Section 9 — Euler's Function

We will explore another multiplicative function — this one is really important.

Recall Fermat's Theorem: if p is prime (1) and $(a,p)=1$ (2), then $a^{p-1} \equiv 1 \pmod{p}$.

Q: what if p is not prime? Can we find a (hopefully small) k such that $a^k \equiv 1 \pmod{m}$. (not nec. prime)

Ex $\boxed{m=6}$ when can we find k s.t. $a^k \equiv 1 \pmod{m}$?

a	a^2	a^3	a^4	a^5	a^6	a^7
0	0	0	0	0	0	0
1	(1)	1	1	1	1	1
2	4	2	4	2	4	2
3	3	3	3	3	3	3
4	4	4	4	4	4	4
5	(1)	5	1	5	1	5

mod 6

$1^1 \equiv 1$

$5^2 \equiv 1$

only when $a=1,5$

what happened with 2,3,4?

Lemma If $a^k \equiv 1 \pmod{m}$ for some $k \in \mathbb{Z}^+$, then $(a,m)=1$.

pf Assume $a^k \equiv 1 \pmod{m}$. Let $d=(a,m)$. we show $d=1$.

- $a^k \equiv 1 \pmod{m} \Rightarrow a^k - 1 \equiv 0 \pmod{m} \Rightarrow m \mid a^k - 1$
- $d \mid m$, $m \mid a^k - 1 \Rightarrow d \mid a^k - 1$
- $(a^k - 1) - a^k = -1$ $\Rightarrow d \mid -1 \Rightarrow d = 1$

(d is a factor of $a^k - 1$; d is a factor of a^k)

□

* So (2) above is necessary

Ex $\boxed{m=10}$ when can we find k s.t. $a^k \equiv 1 \pmod m$? And what is a "k" that works?

a	a^2	a^3	a^4	a^5	a^6	...
0	0	0	0	0	0	
○ (1)	1					
2	4	8	6	2	4	
○ 3	9	7	(1)			
4	6	4	6	4	6	
5	5	5	5	5	5	
6	6	6	6	6	6	
○ 7	9	3	(1)			
8	4	2	6	8	4	
○ 9	(1)					

only 4 that have a chance

mod 10

$1^1 = 1$
$3^4 = 1$
$7^4 = 1$
$9^2 = 1$

* no chance if $(a,10) \neq 1$
* so, if $(a,10) = 1$ then $a^4 = 1$. where did the 4 come from?

Ex $\boxed{m=14}$ show that $a^6 \equiv 1 \pmod{14}$ for all a relatively prime to 14.

only 6 that have a chance

$\boxed{a \equiv 1}$ $1^6 \equiv 1$ ✓

$\boxed{a \equiv 3}$ $3^2 \equiv 9$, $3^3 \equiv 27 \equiv -1$, $3^6 \equiv 3^3 \cdot 3^3 \equiv 1$ ✓

$\boxed{a \equiv 5}$ $5^2 \equiv 25 \equiv -3$, $5^3 \equiv 5(-3) \equiv -1$, $5^6 \equiv 1$ ✓

$\boxed{a \equiv 9}$ $9^6 \equiv (-5)^6 \equiv (-1)^6 \cdot 5^6 \equiv 1$ ✓ (in fact $9^3 \equiv 3^6 \equiv 1$)

$\boxed{a \equiv 11}$ $11^6 \equiv (-3)^6 \equiv 1$ ✓ (in fact $11^3 \equiv (-3)^3 \equiv -1 \cdot 3^3 \equiv 1$)

$\boxed{a \equiv 13}$ $13^6 \equiv (-1)^6 \equiv 1$ ✓ (in fact $13^2 \equiv (-1)^2 \equiv 1$)

* where did the 6 come from?

Def Let $n \in \mathbb{Z}^+$. Define $\varphi(n)$ to be the number of integers between 1 and n that are relatively prime to n. This is called Euler's φ-function.

Ex

- $\varphi(12) = 4$ — 1 2 3 4 5 6 7 8 9 10 11 12
- $\varphi(9) = 6$ — 1 2 3 4 5 6 7 8 9
- $\varphi(11) = 10$ — 1 2 3 4 5 6 7 8 9 10 11

Lemma If p is prime, then $\varphi(p) = p-1$.

pf $1, 2, \ldots, p-1$ are relatively prime to p. □

Question: what about $\varphi(p^n)$? Think about 3^4...

1, 2, 3, 4, 5, 6, 7, 8, 9, 10, 11, 12, 13, 14, 15, ..., 77, 78, 79, 80, 81

So, how many were crossed out? $\frac{1}{3}$ of them.

Thus, $\varphi(3^4) = \underbrace{3^4}_{\#\text{ b/w 1 and } 3^4} - \underbrace{\frac{1}{3}(3^4)}_{\#\text{ not rel. prime to } 3^4}$.

