 1$, then

$$\phi(mn) = \phi(m)\phi(n).$$

(c) For $m = p_1^{\alpha_1} p_2^{\alpha_2} \cdots p_r^{\alpha_r}$

$$\phi(m) = p_1^{\alpha_1} p_2^{\alpha_2} \cdots p_r^{\alpha_r}\left(1 - \frac{1}{p_1}\right) \cdots \left(1 - \frac{1}{p_r}\right)$$

$$= m \cdot \prod_{p \mid m}\left(1 - \frac{1}{p}\right)$$

Proof of (c): By (a), (b)

$$\phi(m) = \phi(p_1^{\alpha_1})\,\phi(p_2^{\alpha_2}) \cdots \phi(p_r^{\alpha_r})$$

$$= (p_1^{\alpha_1} - p_1^{\alpha_1 - 1})(p_2^{\alpha_2} - p_2^{\alpha_2 - 1}) \cdots (p_r^{\alpha_r} - p_r^{\alpha_r - 1})$$

$$= p_1^{\alpha_1}\left(1 - \frac{1}{p_1}\right) p_2^{\alpha_2}\left(1 - \frac{1}{p_2}\right) \cdots p_r^{\alpha_r}\left(1 - \frac{1}{p_r}\right)$$

$$= m \cdot \prod_{p \mid m} \left(1 - \frac{1}{p}\right)$$ □.

Proof of (a). Let p be a prime and $k \geq 1$.

$$\phi(p^k) = \#\{a : 1 \leq a \leq p^k,\ \gcd(a, p^k) = 1\}.$$

$$= p^k - \#\{a : 1 \leq a \leq p^k,\ p \mid a\}$$

We can show:

$$\{a : 1 \leq a \leq p^k,\ p \mid a\} = \{p, 2p, 3p, 4p, \cdots (p^{k-1}-1)p, p^k\}$$

$$\Rightarrow \#\{a : 1 \leq a \leq p^k,\ p \mid a\} = p^{k-1}$$

This implies:

$$\phi(p^k) = p^k - p^{k-1}$$ □.

Let $\gcd(m, n) = 1$.

$$A = \{a : 1 \leq a \leq mn,\ \gcd(a, mn) = 1\} \qquad \phi(mn) = \#A.$$

$$B = \{b : 1 \leq b \leq m,\ \gcd(b, m) = 1\} \qquad \phi(m) = \#B.$$

$C = \{c : 1 \le c \le n,\ \gcd(c, m) = 1\}$ $\quad \phi(n) = \#C$.

(We need to show: $\phi(mn) = \phi(m)\,\phi(n)$ i.e.
$\#A = \#B \cdot \#C$)

We look at the following set:

$$M = \left\{ (b, c) : \begin{array}{l} 1 \le b \le m,\ \gcd(b, m) = 1 \\ 1 \le c \le n,\ \gcd(c, n) = 1 \end{array} \right\}$$

We can show: $\#B \cdot \#C = \#M$

Therefore, it suffices to show: $\#A = \#M$.

Strategy: we construct a <u>bijective</u> map from A to M.

Definition: Let $f: A \to B$ be a map.

- f is <u>injective</u> if $f(b_1) = f(b_2) \Rightarrow b_1 = b_2$
- f is <u>surjective</u> if for any $b \in B$, we can find $a \in A$ such that $f(a) = b$.
- f is a <u>bijection</u> if f is both injective and surjective.

Let A, B be finite sets. If there is a bijective map $f: A \to B$., then $\#A = \#B$.

Lemma: Suppose that $a \equiv b \pmod{m}$, $a \equiv b \pmod{n}$ and $\gcd(m,n) = 1$.

Then $a \equiv b \pmod{mn}$

Proof: Exercise!

Theorem (11.2 Chinese Remainder Theorem) Let m, n be integers with $\gcd(m,n) = 1$. Let b, c be integers

Then the simultaneous congruences

$$x \equiv b \pmod{m} \qquad x \equiv c \pmod{n}$$

has exactly one solution with $0 \le x < mn$.

Moreover, $\gcd(x, mn) = 1$ if and only if

$$\gcd(b, m) = \gcd(b, n) = 1.$$

Proof: We look at the linear congruent equation:

$$my \equiv (c - b) \pmod{n}$$

$\gcd(m,n)=1 \Rightarrow$ we can find y_1 such that

$$my_1 \equiv (c-b) \pmod{n}.$$

Set $\quad x = my_1 + b.$

$$x \equiv b \pmod{m}$$

$$x = my_1 + b \equiv (c-b+b) \pmod{n} \equiv c \pmod{n}.$$

Take a between 1 and mn such that

$$a \equiv x \pmod{mn}.$$

$$a \equiv x \pmod{m} \equiv b \pmod{m}$$

$$a \equiv x \pmod{n} \equiv c \pmod{n}$$

Moreover part:

($\Rightarrow$) Suppose not. WLOG. assume that $\gcd(b,m)>1$

Then can find $p \mid \gcd(b,m) \Rightarrow p \mid b,\ p \mid m$

$a \equiv b \pmod{m} \Rightarrow p \mid a \Rightarrow p \mid \gcd(a,m)$

$\Rightarrow p \mid \gcd(a,mn)$. A contradiction!

($\Leftarrow$) $a \equiv b \pmod{m}$, $\gcd(a,m) = \gcd(b,m) = 1$.

$a \equiv c \pmod{n}$, $\gcd(a,n) = \gcd(c,n) = 1$

$\Rightarrow \gcd(a, mn) = 1$ □

We construct the following map:

$$f: \quad A \longrightarrow M$$

$$\left\{ a: \begin{array}{l} 1 \le a \le mn \\ \gcd(a, mn) = 1 \end{array} \right\} \longrightarrow \left\{ (b,c): \begin{array}{l} 1 \le b \le m \quad \gcd(b,m)=1 \\ 1 \le c \le n \quad \gcd(c,n)=1 \end{array} \right\}$$

$$a \longmapsto \left(a \pmod{m},\ a \pmod{n} \right).$$

We need to show f is both injective and surjective.

- injective: Let $a_1, a_2 \in A$ with $f(a_1) = f(a_2)$

(we need to show: $a_1 = a_2$)

$$\left(a_1 \pmod{m},\ a_1 \pmod{n} \right) = \left(a_2 \pmod{m},\ a_2 \pmod{n} \right)$$

$$\Rightarrow \quad a_1 \equiv a_2 \pmod{m}$$

$$a_1 \equiv a_2 \pmod{n}.$$

$\gcd(m,n) = 1 \Rightarrow a_1 \equiv a_2 \pmod{mn}$

$1 \le a_1 \le mn \quad 1 \le a_2 \le mn \Rightarrow a_1 = a_2$.

- surjective: (let $(b,c) \in M$, then we can find $a \in A$ such that $(a \pmod m, a \pmod n) = (b,c)$.)

This can be proved by apply Chinese Remainder Theorem

Proof of (b): We showed: the map between

$$A = \{ a : 1 \le a \le mn, \ \gcd(a, mn) = 1 \}$$

and

$$M = \left\{ (b,c) : \begin{array}{l} 1 \le b \le m \quad \gcd(b,m) = 1 \\ 1 \le c \le n \quad \gcd(c,n) = 1 \end{array} \right\}$$

is bijective.

Therefore $\# A = \# M$

$$\# A = \phi(mn)$$

$$\# M = \# B \cdot \# C = \phi(m) \cdot \phi(n).$$

$$\Rightarrow \phi(mn) = \phi(m)\,\phi(n).$$

□