Primitive Roots Proofs

Karim El Shenawy

February 2021

Introduction

This course notebook is the collection of theorem proofs, exercises and answers from Unit 6 of the Number Theory Through Inquiry (Mathematical Association of America Textbooks).

Theorems to Mark

6.4 Theorem

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 a prime, $ord_p(a) = d$ and that $ord_p(a^i) = k$ for each natural number i. Then, by definition, $(a^i)^k \equiv 1 \pmod{p}$. This also implies that

$$\begin{aligned}(a^i)^k &\equiv 1 \pmod{p}\\ a^{ik} &\equiv 1 \pmod{p}\end{aligned}$$

Hence, $ord_p(a) = ik$ which is given as $ord_p(a) = d$. By Theorem 4.10, this implies that $d \mid ik$.
Now, suppose that $(i, d) = 1$. Then this implies that $d \nmid i$, thus $d \mid ik \implies d \mid k$. Moreover, since $ord_p(a) = d$ we know that $a^d \equiv 1 \pmod{p}$, which is also,

$$\begin{aligned}a^d &\equiv 1 \pmod{p}\\ (a^d)^i &\equiv 1 \pmod{p}\\ a^{di} &\equiv 1 \pmod{p}\end{aligned}$$

Then by Theorem 4.10, $k \mid d$. Therefore since $k \mid d$ and $d \mid k$, then $k = d$ which also implies that $ord_p(a^i) = ord_p(a)$. □

6.12 Lemma

If p is a prime, then

$$\textstyle\sum_{d|p^k} \phi(d) = p^k$$

Proof. Given prime p, then the only possible d values where $d \mid p$ are 1 and p. Thus, by direct proof,

$$\textstyle\sum_{d|p^k} \phi(d) = \phi(1) + \phi(p) + \phi(p^2) + ... + \phi(p^k)$$
$$= 1 + (p-1) + (p^2 - p) + (p^3 - p^2) + ... + (p^{k-1} - p^{k-2}) + (p^k - p^{k-1})$$
$$= p^k$$

□

6.15 Theorem

If n is a natural number, then

$$\textstyle\sum_{d|n} \phi(d) = n$$

Proof. Let n be a natural number. By the fundamental theorem of arithmetic, we know that any natural n can be expressed in terms of primes, thus $n = p_1^{r_1} \cdot p_2^{r_2} \cdot ... \cdot p_m^{r_m}, p_i \neq p_i$ for $i \neq j$ and where r and m are integers. Now suppose that $\sum_{d|n} \phi(d) = n$, then by direct proof,

$$\sum_{d|n} \phi(d) = (\sum_{d_1|p_1^{r_1}} \phi(d_1)) \cdot (\sum_{d_2|p_2^{r_2}} \phi(d_2)) \cdot ... \cdot (\sum_{d_r|p_m^{r_m}} \phi(d_m))$$

$$\sum_{d|n} \phi(d) = p_1^{r_1} \cdot p_2^{r_2} \cdot ... \cdot p_m^{r_m} \qquad \textbf{By Lemma 6.12}$$

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

Thus, since $n = p_1^{r_1} \cdot p_2^{r_2} \cdot ... \cdot p_m^{r_m}$, $\sum_{d|n} \phi(d) = n$ holds. □

6.21 Theorem

If n is a natural number, k is an integer, and m is an integer relatively prime to n, then the set of n integers

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

is a complete residue system modulo n.

Proof. Assume n is a natural number, k is an integer, and m is an integer relatively prime to n. Also, suppose there exist a set A = $\{k, k+m, k+2m, k+$

$3m, ..., k + (n-1)m\}$. Suppose that $a \in A$ and thus $a \equiv k \pmod{m}$, then

$$\begin{aligned} &\implies a \equiv k \pmod{m} \\ &\implies a - k \equiv 0 \pmod{m} \\ &\implies m \mid a - k \\ &\implies mx = a - k \\ &\textbf{By division algorithm, } \exists x \in \mathbf{Z}, 1 \leq x \leq n-1 \\ &\implies a = k + mx \\ &\implies a = k, k+m, k+2m, k+3m, ..., k+(n-1)m \end{aligned}$$

Thus, the set A is a complete residue system modulo n. □

6.32 Theorem

If k and n are natural numbers with $(k, \phi(n)) = 1$, then there exist positive integers u and v satisfying $ku = \phi(n)v + 1$.

Proof. Suppose k and n are natural numbers with $(k, \phi(n)) = 1$. Also suppose by Theorem 1.39, then $(k, \phi(n)) = 1$ can be expressed as $ku + ks = 1, \exists u, s \in \mathbf{Z}$. Therefore, there exist positive integers u and v satisfying $ku = \phi(n)(-s) + 1$ where $s = -v$. □

6.37 Theorem

If a is an integer, v is a natural number, and n is a product of distinct primes, then $a^{v\phi(n)+1} \equiv a \pmod{n}$.

