Introduction to Number Theory

George Voutsadakis[1]

[1]Mathematics and Computer Science
Lake Superior State University

LSSU Math 400

1. Congruences
   - Definitions
   - Chinese Remainder Theorem
   - The Theorems of Fermat and Euler
   - Wilson's Theorem
   - Lagrange's Theorem
   - Primitive Roots
   - Indices

Subsection 1

Definitions

Congruence Modulo n

- Suppose that a, b are integers and that n is a natural number.
  By $a \equiv b \pmod{n}$ one means n divides $b - a$.
  We say that a is **congruent to** b **modulo** n.
- If $0 \le b < n$ then one refers to b as the **residue** of $a \pmod{n}$.

Residue Classes

Proposition

Congruence modulo n is a equivalence relation on $\mathbb{Z}$.

- One needs to verify reflexivity, symmetry and transitivity:
  - $n \mid 0 = a - a$. So $a \equiv a$.
  - $a \equiv b$ iff $n \mid b - a$ iff $n \mid -(b-a)$ iff $n \mid a - b$ iff $b \equiv a$.
  - $a \equiv b$ and $b \equiv c$ iff $n \mid b - a$ and $n \mid c - b$ imply $n \mid (b-a) + (c-b)$ iff $n \mid c - a$ iff $a \equiv c$.
- The equivalence classes are called **residue classes** or **congruence classes**.
- By a **complete set of residues** $\pmod{n}$ one means a set of n integers, one from each residue class $\pmod{n}$.

Operations on Classes Modulo n

Proposition

If $a \equiv a' \pmod{n}$ and $b \equiv b' \pmod{n}$, then:

- $a + b \equiv a' + b'$ and $a - b \equiv a' - b' \pmod{n}$;
- $a \cdot b \equiv a' \cdot b' \pmod{n}$.

- We show the case of addition, since subtraction is similar.

  We have $a \equiv a'$ and $b \equiv b'$ iff $n \mid a' - a$ and $n \mid b' - b$ imply $n \mid (a' - a) + (b' - b)$ iff $n \mid (a' + b') - (a + b)$ iff $a + b \equiv a' + b'$.
- For multiplication, we get:

  $a \equiv a'$ and $b \equiv b'$ iff $n \mid a' - a$ and $n \mid b' - b$ imply $n \mid (a' - a)b$ and $n \mid a'(b' - b)$ imply $n \mid (a' - a)b + a'(b' - b)$ iff $n \mid a'b' - ab$ iff $a'b' \equiv ab$.

Polynomial Operations on Classes Modulo n

Proposition

If $f(x) = c_n x^n + c_{n-1}x^{n-1} + \cdots + c_1 x + c_0$ is any polynomial with integer coefficients, then

$$a \equiv a' \pmod{n} \quad \text{implies} \quad f(a) \equiv f(a') \pmod{n}.$$

- First, note that, by the preceding theorem and an easy induction, if $a \equiv a'$, then, for every positive i, $a^i \equiv a'^i$.

  Thus, again by the preceding theorem, for all i, $c_i a^i \equiv c_i a'^i$.

  Using the preceding theorem once more,

  $$c_n a^n + c_{n-1}a^{n-1} + \cdots + c_1 a + c_0 \equiv c_n a'^n + c_{n-1}a'^{n-1} + \cdots + c_1 a' + c_0,$$

  i.e., $f(a) \equiv f(a')$.

An Additional Property

Proposition

If $ka \equiv ka' \pmod{n}$, for some natural number k, with $(k,n)=1$, then $a \equiv a' \pmod{n}$.

- We reason as follows:

  $ka \equiv ka'$ iff $n \mid ka' - ka$ iff $n \mid k(a'-a)$ implies, since $(k,n)=1$, $n \mid a'-a$ iff $a \equiv a'$.

- It follows that, if $a_1, \ldots, a_n$ is a complete set of residues $\pmod{n}$ and $(k,n)=1$, then so is $ka_1, \ldots, ka_n$.

