Chapter 7: Recall p prime $a^{p-1} \equiv 1 \mod p$ if $(a,p)=1$

Now $a^{?} \equiv 1 \mod n$ if $\gcd(a,n)=1$

Answer: $\varphi(n)$

Definition:

Let $n \geq 1$, then

$$\varphi(n) = \#\{a : 0 < a \leq n \text{ with } \gcd(a,n)=1\}$$
$$= \#\{\text{units in } \mathbb{Z}/n\mathbb{Z}\}$$
$$= \#(\mathbb{Z}/n\mathbb{Z})^{\times}$$

units in

e.g. $\mathbb{Z}^{\times} = \{\pm 1\}$

$\mathbb{Q}^{\times} = \mathbb{Q} \setminus \{0\}$

Theorem

φ is multiplicative

proof: Let $m, n \in \mathbb{Z}_{\geq 1}$ $\gcd(m,n)=1$

We want to show that

$$\varphi(mn) = \varphi(m)\varphi(n)$$

If m or $n=1$, done since $\varphi(1)=1$

We now count the integers relatively prime to mn among the integers $0 < a \leq mn$

Arrange them all like this:

$$\begin{array}{cccccc}
1 & 2 & \cdots & r & \cdots & m \\
m+1 & m+2 & & m+r & & 2m \\
2m+1 & 2m+2 & & 2m+r & & 3m \\
\vdots & \vdots & & \vdots & & \vdots \\
(n-1)m+1 & (n-1)m+2 & \cdots & (n-1)m+r & \cdots & (n-1)m+m=nm
\end{array}$$

We will

① Eliminate all but $\varphi(m)$ columns

② In remaining columns $\varphi(n)$ numbers are ok

Idea: if s is relatively prime to m and also to n then s is relatively prime to mn.

Why? if $p|s$ & $p|mn$ then $p|m$ or $p|n$

① Among $1 \ldots m$ there are $\varphi(m)$ integers relatively prime to m

Let r be <u>not</u> relatively prime to m

Then every number in the rth column is not relatively prime to m

Why? $\gcd(qm+r, m) = \gcd(m, r)$
(showed this when showing Eucl. alg)

So all but $\varphi(m)$ columns contain only integers not relatively prime to m and therefore not relatively prime to mn. Delete those columns.

② Now assume $\gcd(m, r) = 1$ and look at
$r,\ m+r,\ 2m+r,\ \dots\ (n-1)m+r$

These are n integers. We show these are all different modulo n. Then $\varphi(n)$ of these will be relatively prime to n

Suppose $s_1 m + r \equiv s_2 m + r \mod n$
$s_1 m \equiv s_2 m \mod n$
$s_1 \equiv s_2 \mod n$
since m^{-1} exists modulo n
But $0 \leq s_1, s_2 \leq n-1$ so $s_1 \equiv s_2 \mod n$
$\Rightarrow s_1 = s_2$

Note: if $\gcd(a, n) = 1$ then $\gcd(sn+a, n) = 1$ too
so $\varphi(n)$ of these numbers are rel prime to n. Cross out those that aren't

Fri

Therefore $\varphi(m)\varphi(n)$ are relatively prime to both m and n and so to m and n

$$\varphi(mn)=\varphi(m)\,\varphi(n)$$

$\square$

Example $m=4$ $\varphi(m)=2$
$n=3$ $\varphi(n)=2$

1	2	3	4
5	6	7	8
9	10	11	12

all share a factor with $m=4$

1, 5, 9 is 1, 2, 3 mod 3
3, 7, 11 is 0, 1, 2 mod 3

left with 1, 5, 7, 11 $\varphi(12)=4$

Theorem

Let $n \in \mathbb{Z}_{>0}$ $n = p_1^{k_1} \dots p_r^{k_r}$

Then $\varphi(n) = (p_1^{k_1} - p_1^{k_1 - 1}) \dots (p_r^{k_r} - p_r^{k_r - 1})$

$$= n\left(1 - \frac{1}{p_1}\right)\left(1 - \frac{1}{p_2}\right) \dots \left(1 - \frac{1}{p_r}\right)$$

proof: Since φ is multiplicative

$\varphi(n) = \varphi(p_1^{k_1}) \dots \varphi(p_r^{k_r})$

So it suffices to show $\varphi(p^k) = p^k - p^{k-1}$ $k \geq 1$
p prime

Notice that $\gcd(a, p^k) = 1$ iff $p \nmid a$:

If $p \mid a$ then $\gcd(a, p^k) \geq p$

If $p \nmid a$, all divisors of p^k are divisible by p
except 1 so $\gcd(a, p^k) = 1$

So $\varphi(p^k) = p^k - \#\text{multiples of } p$

$\#$ of $\{a : 0 < a \leq p^k\}$

multiples of p: $p, 2p, 3p \dots p^{k-1} \cdot p = p^k$
p^{k-1} of them

So $\varphi(p^k) = p^k - p^{k-1}$

$\square$