Proof. Suppose $a \in \mathbf{Z}$, $v \in \mathbf{N}$ and n is the product of distinct primes. By Euler's Theorem we know that $a^{\phi(n)} \equiv 1 \pmod{n}$. Then we'll encounter 2 possible cases which we can prove by direct proof,

- Case 1: if $(a, n) = 1$ with $a \neq n$, then

$$\begin{aligned} a^{\phi(n)} &\equiv 1 \pmod{n} \\ a^{v\phi(n)+1} &\equiv a^{v\phi(n)+1} \pmod{n} \\ &\equiv 1^v a \pmod{n} \\ &\equiv a \pmod{n} \end{aligned}$$

- Case 2: if $(a, n) \neq 1$, then

$$\begin{aligned} a &\equiv 0 \pmod{n} \\ a^{\phi(n)} &\equiv 0 \pmod{n} \\ a^{v\phi(n)+1} &\equiv 0 \times a \pmod{n} \\ &\equiv a \equiv 0 \pmod{n} \end{aligned}$$

□

Practice Theorems from Polynomial Congruences and Primitive Roots

6.1 Theorem

Let $a_n x^n + a_{n-1} x^{n-1} + ... + a_0$ *be a polynomial of degree* $n > 0$ *with integer coefficients and assume* $a_n \neq 0$*. Then an integer r is a root of f(x) if and only if there exists a polynomial g(x) of degree n-1 with integer coefficients such that* $f(x) = (x - r)g(x)$*.*

Proof. Let $f(x) = a_n x^n + a_{n-1} x^{n-1} + ... + a_0$ be a polynomial of degree $n > 0$ with integer coefficients and assume $a_n \neq 0$. Suppose that the root of $f(x)$ is the integer r, then by definition $f(r) = 0$.
Now, suppose we divide f(x) by (x-r), then by the remainder theorem we will get f(r) as the remainder. But since f(r) = 0, then the remainder is also 0. Therefore, f(x) is divisible by (x-r) thus $f(x) \mid (x - r)$ if $f(r) = 0$. Since, by definition, $f(x) \mid (x - r) \implies f(x) = (x - r)g(x)$ for some polynomial g(x). This also implies that g(x) is of degree n-1 since f(x) is of degree n and (x-r) is of degree 1. Thus, there must exist a polynomial g(x) of degree n-1 with integer coefficients such that $f(x) = (x-r)g(x)$ when the integer r is a root of f(x).

Conversely, suppose g(x) exists as a polynomial of degree n-1 with integer coefficients such that $f(x) = (x - r)g(x)$, where r is an integer. By definition, x can be the root off(x) if and only if f(x) = 0, thus;

$$\begin{aligned} f(x) &= (x - r)g(x) \\ f(r) &= (r - r)g(x) \\ f(r) &= 0 \times g(x) \\ f(r) &= 0 \end{aligned}$$

Hence, r must be the root of f(x). □

6.2 Theorem

Let $a_n x^n + a_{n-1} x^{n-1} + ... + a_0$ *be a polynomial of degree* $n > 0$ *with integer coefficients and assume* $a_n \neq 0$*. Let p be a prime number and r an integer. Then, if* $f(r) \equiv 0 \pmod{p}$*, there exists a polynomial g(x) of degree n-1 such that*

$$(x - r)g(x) = a_n x^n + a_{n-1} x^{n-1} + ... + a_1 x + b_0$$

where $a_0 \equiv b_0 \pmod{p}$*.*

Proof. Let $f(x) = a_nx^n + a_{n-1}x^{n-1} + ... + a_0$ be a polynomial of degree $n > 0$ with integer coefficients and assume $a_n \neq 0$. Also let p be a prime and r an integer. If we divide f(x) by (x-r) then there must be a polynomial g(x) of degree n-1 since f(x) is of degree n and (x-r) is of degree 1, such that f(x) = (x-r)g(x) + f(r), by the remainder theorem. Also, since (x-r) is of degree 1, then f(r) must be a constant say R, f(x) = (x-r)g(x) + R.
We know that two polynomial are said to be equal if they have the same degree and have the same coefficients of respective terms. Clearly all the coefficients of f(x) and (x-r)g(x) are same except of the constant term. Therefore,

$$(x - r)g(x) = a_nx^n + a_{n-1}x^{n-1} + ... + a_1x + b_0$$

Then from f(x) = (x-r)g(x) + R, we have,

$$\begin{gathered} a_0 = b_0 + R \\ \Longrightarrow a_0 = b_0 + R \equiv b_0 \pmod{p} \\ \Longrightarrow f(r) = R \equiv 0 \pmod{p} \\ \Longrightarrow b_0 + A \equiv b_0 \pmod{p} \end{gathered}$$

Therefore,

$$(x - r)g(x) = a_nx^n + a_{n-1}x^{n-1} + ... + a_1x + b_0$$

where $a_0 \equiv b_0 \pmod{p}$. □

6.3 Theorem (Lagrange's Theorem)

If p is a prime and $f(x) = a_nx^n + a_{n-1}x^{n-1} + ... + a_0$ is a polynomial with integer coefficients and $a_n \neq 0$, then $f(x) \equiv 0 \pmod{p}$ has at most n non-congruent solutions modulo p.