A Generalization

Proposition

If k is any natural number,

$$ka \equiv ka' \pmod{n} \quad \text{implies} \quad a \equiv a' \pmod{\frac{n}{(k,n)}}.$$

- We have

  $ka \equiv ka' \pmod{n}$ iff $n \mid ka' - ka$ iff $n \mid k(a' - a)$ implies $\frac{n}{(k,n)} \mid \frac{k}{(k,n)}(a' - a)$ implies, since $(\frac{k}{(k,n)}, \frac{n}{(k,n)}) = 1$, $\frac{n}{(k,n)} \mid a' - a$ iff $a \equiv a' \pmod{\frac{n}{(k,n)}}$.

Subsection 2

Chinese Remainder Theorem

Solving a Linear Congruence

Proposition

Let a, n be natural numbers and let b be any integer. The linear congruence $ax \equiv b \pmod{n}$ is soluble for some integer x if and only if (a, n) divides b.

- Suppose, first, that, for some integer x, $ax \equiv b \pmod{n}$.

  Then, we get $n \mid b - ax$, i.e., there exists k, such that $b - ax = kn$, or $b = ax + kn$. Since $(a, n) \mid a$ and $(a, n) \mid n$, we get $(a, n) \mid b$.

  Suppose that $d = (a, n)$ divides b.

  Let $a' = \frac{a}{d}$, $b' = \frac{b}{d}$ and $n' = \frac{n}{d}$.

  It suffices to solve $a'x \equiv b' \pmod{n'}$.

  This has precisely one solution $\pmod{n'}$, since $(a', n') = 1$.

  So, $a'x$ runs through a complete set of residues $\pmod{n'}$ as x runs through such a set.

Solving a Linear Congruence (Remarks)

- Keep the notation of the preceding slide.
- Suppose x' is any solution of $a'x' \equiv b' \pmod{n'}$.
- Then the complete set of solutions $\pmod{n}$ of

$$ax \equiv b \pmod{n}$$

  is given by

$$x = x' + mn', \quad m = 1, 2, \ldots, d.$$

- Hence, when $d := (a, n)$ divides b, the congruence $ax \equiv b \pmod{n}$ has precisely d solutions $\pmod{n}$.

The Field $\mathbb{F}_p$

- If p is a prime and if a is not divisible by p, then the congruence $ax \equiv b \pmod{p}$ is always soluble.
- In fact, there is a unique solution $\pmod{p}$.
- This implies that the residues $0, 1, \ldots, p-1$ form a field under addition and multiplication $\pmod{p}$,

  i.e., every non-zero element has a unique multiplicative inverse.
- We shall denote the field of residues $\pmod{p}$ by $\mathbb{F}_p$.
- Obviously the field has characteristic p.
- Since any other finite field with characteristic p is a vector space over $\mathbb{F}_p$, it must have $q = p^e$ elements, for some e.

  An essentially unique field with q elements actually exists.

The Chinese Remainder Theorem

The Chinese Remainder Theorem

Let $n_1,\ldots,n_k$ be natural numbers, such that $(n_i,n_j)=1$ for $i\neq j$. For any integers $c_1,\ldots,c_k$, the congruences

$$x\equiv c_j \pmod{n_j},\quad 1\leq j\leq k,$$

are soluble simultaneously for some integer x. In fact, there is a unique solution modulo $n=n_1\cdots n_k$.

- Let $m_j=\frac{n}{n_j}$, $1\leq j\leq k$. Then $(m_j,n_j)=1$ and, thus, there is x_j, such that $m_jx_j\equiv c_j \pmod{n_j}$. Moreover, $m_ix_i\equiv 0 \pmod{n_j}$, for all $i\neq j$. Thus, for all j, $m_1x_1+\cdots+m_kx_k\equiv c_j \pmod{n_j}$.

  If x,y are two solutions, then $x\equiv y \pmod{n_j}$, for $1\leq j\leq k$.

