Section 7.1: The Euler Phi Function

ϕ – \phi

φ – \varphi

Euler's Thm $\longrightarrow$ useful to compute $\varphi(1001)$

Current approach to $\varphi(1001)$:

- for each $1 \leq x \leq 1001$, check if $(x, 1001) = 1$ $\leftarrow$ Euclidean algorithm
- count the x s.t. $(x, 1001) = 1$

Problem: Very inefficient!

Goal: Find a better way of computing $\varphi(m)$

Easy: $\varphi(p) = p - 1$ when p is prime

b/c $(\mathbb{Z}/p\mathbb{Z})^\times = \{1, 2, 3, \ldots, p-1\}$

Q: what is $\varphi(p^a)$?

Ex: Compute $\varphi(9)$, $\varphi(27)$

$$(\mathbb{Z}/9\mathbb{Z}) = \{1, 2, \cancel{3}, 4, 5, \cancel{6}, 7, 8, \cancel{9}\}$$

$$\downarrow$$

$$(\mathbb{Z}/9\mathbb{Z})^\times = \{1, 2, 4, 5, 7, 8\}$$

$$\varphi(9) = \# \uparrow = 6$$

$$\mathbb{Z}/27\mathbb{Z} = \{1, 2, \cancel{3}, 4, 5, \cancel{6}, 7, \cancel{\ldots}, \cancel{27}\}$$

$$(\mathbb{Z}/27\mathbb{Z})^\times = \{1, 2, 4, 5, 7, 8, \ldots, 25, 26\}$$

$$\varphi(27) = 18$$

In general:

$$\mathbb{Z}/p^a\mathbb{Z} = \{1, 2, 3, \ldots, p-1, \cancel{p}, p+1, \ldots, \cancel{p^a}\}$$

Note: x is not rel. prime to p^a

iff x is a multiple of p

The elts. of $\mathbb{Z}/p^a\mathbb{Z}$ which are not rel. prime to p^a are $p, 2p, 3p, \ldots, p(p^{a-1}-1), p^a$

$$\#\{p, 2p, \ldots, p^a\} = \#\{kp : 1 \le k \le p^{a-1}\}$$

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

$$\varphi(p^a) = \#\left(\mathbb{Z}/p^a\mathbb{Z}\right)^\times = \#\left(\mathbb{Z}/p^a\mathbb{Z}\right) - \#\{p, 2p, \ldots, p^a\}$$

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

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

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

Cor: If you randomly select an integer, x, in $\mathbb{Z}/p^a\mathbb{Z}$, the probability that $x \in (\mathbb{Z}/p^a\mathbb{Z})^\times$ is

$$\frac{\#(\mathbb{Z}/p^a\mathbb{Z})^\times}{\#(\mathbb{Z}/p^a\mathbb{Z})} = \frac{p^a\left(1-\frac{1}{p}\right)}{p^a}$$

$$= \underbrace{1 - \frac{1}{p}}_{\text{independent of } a\,!}$$

Generalizing

If $n = p_1^{e_1} \cdots p_g^{e_g}$ is prime fact. of n, then Sun-Tsu's Thm

$$\to \mathbb{Z}/n\mathbb{Z} \cong \mathbb{Z}/p_1^{e_1}\mathbb{Z} \times \cdots \times \mathbb{Z}/p_g^{e_g}\mathbb{Z}$$

$$\left(\mathbb{Z}/n\mathbb{Z}\right)^\times \cong \left(\mathbb{Z}/p_1^{e_1}\mathbb{Z}\right)^\times \times \cdots \times \left(\mathbb{Z}/p_g^{e_g}\mathbb{Z}\right)^\times$$

$$\varphi(n) = \varphi(p_1^{e_1}) \cdots \varphi(p_g^{e_g})$$

Thm: If $m, n \in \mathbb{Z}_{>0}$ and $\underline{(m,n) = 1}$, then $\varphi(mn) = \varphi(m)\varphi(n)$

necessary

Pf: Fact: $(x, mn) = 1$ iff

$(x, m) = 1$ and $(x, n) = 1$

Consider

contains $\varphi(n)$ elts. rel. prime to mn

1 mod m	1	$1+m$	$1+2m$	$\cdots$	$1+(n-1)m$
2 mod m	2	$2+m$	$2+2m$	$\cdots$	$2+(n-1)m$
3 mod m	3	$3+m$	$3+2m$	$\cdots$	$3+(n-1)m$
	$\vdots$	$\vdots$	$\vdots$		$\vdots$
r mod m	r	$r+m$	$r+2m$	$\cdots$	$r+(n-1)m$
$\vdots$	$\vdots$	$\vdots$	$\vdots$		$\vdots$
0 mod m	m	$2m$	$3m$	$\cdots$	nm

$\varphi(mn)$ counts the # of x rel. prime to mn in this grid

Look at row 1: Since each x in row 1 has $x \equiv 1 \mod m$ and $(1, m)$

$\rightarrow (x, m) = 1$

The elts of row 1:

$$\{0, 1, 2, 3, \ldots, (n-1)\} = \mathbb{Z}/n\mathbb{Z}$$

$$\downarrow \times m$$

$$\{0, m, 2m, 3m, \ldots, (n-1)m\}$$ since $(m,n)=1$ complete set of res. mod n

$$\downarrow +1$$

$$\{1, 1+m, 1+2m, 1+3m, \ldots, 1+(n-1)m\}$$

complete set of res. mod n.