Proof. Suppose p is a prime and $f(x) = a_nx^n+a_{n-1}x^{n-1}+...+a_0$ is a polynomial with integer coefficients and $a_n \neq 0$. □

6.4 Theorem

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 a prime, $ord_p(a) = d$ and that $ord_p(a^i) = k$ for each natural number i. Then, by definition, $(a^i)^k \equiv 1 \pmod{p}$. This also implies that

$$\begin{aligned} (a^i)^k &\equiv 1 \pmod{p} \\ a^{ik} &\equiv 1 \pmod{p} \end{aligned}$$

Hence, $ord_p(a) = ik$ which is given as $ord_p(a) = d$. By Theorem 4.10, this implies that $d \mid ik$.

Now, suppose that $(i, d) = 1$. Then this implies that $d \nmid i$, thus $d \mid ik \implies d \mid k$. Moreover, since $ord_p(a) = d$ we know that $a^d \equiv 1 \pmod p$, which is also,

$$\begin{aligned} a^d &\equiv 1 \pmod p \\ (a^d)^i &\equiv 1 \pmod p \\ a^{di} &\equiv 1 \pmod p \end{aligned}$$

Then by Theorem 4.10, $k \mid d$. Therefore since $k \mid d$ and $d \mid k$, then $k = d$ which also implies that $ord_p(a^i) = ord_p(a)$. □

6.5 Theorem

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

Proof. Suppose a prime p and a natural number d. By Theorem 6.4, we know that for each natural number i with $(i, d) = 1, ord_p(a^i) = d$ with $ord_p(a) = d$. Since, $(i, d) = 1$, i can only be in the range of $1 \leq i \leq d$. Moreover, by Fermat's Little Theorem, if $x^d \equiv 1 \pmod p$, then $ord_p(a) = d$. Thus there are exactly $\phi(d)$ a integers. Not all the powers of a will be distinct modulo p but there is at most $\phi(d)$. □

6.6 Theorem

Let p be a prime and suppose g is a primitive root modulo p. Then the set $\{0, g, g^2, g^3, ..., g^{p-1}\}$ forms a complete residue system modulo p.

Proof. Suppose a prime b and primitive root modulo p is g, thus $g^{p-1} \equiv 1$ (mod p). Given the set $G = \{0, g, g^2, g^3, ..., g^{p-1}\}$. the set is a complete residue system, if every integer belongs to an element from the set.
By Theorem 4.4, we can deduce that there exist natural numbers i and j , with $i \neq j$, such that $g^i \equiv g^j \pmod p$. This implies that all elements in G are all distinct. Now let a be an integer where by the division algorithm, $a = np + r$ where $n, r \in \mathbf{Z}$ with $0 \leq r < p$. Then, $g^a \equiv g^{np+r} \equiv g^{np} g^r \equiv g^r \pmod p$. Thus each integer does belong to an element of the set which then implies that the set $\{0, g, g^2, g^3, ..., g^{p-1}\}$ forms a complete residue system modulo p. □

6.7 Exercise

For each of the primes p less than 20 find a primitive root and make a chart showing what powers of the primitive root give each of the natural numbers less than p.

Prime p	**2**	**3**	**5**	**7**	**11**	**13**	**17**	**19**
Primitive Roots a	1	2	2	3	2	2	3	2
a^1	1	2	2	3	2	2	3	2
a^2	1	1	4	2	4	4	9	4
a^3		2	3	6	8	8	10	8
a^4			1	4	5	3	13	16
a^5				5	10	6	5	13
a^6				1	9	12	15	17
a^7					7	11	11	14
a^8					3	9	16	9
a^9					6	5	14	18
a^{10}					1	10	8	17
a^{11}						7	7	15
a^{12}						1	4	11
a^{13}							12	3
a^{14}							2	6
a^{15}							6	12
a^{16}							1	5
a^{17}								10
a^{18}								1

6.8 Theorem

Every prime p has a primitive root.