Lemma If p is prime, then $\varphi(p^n) = p^n - p^{n-1} = \boxed{p^{n-1}(p-1)}$

Pf The numbers not rel. prime to p^n are the multiples of p. Of the numbers from 1 to p^n, $\frac{1}{p}$ of them multiples of p. Thus,

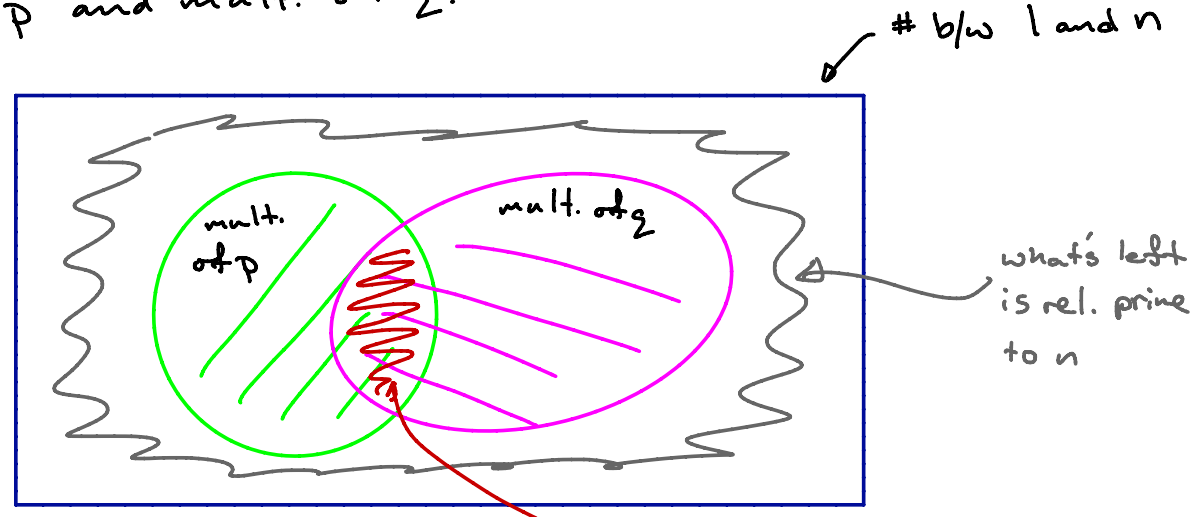
$$\varphi(p^n) = \underbrace{p^n}_{\#\text{ b/w 1 and } p^n} - \underbrace{\frac{1}{p} \cdot p^n}_{\#\text{ not rel. prime to } p^n} = p^n - p^{n-1} = p^{n-1}(p-1)$$

Ex $\varphi(125) = \varphi(5^3) = 5^2 \cdot (5-1) = 100$

But what about $\varphi(2^2 \cdot 5^2)$? or more generally $\varphi(p^a q^b)$?

Suppose p, q are different primes. Let $n = p^a q^b$.

What numbers are not rel. prime to n? ... multiples of p and mult. of q. So



$$\varphi(n) = n - \frac{n}{p} - \frac{n}{q} + \frac{n}{pq}$$

$\frac{n}{p}$: mult. of p $\quad$ $\frac{n}{q}$: mult. of q $\quad$ $\frac{n}{pq}$: but we removed mult. of pq twice!

$$= p^a q^b - p^{a-1} q^b - p^a q^{b-1} - p^{a-1} q^{b-1}$$

$$= q^b (p^a - p^{a-1}) - q^{b-1} (p^a - p^{a-1})$$

$$= (p^a - p^{a-1})(q^b - q^{b-1}) = \varphi(p^a) \cdot \varphi(q^b).$$

! this generalizes...

Theorem 3 Let $n \in \mathbb{Z}^+$, and let $n = p_1^{e_1} p_2^{e_2} \cdots p_k^{e_k}$ be the prime-power decomposition of n. Then

$$\varphi(n) = \varphi(p_1^{e_1})\,\varphi(p_2^{e_2}) \cdots \varphi(p_k^{e_k}).$$

Ex

$$\varphi(1200) = \varphi(2^4 \cdot 3 \cdot 5^2) = \varphi(2^4)\varphi(3)\varphi(5^2) = 2^4(2-1)\cdot(3-1)\cdot 5^2(5-1) = \boxed{320}$$

As with d and σ...

Theorem 2 φ is multiplicative.

Great! ... but why do we care about φ?

Theorem 1 Let $m \in \mathbb{Z}^+$. If $(a, m) = 1$, then $a^{\varphi(m)} \equiv 1 \pmod{m}$.