Aside $\{0, 1, 2, 3\}$ is complete set of res. mod 4

but $\{0, 2, 4, 6\}$ is not complete set of res. mod 4

Why not?

In row 1, there are $\varphi(n)$ entries which are rel. prime to n.

In row 1, every entry is rel. prime to m.

So there are $\varphi(n)$ entries in row 1 which are rel. prime to m and n, i.e. rel. prime to mn.

Now consider row 2:

$2 \quad 2+m \quad 2+2m \quad 2+3m \quad \cdots \quad 2+(n-1)m$

If $(2,m) > 1$, note that every elt. in row 2 has gcd with m greater than 1.

I.e. every elt. of row 2 is not rel. prime to mn.

$\rightarrow$ row 2 contributes 0 elts. of $(\mathbb{Z}/mn\mathbb{Z})^\times$

If $(2,m)=1$, then every elt. of row 2 is rel. prime to m. Similar arg. as for row 1 gives that row 2 contributes $\varphi(n)$ elts. of $(\mathbb{Z}/mn\mathbb{Z})^\times$

For row r.

if $(r,m)>1$, then row r contributes 0 elts. of $(\mathbb{Z}/mn\mathbb{Z})^\times$

if $(r,m)=1$, then row r contributes $\varphi(n)$ elts of $(\mathbb{Z}/mn\mathbb{Z})^\times$

There are $\varphi(m)$ rows, each of which gives $\varphi(n)$ elts. of $(\mathbb{Z}/mn\mathbb{Z})^\times$

So $\varphi(mn) = |(\mathbb{Z}/mn\mathbb{Z})^\times| = \varphi(m)\varphi(n)$

Q: Is it true that

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

for all m, n?

A: No

$$\varphi(4) = 2$$

$$\varphi(2)\,\varphi(2) = 1\cdot 1 = 1$$

Q: Do there exist m, n with $(m,n) > 1$ and $\varphi(m)\varphi(n) = \varphi(mn)$?

Examples

- $\varphi(1001) = \varphi(7\cdot 11\cdot 13) \underset{\substack{\uparrow \\ (7,\, 11\cdot 13) = 1}}{=} \varphi(7)\,\varphi(11\cdot 13)$

$$= 6\cdot\varphi(11)\,\varphi(13) = 6\cdot 10\cdot 12 = 720$$

- $\varphi(36) = \varphi(2^2\, 3^2) \underset{\substack{\uparrow \\ (2^2,\, 3^2)}}{=} \varphi(2^2)\cdot\varphi(3^2)$

$$= 2^{2-1}(2-1)\cdot 3^{2-1}(3-1) = 12$$

$$\cdot\ \varphi(p_1^{e_1}\cdots p_g^{e_g}) = \varphi(p_1^{e_1})\,\varphi(p_2^{e_2}\cdots p_g^{e_g})$$

$$(n = p_1^{e_1}\cdots p_g^{e_g})$$

$$= \varphi(p_1^{e_1})\,\varphi(p_2^{e_2})\,\varphi(p_3^{e_3}\cdots p_g^{e_g})$$

$$\vdots$$

$$= \varphi(p_1^{e_1})\cdots\varphi(p_g^{e_g})$$

$$= (p_1^{e_1-1})(p_1-1)\cdots(p_g^{e_g-1})(p_g-1)$$

$$= p_1^{e_1-1}\cdots p_g^{e_g-1}\,(p_1-1)\cdots(p_g-1)$$

$$= p_1^{e_1}\left(1-\frac{1}{p_1}\right)\cdots p_g^{e_g}\left(1-\frac{1}{p_g}\right)$$

$$= p_1^{e_1}\cdots p_g^{e_g}\left(1-\frac{1}{p_1}\right)\cdots\left(1-\frac{1}{p_g}\right)$$

$$\varphi(n) = n\left(1-\frac{1}{p_1}\right)\cdots\left(1-\frac{1}{p_g}\right)$$

$$\varphi(n) = n\prod_{\substack{p\mid n \\ p \text{ prime}}}\left(1-\frac{1}{p}\right)$$

You can use the following w/o proof on HW.