Proof. Given a prime p. There are p-1 positive integers, $1, 2, ..., p-1$ where each of them is less than p. Also let x be a positive integer where $p-1 = xk, \exists k \in \mathbf{Z}$. Each of these will have some multiplicative order modulo p. So if we count all those of order 1, and all of those of order 2, etc. Then the total count will of course be p-1. Now, suppose that the function f(x) results to the total number of integers of order x, for example f(1) of order 1. Then,

$$p - 1 = \sum_{x=1}^{\infty} f(x)$$

However, there will be orders that divide p-1. Thus, most terms in the sum above will be zero and only those with $x \mid p-1$ will contribute to the sum. Therefore,

$$p - 1 = \sum_{x|p-1}^{\infty} f(x)$$

This then implies that every prime will have a primitive root since $x \mid p-1$ holds for all integer values of x. □

6.9 Exercise

Consider the prime p = 13. For each divisor d = 1,2,3,4,6,12 of 12 = p-1, mark which of the natural numbers in the set $\{1, 2, 3, 4, 5, 6, 7, 8, 9, 10, 11, 12\}$ *have order d.*

- d = 1, then only 1.
  - $1^1 \equiv 1 \pmod{13}$
- d = 2, then only 12.
  - $12^2 \equiv 1 \pmod{13}$
- d = 3, then 3 and 9 only.
  - $3^3 \equiv 1 \pmod{13}$
  - $9^3 \equiv 1 \pmod{13}$
- d = 4, then 5 and 8 only.
  - $5^4 \equiv 1 \pmod{13}$
  - $8^4 \equiv 1 \pmod{13}$
- d = 6, then 4, 10, 11 and 12.
  - $4^6 \equiv 1 \pmod{13}$
  - $10^6 \equiv 1 \pmod{13}$
  - $11^6 \equiv 1 \pmod{13}$
  - $12^6 \equiv 1 \pmod{13}$

6.10 Exercise

Compute each of the following sums.

1. $\sum_{d|6}^{\infty} \phi(d)$

$$\begin{aligned} &\implies \phi(1) + \phi(2) + \phi(3) + \phi(6) \\ &\implies 1 + 1 + 2 + 2 \\ &\implies 6 \end{aligned}$$

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

$$\begin{aligned} &\implies \phi(1) + \phi(2) + \phi(5) + \phi(10) \\ &\implies 1 + 1 + 4 + 4 \\ &\implies 10 \end{aligned}$$

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

$$\begin{aligned} &\Longrightarrow \phi(1)+\phi(2)+\phi(3)+\phi(4)+\phi(6)+\phi(8)+\phi(12)+\phi(24) \\ &\Longrightarrow 1+1+2+2+2+4+4+8 \\ &\Longrightarrow 24 \end{aligned}$$

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

$$\begin{aligned} &\Longrightarrow \phi(1)+\phi(2)+\phi(3)+\phi(4)+\phi(6)+\phi(9)+\phi(12)+\phi(18)+\phi(36) \\ &\Longrightarrow 1+1+2+2+2+6+4+6+12 \\ &\Longrightarrow 36 \end{aligned}$$

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

$$\begin{aligned} &\Longrightarrow \phi(1)+\phi(3)+\phi(9)+\phi(27) \\ &\Longrightarrow 1+2+6+18 \\ &\Longrightarrow 27 \end{aligned}$$

Conjecture. *For a natural number n,*

$$\textstyle\sum_{d|n} \phi(d) = n$$

Proof. We can proof this by Lemma 6.12 and by the Fundamental Theorem of Arithmetic. □

6.11 Lemma

If p is a prime, then

$$\textstyle\sum_{d|p} \phi(d) = p$$

Proof. Given prime p, then the only possible d values where $d \mid p$ are 1 and p. Thus, by direct proof,

$$\textstyle\sum_{d|p} \phi(d) = \phi(1) + \phi(p) = 1 + p - 1 = p$$

□

6.12 Lemma

If p is a prime, then

$$\textstyle\sum_{d|p^k} \phi(d) = p^k$$

Proof. Given prime p, then the only possible d values where $d \mid p$ are 1 and p. Thus, by direct proof,

$$\begin{gathered} \textstyle\sum_{d|p^k} \phi(d) = \phi(1) + \phi(p) + \phi(p^2) + ... + \phi(p^k) \\ = 1 + (p-1) + (p^2 - p) + (p^3 - p^2) + ... + (p^{k-1} - p^{k-2}) + (p^k - p^{k-1}) \\ = p^k \end{gathered}$$

□

6.13 Lemma

If p and q are two different primes, then

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

Proof. Given distinct primes p and q, then the only possible d values where $d \mid pq$ are 1, p, q and pq. Thus, by direct proof,

$$\begin{gathered}\sum_{d|p} \phi(d) = \phi(1) + \phi(p) + \phi(q) + \phi(pq) \\ = 1 + (p-1) + (q-1) + (p-1)(q-1) \\ = p + q - 1 + pq - p - q + q \\ = pq\end{gathered}$$