* Note that if m is a prime p, then $a^{\varphi(p)} = a^{p-1} \equiv 1 \pmod{p}$, which was Fermat's Theorem.
* proof is very similar to Fermat's Theorem — see book.

Ex Compute each of the following

(a) $14^{50} \pmod{45}$ $\quad \varphi(45) = \varphi(9)\varphi(5) = 3 \cdot 2 \cdot 4 = \underline{\underline{24}}$

$\Rightarrow 14^{24} \equiv 1 \pmod{45} \Rightarrow 14^{50} \equiv 14^{48} \cdot 14^2 \equiv 140 + 56 \equiv 196 \equiv \boxed{16}$

(b) $12^{49} \pmod{45}$

$\varphi(45) = 24 \Rightarrow 12^{49} \equiv 12^{48} \cdot 12 \equiv 12 \pmod{45}$

No!! $(12, 45) \neq 1$

Need to do what we did before — solve a system:

Let $a \equiv 12^{49} \pmod{45}$

① $a \equiv 12^{49} \bmod 5$

② $a \equiv 12^{49} \bmod 9$

mod 5 ① $a \equiv 12^{49} \equiv 2^{49} \equiv (2^4)^{12} \cdot 2 \equiv \boxed{2} \pmod 5$

$(2,5) = 1$ so use Fermat

mod 9 ② $a \equiv 12^{49} \equiv 3^{49} \equiv \boxed{0} \pmod 9$

$(3,9) \neq 1$, so ad hoc: $3^1, 3^2 \equiv 9 \equiv 0, 3^3 \equiv 0, \ldots, 3^{49} \equiv 0$

Answer: $a \equiv 2 \pmod 5 \Rightarrow a = 5k+2$

$a \equiv 0 \pmod 9 \Rightarrow 5k+2 \equiv 0 \bmod 9$

$\Rightarrow 5k \equiv -2 \equiv 7 \equiv 16 \equiv 25$

$\Rightarrow k \equiv 5 \bmod 9$

$\Rightarrow k = 9s + 5$

$\Rightarrow a = 45s + 27$

$\Rightarrow a \equiv \boxed{27} \pmod{45}$

A final theorem about φ...

Theorem 4 Let $n \geq 1$. Let $d_1, d_2, \ldots, d_k$ be the divisors of n. Then

$$\varphi(d_1) + \varphi(d_2) + \cdots + \varphi(d_k) = n.$$

In other notation,

the sum ranges over all d s.t. $d \mid n$

$$\sum_{d \mid n} \varphi(d) = n$$

Ex Let $n=45$.

- The divisors of 45 are $1,3,9,5,15,45$
- $\varphi(1)+\varphi(3)+\varphi(9)+\varphi(5)+\varphi(15)+\varphi(45)=$

$= 1+2+6+4+2\cdot 4+3\cdot 2\cdot 4 = 1+2+6+4+8+24 = 45$

But why? Let's repeat the above example for $n=12$ and cleverly group the numbers.

Let $n=12$.

- The divisors of 12 are $1,2,3,4,6,12$
- Group the numbers $1,2,3,4,5,6,7,8,9,10,11,12$ according to their gcd with $n=12$

$(a,12)=1$: $G_1=\{1,5,7,11\}$ $\quad$ $(a,12)=4$: $G_4=\{4,8\}$

$(a,12)=2$: $G_2=\{2,10\}$ $\quad$ $(a,12)=6$: $G_6=\{6\}$

$(a,12)=3$: $G_3=\{3,9\}$ $\quad$ $(a,12)=12$: $G_{12}=\{12\}$

* $a\in G_3 \iff (a,12)=3 \iff (a/3, 12/3)=1 \iff \frac{a}{3}$ is rel. prime to $12/3$

  Thus G_3 contains $\varphi(12/3)$ numbers.

* $a\in G_d \iff (a,12)=d \iff \left(\frac{a}{d}, \frac{12}{d}\right)=1 \iff \frac{a}{d}$ is rel. prime to $\frac{12}{d}$

  Thus G_d contains $\varphi\left(\frac{12}{d}\right)$ numbers.

Now,

$$\begin{aligned} n &= \text{size of } G_1 + \text{size of } G_2 + \cdots + \text{size of } G_{12} \\ &= \varphi\left(\tfrac{12}{1}\right) + \varphi\left(\tfrac{12}{2}\right) + \varphi\left(\tfrac{12}{3}\right) + \varphi\left(\tfrac{12}{4}\right) + \varphi\left(\tfrac{12}{6}\right) + \varphi\left(\tfrac{12}{12}\right) \\ &= \varphi(12) + \varphi(6) + \varphi(4) + \varphi(3) + \varphi(2) + \varphi(1) \\ &= \sum_{d \mid n} \varphi(d). \end{aligned}$$

The same idea can be used to prove Theorem 4 — see the book.