Unit 6: Polynomial Congruences and Primitive Roots

Paul Ycay
MATH 409

December 13, 2019

The following theorems are ones to be marked. There is a separate file of handwritten notes for the rest of the theorems in this chapter

Theorem 6.4. Suppose p is a prime and $ord_p(a) = d$. Then for each natural number i with $(i, d) = 1$, $ord_p(a^i) = d$.

Proof. Suppose p is prime and $ord_p(a) = d$. Suppose $e = ord_p(a^i)$. Then, $(a^i)^d = a^{id} = a^{di} = (a^d)^i \equiv 1^i \equiv 1 \ mod\ p$. Then, $e|d$, from 4.10: Let a and n be natural numbers with $(a, n) = 1$, let $k = ord_n(a)$, and let $m \in \mathbb{N}$. Then $a^m \equiv 1\ (mod\ n)$ if and only if $k|m$. Furthermore, $(i, d) = 1 \implies ix + dy = 1,\ x, y \in \mathbb{Z}$. Then, $a^e = a^{(ix+dy)}e = a^{ixe}a^{dye} = (((a^i)^e)^x)(a^d)^{ye} \equiv 1^x 1^{ye} \equiv 1\ (mod\ p)$. Then d must divide e, which leaves d and e to be equivalent to each other. $\square$

Theorem 6.5. For a prime p and natural number d, at most $\phi(d)$ incongruent integers *modulo* p have *order* d *modulo* p

Proof. By Fermat's Little Theorem, if $x^d \equiv 1\ (mod\ p)$, then $d|(p-1)$ $a \in \mathbb{Z}$, $ord_p(a) = d$. By 6.4, $ord_p(a^i) = d$ for each $1 \leq i \leq d$, with $(i, d) = 1$. There are exactly $\phi(d)$ integers. Some of these powers of a may not be distinct *mod* p, so there are at most $\phi(d)$ of them having *order* d $\square$

Exercise 6.10. Compute each of the following sums.
1. $\sum_{d|6}^{\infty} \phi(d)$

2. $\sum_{d|10} \phi(d)$

3. $\sum_{d|24} \phi(d)$

4. $\sum_{d|36} \phi(d)$

5. $\sum_{d|27} \phi(d)$

Solution. 1. $\phi(1) + \phi(2) + \phi(3) + \phi(6) = 1 + 1 + 2 + 2 = 6$

2. $\phi(1) + \phi(2) + \phi(5) + \phi(10) = 1 + 1 + 4 + 4 = 10$

3. $\phi(1)+\phi(2)+\phi(3)+\phi(4)+\phi(6)+\phi(8)+\phi(12)+\phi(24) = 1+1+2+2+2+4+4+8 = 24$

4. $\phi(1) + \phi(2) + \phi(3) + \phi(4) + \phi(6) + \phi(9) + \phi(12) + \phi(18) + \phi(36) = 1 + 1 + 2 + 2 + 2 + 6 + 4 + 6 + 12 = 36$

5. $\phi(1) + \phi(3) + \phi(9) + \phi(27) = 1 + 2 + 6 + 18 = 27$

□

Lemma 6.13. If p, q are two different primes, then

$\sum_{d|pq} \phi(d) = pq$

Proof. To compute above summation, only possible choices of $d := 1, p, q, pq$. Then, the number of integers prime to each choice of d would be $\phi(1) = 1,\ \phi(p) = p - 1,\ \phi(q) = q - 1,\ \phi(pq) = (p-1)(q-1)$. Upon summation, we then have $1 + p - 1 + q - 1 + pq - p - q + 1 = 1 - 1 - 1 + 1 + p + q - p - q + pq = pq$, as was to be shown. □

Theorem 6.38. If n is a natural number that is a product of distinct primes, and k is a natural number such that $(k, \phi(n)) = 1$, then $x^k \equiv b\ (mod\ n)$ has a unique solution *modulo* n for any integer b. Moreover, that solution is given by $x \equiv b^u\ (mod\ n)$ where $u, v \in \mathbb{Z}^+$ such that $ku - \phi(n)v = 1$.

Proof. Since $(k, \phi(n)) = 1, \exists u, v \in \mathbb{Z}$ such that $ku - \phi(n)v = 1$, i.e., $ku \equiv 1\ (mod\ \phi(n)$.
Suppose $(b, n) = 1$, then $b^{ku} = b^{1+v\phi(n)} = b * (b^{\phi(n)})^v \equiv b\ (mod\ n)$. Since $b^{\phi(n)} \equiv 1\ (mod\ n)$, we have $(b^{\phi(n)})^v \equiv 1\ (mod\ n)$. Thus, we have 1 $(b^u)^k \equiv b\ (mod\ n)$.
Fix $x \equiv b^u\ (mod\ n)$, then $x^k \equiv b^{uk}\ (mod\ n) \equiv b\ (mod\ n)$, from 1.
Hence, $x \equiv b^u\ (mod\ n)$ is a solution of $x^k \equiv b\ (mod\ n)$, where $b \in \mathbb{Z}, (b, n) = 1$. □

Exercise 6.39. Find the $37th$ root of 100 *modulo* 210.

Solution. $x^{37} \equiv 100\ (mod\ 210)$,
$k = 37, \phi(210) = 210(1 - 1/2)(1 - 1/5)(1 - 1/7)(1 - 1/3) = 48$
Thus, find $u, v \in \mathbb{Z}$ such that $37u = 48v + 1$

$48 = 37 * 1 + 1$
$37 = 11 * 3 + 4$
$11 = 4 * 2 + 3$
$4 = 3 * 1 + 1$
$1 = 4 - (11 - 4 * 2) * 1$
$1 = 4 * 3 - 11 * 1$
$1 = (37 - 11 * 3) * 3 - 11 * 1$
$1 = 37 * 3 - 11 * 10$
$1 = 37 * 3 - (48 - 37 * 1) * 10$
$1 = 37 * 13 - 48 * 10$
Therefore, $u = 13, v = 10$
Then, $x \equiv 100^{13}\ (mod\ 210)$. Thus, $x = 100$, after reducing the congruence using an online calculator. $\square$