□

6.14 Lemma

If n and m are are relatively prime natural numbers, then

$$(\sum_{d|m} \phi(d)) \cdot (\sum_{d|n} \phi(d)) = (\sum_{d|nm} \phi(d))$$

Proof. Considering relatively prime natural numbers n and m. Suppose

$$(\sum_{d|nm} \phi(d)).$$

By Theorem 1.3, we can express $d \mid nm$ as $d \mid n$ and $d \mid m$, thus the new sum can be,

$$\begin{gathered}(\sum_{d|nm} \phi(d)) \\ \Longrightarrow (\sum_{d_1|n \text{ and } d_2|m} \phi(d_1 d_2)) \\ \Longrightarrow (\sum_{d_1|n \text{ and } d_2|m} \phi(d_1)\phi(d_2)) \\ \Longrightarrow (\sum_{d_1|n \text{ and } d_2|m} \phi(d_1)\phi(d_2)) \\ \Longrightarrow (\sum_{d|m} \phi(d)) \cdot (\sum_{d|n} \phi(d))\end{gathered}$$

□

6.15 Theorem

If n is a natural number, then

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

Proof. Let n be a natural number. By the fundamental theorem of arithmetic, we know that any natural n can be expressed in terms of primes, thus $n =$

$p_1^{r_1} \cdot p_2^{r_2} \cdot ... \cdot p_m^{r_m}, p_i \neq p_i$ for $i \neq j$ and where r and m are integers. Now suppose that $\sum_{d|n} \phi(d) = n$, then by direct proof,

$$\sum_{d|n} \phi(d) = (\sum_{d_1|p_1^{r_1}} \phi(d_1)) \cdot (\sum_{d_2|p_2^{r_2}} \phi(d_2)) \cdot ... \cdot (\sum_{d_r|p_m^{rm}} \phi(d_m))$$

$$\sum_{d|n} \phi(d) = p_1^{r_1} \cdot p_2^{r_2} \cdot ... \cdot p_m^{r_m} \qquad \textbf{By Lemma 6.12}$$

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

Thus, since $n = p_1^{r_1} \cdot p_2^{r_2} \cdot ... \cdot p_m^{r_m}$, $\sum_{d|n} \phi(d) = n$ holds. □

6.16 Exercise

For a natural number n consider the fractions

$$\tfrac{1}{n}, \tfrac{2}{n}, \tfrac{3}{n}, ..., \tfrac{n}{n},$$

all written in reduced form. For example, with n = 10 we would have

$$\tfrac{1}{10}, \tfrac{1}{5}, \tfrac{3}{10}, \tfrac{2}{5}, \tfrac{1}{5}, \tfrac{3}{5}, \tfrac{7}{10}, \tfrac{4}{5}, \tfrac{9}{10}, 1$$

Try to find a natural one-to-one correspondence between the reduced fractions and the numbers ϕd for $d \mid n$. Show how that observation provides a very clever proof to the preceding theorem.

We can attempt to express them as the form of pairs,

$$(1, 10), (1, 5), (3, 10), (2, 5), (1, 5), (3, 5), (7, 10), (4, 5), (9, 10), (1, 1)$$

This represents a one-to-one correspondence between the reduced fractions and the numbers ϕd for $d \mid n$. Thus the preceding theorem can be proved by

$$(1, p_1^{r_1}), (2, p_1^{r_1}), ..., (m, p_m^{r_m}).$$

6.17 Theorem

Every prime p has $\phi(p-1)$ primitive roots.

Proof. Suppose a prime p, we know by Theorem 6.8 that p has a primitive root. Now let the residues of p be $1, 2, 3, .., p-1$ which will have order equal to some divisor d of p-1 modulo p. Now let f(d) be the number of residues that have order d modulo p. Then,

$$\textstyle\sum_{d|p-1} f(d) = p - 1$$

Suppose that for each d of p-1, we have,

$$f(d) \leq \phi(d).$$

By Theorem 6.15, we can then obtain,

$$\begin{gathered}\sum_{d|p-1} f(d) \leq \sum_{d|p-1} \phi(d) \\ p-1 \leq p-1\end{gathered}$$

Thus, by the central equality every prime p has $\phi(p-1)$ primitive roots must hold. □

6.18 Exercise

Make a conjecture about the value $\phi(p)$ for a prime p.

Conjecture. *For a prime p, $\phi(p) = p - 1$.*

Proof. By definition, Euler's function counts the number of integers less than p that are relatively prime to p. Since, p is prime then all numbers under p are relatively prime to p thus $\phi(p) = p - 1$. □

6.19 Exercise

Make a conjecture about the value $\phi(p^k)$ for a prime p and natural number k.

Conjecture. *For a prime p, $\phi(p^k) = p^k - p^{k-1}$.*

6.20 Theorem

If n is a natural number and A is a complete residue system modulo n, then the number of numbers in A that are relatively prime to n is equal to $\phi(n)$.