① Find all $n \in \mathbb{Z}_{>0}$ with $\varphi(n) = 1$

Note $\varphi(1) = 1$

(b/c $\varphi(1 \cdot n) = \varphi(1)\varphi(n)$)

Otherwise $n = p_1^{e_1} \cdots p_g^{e_g}$ for $p_1, \dots, p_g$ distinct primes, $e_1, \dots, e_g > 0$

$$1 = \varphi(n) = \underset{\overset{\|}{1}}{p_1^{e_1-1}} \cdots \underset{\overset{\|}{1}}{p_g^{e_g-1}} \underset{\overset{\|}{1}}{(p_1-1)} \cdots \underset{\overset{\|}{1}}{(p_g-1)}$$

$$\Downarrow$$

$$p_1 = 2$$

So 2 is the <u>only</u> prime factor of n

$2^{e_1-1} = 1 \to e_1 = 1 \to n = 2$

Conclusion: $n = 1, 2$ are the only possibilities

② Find all $n \in \mathbb{Z}_{>0}$ s.t. $\varphi(n) = 2$

$n \neq 1$

$n = p_1^{e_1} \cdots p_g^{e_g}$

$2 = \varphi(n) = p_1^{e_1 - 1} \cdots p_g^{e_g - 1} (p_1 - 1) \cdots (p_g - 1)$

Suppose $e_i > 1$ for some i (WLOG, $e_1 > 1$)

So $p_1^{e_1 - 1} \mid 2 \to p_1 = 2,\ e_1 = 2$

$\to$ no more primes dividing n

$\to n = 2^2 = 4$

Suppose $e_i = 1$ for all i

So $p_i - 1 = 2$ for some $i \to p_i = 3$

So $n = 3, 6$

Conclusion: $\varphi(n) = 2 \to n = 3, 4, 6$

Thm: Let $n \in \mathbb{Z}_{>0}$. Then

$$\sum_{\substack{d \mid n \\ d > 0}} \varphi(d) = n$$

Ex: $n = 18$

Divisors of 18: 1, 2, 3, 6, 9, 18

$$\begin{array}{cccccc} \varphi(1), & \varphi(2), & \varphi(3), & \varphi(6), & \varphi(9), & \varphi(18) \\ \shortparallel & \shortparallel & \shortparallel & \shortparallel & \shortparallel & \shortparallel \\ 1 & 1 & 2 & 2 & 6 & 6 \end{array}$$

$$\rightarrow \sum_{d \mid 18} \varphi(d) = 18 \quad \checkmark$$

Note: $(x, 18)$ is a divisor of 18

Q: Which elts. of $\mathbb{Z}/18\mathbb{Z}$ have $(x, 18) = 1$?

$\rightarrow$ $x = 1, 5, 7, 11, 13, 17$

$\rightarrow$ There are $\varphi(18)$

Q: Which elts. of $\mathbb{Z}/18\mathbb{Z}$ have $(x, 18) = 2$?

$\rightarrow x = 2, 4, 8, 10, 14, 16$

Note $(x, 18) = 2 \Longleftrightarrow (\frac{x}{2}, 9) = 1$

$\frac{x}{2} = 1, 2, 4, 5, 7, 8$

$\hookrightarrow$ reduced res. sys. for 9

$\rightarrow \varphi(9)$ numbers here

Q: Which elts. of $\mathbb{Z}/18\mathbb{Z}$ have $(x, 18) = 3$?

$x = 3, 15$

$(x, 18) = 2 \Longleftrightarrow (\frac{x}{3}, 6) = 1$

$\frac{x}{3} = 1, 5$

↳ reduced res. sys. for 6

$\to \varphi(6)$ numbers here

For elts. of $\mathbb{Z}/18\mathbb{Z}$ with $(x, 18) = 6$, we get $x = 6, 12$

$\to \varphi(3)$ numbers here

For elts. of $\mathbb{Z}/18\mathbb{Z}$ $(x, 18) = 9$, we get

$x = 9$

$\longrightarrow \varphi(2)$

For elts. of $\mathbb{Z}/18\mathbb{Z}$ with $(x, 18) = 18$, we get

$x = 0$

$\longrightarrow \varphi(1)$

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

For each $d \mid n$, define

$$C_d := \{0 \leq x < n : (x, n) = d\}$$

Note that these sets are disjoint and

$$\mathbb{Z}/n\mathbb{Z} = \bigcup_{d \mid n} C_d$$

$x \in C_d$ iff $0 \le x < n$ and $(x, n) = d$

iff $0 \le \frac{x}{d} < \frac{n}{d}$ and $\left(\frac{x}{d}, \frac{n}{d}\right) = 1$

there are $\varphi\left(\frac{n}{d}\right)$ such numbers

$\longrightarrow \quad |C_d| = \varphi\left(\frac{n}{d}\right)$

$$n = \#\left(\mathbb{Z}/n\mathbb{Z}\right) = \#\left(\bigcup_{d \mid n} C_d\right)$$

$$= \sum_{d \mid n} \# C_d = \sum_{d \mid n} \varphi\left(\frac{n}{d}\right)$$

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

$n = 18$

$$\sum_{d \mid 18} \varphi\left(\frac{18}{d}\right) = \varphi(18) + \varphi(9) + \varphi(6) + \varphi(3) + \varphi(2) + \varphi(1)$$

$$\sum_{d \mid 18} \varphi(d) = \varphi(1) + \varphi(2) + \varphi(3) \\ \varphi(6) + \varphi(9) + \varphi(18)$$