Section 6.3 - Euler's Theorem

Recall Fermat's Little Thm: If p is prime, and $a \not\equiv 0 \bmod p$, then $a^{p-1} \equiv 1 \bmod p$.

↳ answers the question: given a, to what power should I raise a to get $1 \bmod p$?

Fact (proved later, in Ch. 10): If p prime, $\exists\, a \not\equiv 0 \bmod p$, s.t. $a^x \not\equiv 1 \bmod p$ when $1 \leq x < p-1$

Interpretation: FLT gives best possible (general) exponent.

Q: How does FLT generalize to a composite modulus?

Goal: If $\underline{\text{(about } a)}$, then

$$a^{???} \equiv 1 \bmod m$$

Ex: $m = 9$, make a table of $a^x \bmod 9$ for $0 \le a \le 8$, and sufficient x

(mod 9)

x	1	2	3	4	5	6
0^x	0	0	0	0	0	0
1^x	1	1	1	1	1	1
2^x	2	4	8	7	5	1
3^x	3	0	0	0	0	0 .....
4^x	4	7	1	4	7	1
5^x	5	7	8	4	2	1
6^x	6	0	0	0	0	0 ....
7^x	7	4	1	7	4	1
8^x	8	1	8	1	8	1

Q1: For which a is it possible that $a^x \equiv 1 \bmod 9$ for some x?

A1: $\{1, 2, 4, 5, 7, 8\}$

$= \{n : 0 \le n \le 8,\ (n,9)=1\}$

Q2: For which x is $a^x \equiv 1 \mod 9$

when $(a,9)=1$?

A2: possibilities: $\{2,3,4,6\}$

universal

Generalize:

Lemma: If $m > 0$ and $\underline{b^x \equiv 1 \mod m}$ for some $x > 0$, then $(b,m)=1$

pf: Suppose p is prime, $p \mid m$

If $p \mid b$, then $p \mid b^x$

Also, $p \mid \underline{m \mid b^x - 1}$

So $p \mid b^x - (b^x - 1) = 1$ $\lightning$

So $p \nmid b$, hence $(b, m) = 1$

Euler Phi Function

Recall: $\mathbb{Z}/n\mathbb{Z} := \{0, 1, \dots, n-1\}$

times

Def. $\left(\mathbb{Z}/n\mathbb{Z}\right)^{\times} := \{x : 0 \le x \le n-1, (x,n) = 1\}$

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

$\left(\mathbb{Z}/5\mathbb{Z}\right)^{\times} = \{1, 2, 3, 4\}$

$\left(\mathbb{Z}/p\mathbb{Z}\right)^{\times} = \{1, 2, 3, \dots, p-1\}$

for prime p

Def: $\varphi(n) := \#\left(\mathbb{Z}/_{n}\mathbb{Z}\right)^{\times}$

$$= \left|\left(\mathbb{Z}/_{n}\mathbb{Z}\right)^{\times}\right|$$