Proof. Let n be a natural number and A is a complete residue system modulo n. This implies that there exists numbers in A that are relatively prime to n such that $\{a \in A|(n,a) = 1, 1 \leq a \leq n\}$. By definition of Euler's function, $\phi(n)$ is equal to the number of natural numbers less than or equal to n that are relatively prime to n, thus proven. □

6.21 Theorem

If n is a natural number, k is an integer, and m is an integer relatively prime to n, then the set of n integers

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

is a complete residue system modulo n.

Proof. Assume n is a natural number, k is an integer, and m is an integer relatively prime to n. Also, suppose there exist a set A = $\{k, k+m, k+2m, k+$

$3m, ..., k + (n-1)m\}$. Suppose that $a \in A$ and thus $a \equiv k \pmod{m}$, then

$$\begin{aligned}
&\implies a \equiv k \pmod{m} \\
&\implies a - k \equiv 0 \pmod{m} \\
&\implies m \mid a - k \\
&\implies mx = a - k \\
&\textbf{By division algorithm, } \exists x \in \mathbf{Z}, 1 \leq x \leq n-1 \\
&\implies a = k + mx \\
&\implies a = k, k+m, k+2m, k+3m, ..., k+(n-1)m
\end{aligned}$$

Thus, the set A is a complete residue system modulo n. □

6.22 Exercise

Consider the relatively prime natural numbers 9 and 4. Write down all the natural numbers less than or equal to $36 = 9 \cdot 4$ *in a rectangular array that is 9 wide and 4 high. Then circle those numbers in that array that are relatively prime to 36. Try some other examples using relatively prime natural numbers.*

1	2	3	4	⑤	6	⑦	8	9
10	⑪	12	⑬	14	15	16	⑰	18
⑲	21	22	㉓	24	㉕	26	27	28
㉙	30	㉛	32	34	㉟	36		

6.23 Theorem

If n and m relatively prime natural numbers, then

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

Proof. Given relatively prime natural numbers n and m. We know from Conjecture 6.19 that, Incomplete, no clue. □

6.24 Exercise

Compute each of the following

1. $\phi(3) = 2$
2. $\phi(5) = 4$
3. $\phi(15) = \phi(3)\phi(5) = 8$
4. $\phi(45) = \phi(5)\phi(9) = 32$
5. $\phi(98) = \phi(2)\phi(49) = 48$
6. $\phi(5^6 11^4 17^{10}) = \phi(5^6)\phi(11^4)\phi(17^{10}) = (5^6 - 5^5)(11^4 - 11^3)(17^{10} - 17^9)$

6.25 Question

To what power would you raise 15 to be certain that you would get an answer that is congruent to 1 modulo 98? Why?

$15^{\phi(98)}$ and by Euler's Theorem.

6.26 Question

How many primitive root does the prime 251 have?

$\phi(251) = 250$.

6.27 Exercise

Try, using paper and pencil, to solve several congruences of the form $x^k \equiv b \pmod 5$ *and* $x^k \equiv b \pmod 6$.

$$\begin{aligned} x^2 &\equiv \{2,3\} \pmod 5 & x &= nosolution \\ x^3 &\equiv \{2,3\} \pmod 5 & x &= \{3\} \\ x^4 &\equiv \{2,3\} \pmod 5 & x &= nosolution \end{aligned}$$

$$\begin{aligned} x^2 &\equiv \{2,5\} \pmod 6 & x &= nosolution \\ x^3 &\equiv \{2,3\} \pmod 6 & x &= \{1,2,3,4,5\} \end{aligned}$$

6.28 Exercise

Compute $a^9 \pmod 5$ *for several choices of a. Can you explain what happens? Now compute* $a^{17} \pmod{15}$ *for several choices of a. Does your previous explanation apply here too?*

$$\begin{aligned} 2^9 &\equiv 512 \equiv 2 \pmod 5 \\ 3^9 &\equiv 19683 \equiv 3 \pmod 5 \\ 4^9 &\equiv 262144 \equiv 4 \pmod 5 \\ 5^9 &\equiv 1953125 \equiv 0 \pmod 5 \end{aligned}$$

We notice that we can compute modulo to that last digit. Also another observation is that a and modulo result matched up until 5. Therefore, my explanation is that the result of the modulo is the same as the value for a up until the modulo value.

$$
\begin{aligned}
2^{17} &\equiv 131072 \equiv 2 \pmod{15}\\
3^{17} &\equiv 129140163 \equiv 3 \pmod{15}\\
4^{17} &\equiv 17179869184 \equiv 4 \pmod{15}\\
5^{17} &\equiv 762939453125 \equiv 5 \pmod{15}\\
6^{17} &\equiv 16926659444736 \equiv 6 \pmod{15}\\
15^{17} &\equiv 98526125335693359375 \equiv 0 \pmod{15}
\end{aligned}
$$

Yes my explanation holds until the value of modulo which is 15.

