Number Theory Section Summary: 7.1-7.3
Euler's Phi Function

1. Summary

Now we put Euler's phi function to work, generalizing Fermat's Little Theorem.

2. Theorems

Lemma: Let $n > 1$ and $\gcd(a, n) = 1$. If $a_1, a_2, \ldots, a_{\phi(n)}$ are the positive integers less than n and relatively prime to n, then $aa_1, aa_2, \ldots, aa_{\phi(n)}$ are congruent modulo n to $a_1, a_2, \ldots, a_{\phi(n)}$ in some order.

Theorem 7.5 (Euler): If $n \geq 1$ and $\gcd(a, n) = 1$, then $a^{\phi(n)} \equiv 1 \pmod{n}$.

Corollary: Fermat's Little theorem

when n is prime, e.g. $n = p$

$\varphi(p) = p - 1$

$a^{p-1} \equiv 1 \pmod{p}$

translates to $p \nmid a$

2nd proof, p 137

Lemma: if $p \nmid a$ (p prime), then

$$a^{\varphi(p^k)} \equiv 1 \pmod{p^k}$$

$(k > 0)$

Proof: By induction, using the binomial theorem (Look into that for next test)

To establish Euler's theorem:

Assume $n = p_1^{k_1} \cdots p_r^{k_r}$ is the prime factorization of n. For each prime p_i we can write $n = p_i^{k_i} \cdot m_i$, where $\gcd(p_i, m_i) = 1$

So $\varphi(n) = \varphi(p_i^{k_i}) \cdot \varphi(m_i)$. From the lemma we know that

$$a^{\varphi(p_i^{k_i})} \equiv 1 \pmod{p_i^{k_i}}.$$

$$\therefore \left(a^{\varphi(p_i^{k_i})}\right)^{\varphi(m_i)} = \boxed{a^{\varphi(n)} \equiv 1 \pmod{p_i^{k_i}}}$$

Since the p_i are relatively prime, we can conclude that

$$a^{\varphi(n)} \equiv 1 \pmod{p_1^{k_1} \cdots p_r^{k_r}}$$
$$\equiv 1 \pmod{n}$$

#9

$$2^{100000} \pmod{77}$$

$a = 2$

$n = 77 = 7 \cdot 11$ $\qquad \gcd(a, n) = 1$

$$a^{\varphi(77)} \equiv 1 \pmod{77}$$

$$\varphi(77) = \varphi(7 \cdot 11) = \varphi(7) \cdot \varphi(11)$$

$= 6 \cdot 10 = 60$

$a^{60} \equiv 1 \pmod{77}$

$2^{100^{100}} \equiv 2^{40} \pmod{77}$ .... $= 23 \pmod{77}$

now we play the same old game ....

#2 $51 \mid 10^{32n+9} - 7$

alternatively

$10^{32n+9} - 7 \equiv 0 \pmod{51}$

$\varphi(51) = \varphi(3) \cdot \varphi(17)$

$= 2 \cdot 16 = 32$, so

$(10^{32})^n \cdot 10^9 - 7 \equiv 1^n \cdot 10^9 - 7 \pmod{51}$

$\equiv 10^9 - 7 \pmod{51}$

$\equiv (10^2)^4 \cdot 10 - 7 \pmod{51}$

$\equiv (-2)^4 \cdot 10 - 7 \pmod{51}$ same ol', same ol'

$\vdots$

$\equiv 0 \pmod{51}$
