Lecture 6 Euler's Phi Function

Def: Recall that $\phi(n) = \#U(n) = \#\{x \mid 1 \le x < n,\ \gcd(x,n) = 1\}$

Note: If p is prime then $\phi(p) = p - 1$

Ex:

$\phi(2) = 1, \quad U(2) = \{1\}$
$\phi(3) = 2, \quad U(3) = \{1,2\}$
$\phi(4) = 2, \quad U(4) = \{1,3\}$
$\phi(5) = 4, \quad U(5) = \{1,2,3,4\}$
$\phi(6) = 2, \quad U(6) = \{1,5\}$
$\vdots$
$\phi(15) = 8, \quad U(15) = \{1,2,4,7,8,11,13,14\}$

Thm: Suppose $\gcd(x,n) = 1$. Then $x^{\phi(n)} \equiv 1 \pmod{n}$

Pf: Suppose that $U(n) = \{a_1, a_2, ..., a_k\}$ (note n need not be prime). Here $k = \phi(n)$.

Since $\gcd(x,n) = 1$, we must have $x \in U(n)$. Consider the set $x * U(n) = \{x * a_1, x * a_2, ..., x * a_k\}$. $U(n)$ is closed under multiplication. Hence each $x * a_i \in U(n)$.

Claim: If $i \neq j$ then $x * a_i \not\equiv x * a_j \pmod{n}$

Pf of claim: Assume $x * a_i \equiv x * a_j \pmod{n}$ then

$x^{-1} * x * a_i \equiv x^{-1} * x * a_j \pmod{n}$
$a_i \equiv a_j \pmod{n} \Rightarrow i = j$

The claim implies that $U(n) = x * U(n)$ (as sets). Hence the product of all the elements in each set are equal.

$a_1 a_2 \cdots a_k \equiv (xa_1)(xa_2)\cdots(xa_k) \pmod{n} \equiv x^{\phi(n)} a_1 a_2 \cdots a_k \pmod{n}$
$x^{\phi(n)} \equiv 1 \pmod{n}$

Corollary: Suppose $\gcd(x,n) = 1$ and $e_1 \equiv e_2 \pmod{n}$ then $x^{e_1} \equiv x^{e_2} \pmod{\phi(n)}$

Pf: $e_1 \equiv e_2 \pmod{\phi(n)} \Rightarrow e_1 = e_2 + k\phi(n) \Rightarrow x^{e_1} \equiv x^{e_2 + k\phi(n)} \equiv x^{e_2}(x^{\phi(n)}) \equiv x^{e_2} \pmod{n}$

This means that we can reduce powers $\bmod \phi(n)$.