6.29 Theorem

If a is an integer and v and n are natural numbers such that $(a, n) = 1$, then $a^{v\phi(n)+1} \equiv a \pmod{n}$.

Proof. Suppose a is an integer and v and n are natural numbers such that $(a, n) = 1$. Thus with Fermat's Little Theorem and by direct proof, we have

$$
\begin{aligned}
a^{\phi(n)} &\equiv 1 \pmod{n}\\
a^{\phi(n)v} &\equiv 1^v \pmod{n}\\
a^{\phi(n)v} \cdot a &\equiv 1^v \cdot a \pmod{n}\\
a^{\phi(n)v+1} &\equiv a^v \pmod{n}
\end{aligned}
$$

□

6.30 Question

Consider the congruence $x^5 \equiv 2 \pmod{7}$. Can you think of an appropriate operation we can apply to both sides of the congruence that would allow us to "solve" for x? If so, is the value obtained for x a solution to the original congruence?

$$
\begin{aligned}
x^5 &\equiv 2 \pmod{7}\\
x^{5\phi(7)} &\equiv 2^{\phi(7)} \pmod{7}\\
x^{5\phi(7)}x &\equiv 2^{\phi(7)}x \pmod{7}\\
x^{5\phi(7)+1} &\equiv 64x \pmod{7}\\
x^{31} &\equiv x \pmod{7}
\end{aligned}
$$

By trial and error, we conclude that x = 4.

6.31 Question

Consider the congruence $x^3 \equiv 7 \pmod{10}$. Can you think of an appropriate operation we can apply to both sides of the congruence that would allow us to "solve" for x? If so, is the value obtained for x a solution to the original congruence?

$$\begin{aligned} x^3 &\equiv 7 \pmod{10} \\ x^{3\phi(10)} &\equiv 7^{\phi(10)} \pmod{10} \\ x^{3\phi(10)}x &\equiv 7^{\phi(10)}x \pmod{10} \\ x^{3\phi(10)+1} &\equiv x \pmod{7} \\ x^{13} &\equiv x \pmod{7} \end{aligned}$$

By trial and error, we conclude that x = 3.

6.32 Theorem

If k and n are natural numbers with $(k, \phi(n)) = 1$, then there exist positive integers u and v satisfying $ku = \phi(n)v + 1$.

Proof. Suppose k and n are natural numbers with $(k, \phi(n)) = 1$. Also suppose by Theorem 1.39, then $(k, \phi(n)) = 1$ can be expressed as $ku + ks = 1, \exists u, s \in \mathbf{Z}$. Therefore, there exist positive integers u and v satisfying $ku = \phi(n)(-s) + 1$ where $s = -v$. □

6.33 Exercise

Use your observations so far to find solutions to the following congruences. Be sure to check that your answers are indeed solutions.

1. $x^7 \equiv 4 \pmod{11}$

   - $\phi(11) = 10$
   - $7u - 10v = 1, u = 3, v = 2$
   - $x \equiv b^3 \pmod{11}$

$$x \equiv 4^3 \equiv 9 \pmod{11}$$

2. $x^5 \equiv 11 \pmod{18}$

   - $\phi(18) = 6$
   - $5u - 6v = 1, u = -1, v = -1$
   - $x \equiv b^{-1} \pmod{11}$

$$x \equiv 11^{-1} \equiv 5 \pmod{11}$$

3. $x^7 \equiv 2 \pmod 8$
    - $\phi(8) = 4$
    - $7u - 4v = 1, u = -1, v = -2$
    - $x \equiv b^{-1} \pmod 8$

$$x \equiv 2^{-1} \equiv 0 \pmod 8$$

6.34 Question

What hypotheses on k,b and n do you think are necessary for your method to produce a solution to the congruence $x^k \equiv b \pmod n$? Make a conjecture and prove it.

Conjecture. *Let k,b and n be natural numbers. (b, n) must be 1 to find a solution for $x^k \equiv b \pmod b$*

Proof. By definition of modulo, given natural numbers a and n. If $(a, n) \neq 1$, then $a \equiv 0 \pmod b$. Thus by Theorem 6.32, there will be no solution. □

6.35 Theorem

If b is an integer and k and n are natural numbers such that $(k, \phi(n)) = 1$ and $(b, n) = 1$, then $x^k \equiv b \pmod n$ has a unique solution modulo n. Moreover, that solution is given by

$$x \equiv b^u \pmod n,$$

where u and v are positive integers such that $ku = \phi(n)v + 1$.