Ex.
(1) Compute 3^{43} in F_{23}^*

Fast power algorithm
43 = 32 + 8 + 2 + 1

$$3^1 \equiv 3 \pmod{23}$$

$$3^2 \equiv 9 \pmod{23}$$

$$3^4 \equiv 9^2 \equiv 81 \equiv 12 \pmod{23}$$

$$3^8 \equiv 12^2 \equiv 144 \equiv 6 \pmod{23}$$

$$3^{16} \equiv 6^2 \equiv 36 \equiv 13 \pmod{23}$$

$$3^{32} \equiv 13^2 \equiv 169 \equiv 8 \pmod{23}$$

$$3^{43} \equiv 8 * 6 * 9 * 3 \equiv 8 \pmod{23}$$

Euler's Theorem

$$\phi(23) = 22$$

$$43 \equiv 21 \pmod{22}$$

$$3^{43} \equiv 3^{21} \equiv 3^{16+4+1} \equiv 13 * 12 * 3 \equiv 8 \pmod{23}$$

(2)
Compute 5^{37} in F_{19}^*

Fast power algorithm
37 = 32 + 4 + 1

$$5^1 \equiv 5 \pmod{19}$$

$$5^2 \equiv 25 \equiv 6 \pmod{19}$$

$$5^4 \equiv 6^2 \equiv 36 \equiv 17 \pmod{19}$$

$$5^8 \equiv 17^2 \equiv 281 \equiv 4 \pmod{19}$$

$$5^{16} \equiv 4^2 \equiv 16 \pmod{19}$$

$$5^{32} \equiv 16^2 \equiv 256 \equiv 9 \pmod{19}$$

$$5^{37} \equiv 9 * 17 * 5 \equiv 5 \pmod{19}$$

Euler's Theorem

$$\phi(19) = 18$$

$$37 \equiv 1 \pmod{18}$$

$$5^{37} \equiv 5^1 \equiv 5 \pmod{19}$$

Corollary 2: Let $f(x) = x^a$ considered as a function $f : Z_n \to Z_n$. Suppose that $\gcd(a, \phi(n)) = 1$, then a has an inverse $d = a^{-1} \pmod{\phi(n)}$. Define the function $g(x) = x^d$, this is an inverse to the function f for $x \in U(n)$.

Pf: Let $x \in U(n)$, we need to show $g(f(x)) \equiv 1 \pmod{n}$

$g(f(x)) \equiv g(x^a) \equiv (x^a)^d \equiv x^{ad} \equiv x \pmod{n}$ where the last congruence follows from the previous Corollary.

Ex:
Let $f(x) = x^5 \pmod{37}$. Since 37 is prime, $\phi(37) = 36$ and $\gcd(5, 36) = 1$.

$$36 = 7 * 5 + 1 \Rightarrow 1 = 36 - 7 * 5 \Rightarrow 5^{-1} \equiv -7 \equiv 29 \pmod{36}$$

Hence the function $g(x) = x^{29}$ is the inverse of f mod 37.

For example,
$f(9) = 9^5 \equiv 9^{4+1} \equiv 12 * 9 \equiv 34 \pmod{37}$
$g(34) \equiv 34^{29} \equiv 34^{16+8+4+1} \equiv 9 \pmod{37}$

Note: We can use this Corollary for encryption. Namely we encrypt using *f* and decrypt using *g*.

Ex
Let $p = 2953$ (which is a prime). Define $f(x) = x^{55} \pmod{2953}$.

Note that $\gcd(55, \phi(2953)) = \gcd(55, 2952) = 1$, since $2952 = 2^3 * 3^2 * 41$.

$$2952 = 53 * 55 + 37$$
$$55 = 1 * 37 + 18$$
$$37 = 2 * 18 + 1$$
$$1 = 37 - 2 * 18 = 37 - 2 * (55 - 37) = 3 * 37 - 2 * 55 = 3 * (2952 - 53 * 55) - 2 * 55 = 3 * 2952 - 161 * 55$$

$$55^{-1} \equiv -161 \equiv 2791 \pmod{2952}$$

So the inverse function to *f* is $g(x) = x^{2791} \pmod{2952}$

Embed message in U(2953) two at a time, using the encoding 1-26 for letters of the alphabet.

Message: WHOAREYOU

WH = 2308, OA = 1501, RE = 1805, YO = 2515, U = 0021

$f(x) \equiv x^{55} \pmod{2953}$
$f(2308) \equiv 797 \pmod{2953}$
$f(1501) \equiv 1044 \pmod{2953}$
$f(1805) \equiv 978 \pmod{2953}$
$f(2515) \equiv 479 \pmod{2953}$
$f(21) \equiv 2681 \pmod{2953}$

So the coded message is 0797 1044 0978 0479 2681

Let's decode it using *g* to decode the message.
$g(x) \equiv x^{2791} \pmod{2953}$
$g(0797) \equiv 797^{2791} \equiv 2308 \pmod{2953} =$ **WH**
$g(1044) \equiv 1044^{2791} \equiv 1501 \pmod{2953} =$ **OA**
$g(0978) \equiv 978^{2791} \equiv 1805 \pmod{2953} =$ **RE**
$g(0479) \equiv 479^{2791} \equiv 2515 \pmod{2953} =$ **YO**
$g(2681) \equiv 2681^{2791} \equiv 21 \pmod{2953} =$ **U**

Chinese Remainder Theorem, version 2
Suppose $\gcd(m,n) = 1$. Define the function $f : Z_{mn} \to Z_m \times Z_n$ by $f(x) = (x,x)$. Then *f* is a 1-1 correspondence.