Proof. Suppose b is an integer and k and n are natural numbers such that $(k, \phi(n)) = 1$. Then by Theorem 6.32, we know that $x^k \equiv b \pmod n$ has a solution modulo n. Now suppose that, $(b, n) = 1$ and that there exits two distinct solutions x_1 and x_2 such that $x_1^k \equiv b \pmod n$ and $x_2^k \equiv b \pmod n$. Therefore, by direct proof,

$$\begin{aligned} x_1 - x_2 &\equiv 0 \pmod n \\ x_1 &\equiv x_2 \pmod n \end{aligned}$$

Thus, the solution must be unique if $(b, n) = 1$. □

6.36 Exercise

Find the 49th root of 100 modulo 151.

$$\begin{aligned}
&x^{49} \equiv 100 \pmod{151}\\
&k = 49\\
&\phi(151) = 150\\
&(k, \phi(151)) = (49, 150) \implies 49u = 150v + 1, \exists u, v \in \mathbf{Z}\\
&u = 49\\
&v = 16\\
&x \equiv 100^{49} \equiv 103 \pmod{151}
\end{aligned}$$

6.37 Theorem

If a is an integer, v is a natural number, and n is a product of distinct primes, then $a^{v\phi(n)+1} \equiv a \pmod{n}$.

Proof. Suppose $a \in \mathbf{Z}$, $v \in \mathbf{N}$ and n is the product of distinct primes. By Euler's Theorem we know that $a^{\phi(n)} \equiv 1 \pmod{n}$.

- Case 1: if $(a, n) = 1$ with $a \neq n$, then

$$\begin{aligned}
a^{\phi(n)} &\equiv 1 \pmod{n}\\
a^{v\phi(n)+1} &\equiv a^{v\phi(n)+1} \pmod{n}\\
&\equiv 1^v a \pmod{n}\\
&\equiv a \pmod{n}
\end{aligned}$$

- Case 2: if $(a, n) \neq 1$, then

$$\begin{aligned}
a &\equiv 0 \pmod{n}\\
a^{\phi(n)} &\equiv 0 \pmod{n}\\
a^{v\phi(n)+1} &\equiv 0 \times a \pmod{n}\\
&\equiv a \equiv 0 \pmod{n}
\end{aligned}$$

□

6.38 Theorem

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 $x^k \equiv b \pmod{n}$ has a unique solution modulo n for any integer b. Moreover, that solution is given by

$$x \equiv b^u \pmod{n},$$

where u and v are positive integers such that $ku - \phi(n)v = 1$.

Proof. Suppose n is natural number that is a product of distinct primes and k is a natural number such that $(k, \phi(n)) = 1$. By Theorem 1.39, we can express $(k, \phi(n)) = 1 \Longrightarrow ku + \phi(n)(-v) = 1, \exists u, v \in \mathbf{Z}$.
Now there exists integer b such that $(b, n) = 1$. Thus, by Theorem 6.32 and 6.37, $b^{ku} \equiv b^{v\phi(n)+1} \equiv b \pmod{n}$. Now we know, using Euler's Theorem, that $b^{\phi(n)} \equiv 1 \pmod{n}$, which then can be express as,

$$\begin{aligned} b^{\phi(n)} &\equiv 1 \pmod{n} \\ b^{v\phi(n)} &\equiv 1^v \pmod{n} \\ b^{v\phi(n)} &\equiv 1 \pmod{n} \end{aligned}$$

Now suppose x is the solution to $x \equiv b^u \pmod{n}$. Given $b^{ku} \equiv b \pmod{n}$, we can express it in terms of the solution x as $b^{ku} \equiv (b^u)^k \equiv x^k \equiv b \pmod{n}$. Thus, $x^k \equiv b \pmod{n}$ has a unique solution modulo n for any integer b. □

6.39 Exercise

Find the 37th root of 100 modulo 210.

$$\begin{aligned} &x^{37} \equiv 100 \pmod{210} \\ &k = 37 \\ &\phi(210) = 48 \\ &(k, \phi(210)) = (37, 48) \Longrightarrow 37u = 48v + 1, \exists u, v \in \mathbf{Z} \\ &u = 13 \\ &v = 10 \\ &x \equiv 100^{13} \equiv 100 \pmod{210} \end{aligned}$$

6.40 Theorem

Let p be a prime, b an integer, and k a natural number. Then the number of kth roots of b modulo p is either 0 or (k, p-1).

Proof. Let p be a prime, b an integer, and k a natural number. Suppose $x^k \equiv b \pmod{p}$ has a solution where $x = a, \exists \in \mathbf{Z}$. Then the other solutions are $x = ad, \exists d \in \mathbf{Z}$ with $d^k \equiv 1 \pmod{p}$. This solution must be in the set of $\{d \pmod{p} andord_p(d) \mid k\}$ which also implies that the set is $\{d \pmod{p}, ord_p(d) \mid kandord_p(d) \mid p-1\}$. This suggests that that the solution has to be $(k, p-1)$. □

6.41 Blank Paper Exercise

- Modulo to the power
- Polynominal Modulo
- Canoical complete residue systems
- Linear Congrueneces
- Chinese Remainder Theorem
- Proof 6.23 were extremely difficult. Did not complete