Pf:
First, *f* is well-defined. Suppose $x \equiv y \pmod{mn} \Rightarrow x \equiv y \pmod{m}$ and $x \equiv y \pmod{n}$ (because $mn \mid (x-y) \Rightarrow m \mid (m-n)$ and $n \mid (x-y)$

Hence $f(x) = (x,x) = (y,y) = f(y)$

Second, *f* is 1-1.

Suppose
$f(x) = f(y) \Rightarrow (x,x) = (y,y) \Rightarrow x \equiv y \pmod{m},\ x \equiv y \pmod{n}$
$\Rightarrow m \mid (x-y),\ n \mid (x-y) \Rightarrow mn \mid (x-y) \Rightarrow x \equiv y \pmod{mn}$

The next to last step is valid because $\gcd(m,n) = 1$

Finally, *f* is onto.
Let $(a,b) \in Z_m \times Z_n$. We need to find $x \in Z_{mn}$ such that $f(x) = (x,x) = (a,b)$. We must solve the system: $x \equiv a \pmod{m},\ x \equiv b \pmod{n}$. Since $\gcd(m,n) = 1$ the usual Chinese Remainder Theorem implies the existence of such a solution.

Ex

$Z_{15} \to Z_3 \times Z_5$

$0 \to (0,0),\ 1 \to (1,1),\ 2 \to (2,2),\ 3 \to (0,3),\ 4 \to (1,4)$

$5 \to (2,0),\ 6 \to (0,1), 7 \to (1,2),\ 8 \to (2,3),\ 9 \to (0,4)$

$10 \to (1,0), 11 \to (2,1),\ 12 \to (0,2),\ 13 \to (1,3),\ 14 \to (2,4)$

Corollary: Let $\gcd(m,n) = 1$ then $\phi(mn) = \phi(m)\phi(n)$

Pf:

From the previous theorem the function f is a 1-1 correspondence between Z_{mn} and $Z_m \times Z_n$. This implies a 1-1 correspondence between $U(mn)$ and $U(m) \times U(n)$

Suppose $x \in U(mn)$. Then there is a

$d \in U(mn)$, such that $xd \equiv 1 (\mathrm{mod}\, mn) \Rightarrow mn \mid (xd-1) \Rightarrow m \mid (xd-1)$ and $n \mid (xd-1)$

$\Rightarrow xd \equiv 1 (\mathrm{mod}\, m),\ xd \equiv 1 (\mathrm{mod}\, n) \Rightarrow (x,x) \in U(m) \times U(n)$ since (d,d) is the inverse

Hence

$\phi(mn) = \#U(mn) = \#(U(m) \times U(n)) = \#U(m) * \#U(n) = \phi(m) * \phi(n)$

Ex

(1) $\phi(26) = \phi(2)\phi(13) = 1 * 12 = 12$

Note, we can verify this by $U(26) = \{1,3,5,7,9,11,15,17,19,21,23,25\}$

(2) 4807 = 11*19*23. Hence $\phi(4807) = \phi(11*19*23) = \phi(11) * \phi(19) * \phi(23) = 10 * 18 * 22 = 3960$

(3) Note that this corollary is not true if $\gcd(m,n) \neq 1$

For example.

$\phi(18) = 6,\ U(18) = \{1,5,7,11,13,17\}$

$\phi(3) = 2,\ \phi(6) = 2 \Rightarrow \phi(18) \neq \phi(3) * \phi(6)$

Euler Product Formula

Suppose that $n = p_1^{k_1} p_2^{k_2} \cdots p_r^{k_r}$ is the prime factorization of *p*. Then we have

$$\phi(n) = (p_1^{k_1} - p_1^{k_1-1})(p_2^{k_2} - p_2^{k_2-1}) \cdots (p_r^{k_r} - p_r^{k_r-1}) = n\left(1 - \frac{1}{p_1}\right)\left(1 - \frac{1}{p_2}\right) \cdots \left(1 - \frac{1}{p_r}\right)$$

Pf

We first need to show for a single prime *p*, $\phi(p^k) = p^k - p^{k-1} = p^k\left(1 - \frac{1}{p}\right)$

Consider the ring Z_{p^k}. What are the units in this set? Precisely numbers that are not multiples of p. The multiples of p are $\{0, p, 2p, ..., (p^{k-1}-1)p\}$. There are p^{k-1} elements in this set (hence that many non-units).

So there are $p^k - p^{k-1} = p^k\left(1-\frac{1}{p}\right)$. Apply this repeatedly to

$$\phi(p_1^{k_1}p_2^{k_2}\cdots p_r^{k_r}) = \phi(p_1^{k_1})\phi(p_2^{k_2})\cdots\phi(p_r^{k_r}) = (p_1^{k_1}-p_1^{k_1-1})(p_2^{k_2}-p_2^{k_2-1})\cdots(p_r^{k_r}-p_r^{k_r-1})$$
$$= p_1^{k_1}\left(1-\frac{1}{p_1}\right)p_2^{k_2}\left(1-\frac{1}{p_2}\right)\cdots p_r^{k_r}\left(1-\frac{1}{p_r}\right) = n\left(1-\frac{1}{p_1}\right)\left(1-\frac{1}{p_2}\right)\cdots\left(1-\frac{1}{p_r}\right)$$

Ex

(1) $\phi(40)$

$$40 = 2^3 * 5 \Rightarrow \phi(40) = 40\left(1-\frac{1}{2}\right)\left(1-\frac{1}{5}\right) = 40 * \frac{1}{2} * \frac{4}{5} = 16$$

(2) $\phi(19602)$

$$19602 = 2 * 3^4 * 11^2 \quad \phi(19602) = 19602\left(1-\frac{1}{2}\right) * \left(1-\frac{1}{3}\right) * \left(1-\frac{1}{11}\right) = 19602 * \frac{1}{2} * \frac{2}{3} * \frac{10}{11} = 5940$$

Computing order of elements in Z_n^*

Use the fact that the order of an element divides $\phi(n)$.

Ex.

(1) Find the order of 98 in U(163)

First note that 163 is prime, hence $\phi(n) = 162 = 2 * 3^4$

The divisors of 162 = $\{1, 2, 3, 6, 9, 18, 27, 54, 81, 162\}$

$$98^2 \equiv 150 \pmod{163},\ 98^3 \equiv 30 \pmod{163},\ 98^6 \equiv 85 \pmod{163},\ 98^9 \equiv 105 \pmod{163}$$
$$98^{18} \equiv 104 \pmod{163},\ 98^{27} \equiv 162 \pmod{163},\ 98^{54} \equiv 1 \pmod{163}$$

Therefore the order of 98 in U(163) is 54.

(2) Find the order of 185 in U(391)

First note that $391 = 17 * 23,\ \phi(391) = \phi(17) * \phi(23) = 16 * 22 = 352 = 2^5 * 11$

The divisors of 352 = $\{1,2,4,8,11,16,22,32,44,88,176,352\}$

$185^2 \equiv 208 \pmod{391}$, $185^4 \equiv 254 \pmod{391}$, $185^8 \equiv 1 \pmod{391}$

Hence order of 185 in U(391) is 8.

Note: one can do this in Sage by the commands

```
divisors(352)
[185^i  %  391 for i in divisors(352)]
```

(3) Find all the elements of order 6 in U(209)

First note that $209 = 11 * 19$, $\phi(209) = \phi(11) * \phi(19) = 10 * 18 = 180$

One can do this in Sage

```
R = Integers(209)
L = [i for i in R if i^6 % 209 == 1]
```

This gives an answer [1,12,45,56,65,87,122,144,153,164,197,208]

But all we can say at the moment is that the order of these numbers divides 6. That means (except for 1) the order could be 2,3, or 6.We need to see which it is. We can use the commands

```
L2 = [i^2 % 209 for i in L]  (where L is defined above)
L3 = [i^3 % 209 for i in L]
```

The numbers in L which have order 6 have numbers different from 1 in both L2 and L3.

These are {12,65,87,122,164,197}