  Since the n_j are coprime in pairs, we have $x\equiv y \pmod{n}$.

A Generalization of the Chinese Remainder Theorem

Theorem (Generalized Chinese Remainder Theorem)

If $n_1, \ldots, n_k$ are coprime in pairs, then the congruences

$$a_j x_j \equiv b_j \pmod{n_j}, \quad 1 \leq j \leq k,$$

are soluble simultaneously if and only if (a_j, n_j) divides b_j, for all j.

- Suppose $n_1, \ldots, n_k$ are coprime in pairs.

  By the Chinese Remainder Theorem, $y \equiv b_j \pmod{n_j}$, $j = 1, \ldots, k$, are soluble simultaneously for some y.

  By the first theorem, $a_j x_j \equiv b_j \mod n_j$ is soluble iff $(a_j, n_j) \mid b_j$.

Example

- Consider the congruences

$$x \equiv 2 \pmod{5}, \quad x \equiv 3 \pmod{7}, \quad x \equiv 4 \pmod{11}.$$

The solution is given by $x = 77x_1 + 55x_2 + 35x_3$, where x_1, x_2, x_3 satisfy

$$2x_1 \equiv 2 \pmod{5}, \quad 6x_2 \equiv 3 \pmod{7}, \quad 2x_3 \equiv 4 \pmod{11}.$$

Thus, we can take $x_1 = 1$, $x_2 = 4$, $x_3 = 2$.

These give $x = 367$, i.e., the complete solution is $x \equiv -18 \pmod{385}$.

Example

- Consider the congruences

$$x \equiv 1 \pmod{3}, \quad x \equiv 2 \pmod{10}, \quad x \equiv 3 \pmod{11}.$$

The solution is given by $x = 110x_1 + 33x_2 + 30x_3$, where x_1, x_2, x_3 satisfy

$$2x_1 \equiv 1 \pmod{3}, \quad 3x_2 \equiv 2 \pmod{10}, \quad 8x_3 \equiv 3 \pmod{11}.$$

Thus, we can take $x_1 = 2$, $x_2 = 4$, $x_3 = 10$.

These give $x = 652$, i.e., the complete solution is $x \equiv -8 \pmod{330}$.

Subsection 3

The Theorems of Fermat and Euler

Reduced Set of Residues

- A **reduced set of residues** $\pmod{n}$ is a set of $\varphi(n)$ numbers, one from each of the $\varphi(n)$ residue classes that consist of numbers relatively prime to n.
- The set

$$\{a : 1 \le a \le n \text{ and } (a,n) = 1\}$$

is a reduced set of residues $\pmod{n}$.

Multiplicativity of φ

Theorem (Multiplicativity of φ)

φ is multiplicative.

- Let n, n' be natural numbers with $(n, n') = 1$. Let a and a' run through reduced sets of residues $\pmod{n}$ and $\pmod{n'}$, respectively. To see that $\varphi(n)\varphi(n') = \varphi(nn')$, we must show that $an' + a'n$ runs through a reduced set of residues $\pmod{nn'}$.
  First, note that:
  - $(a, n) = 1$ implies $(an' + a'n, n) = 1$;
  - $(a', n') = 1$ implies $(an' + a'n, n') = 1$.

  Now, since $(n, n') = 1$, we get $(an' + a'n, nn') = 1$.
  Note, also, that any two distinct numbers of this form are incongruent $\pmod{nn'}$.
  Let $an' + a'n \equiv bn' + b'n \pmod{nn'}$. Then, $nn' \mid (bn' + b'n) - (an' + a'n)$. Hence, $nn' \mid (b - a)n' + (b' - a')n$. Since $(n, n') = 1$, we get $a = b$ and $a' = b'$.

Multiplicativity of φ (Cont'd)

- Finally, we show that if $(b, nn') = 1$, then

$$b \equiv an' + a'n \pmod{nn'},$$

  for some a, a' as above.

  Since $(n, n') = 1$, there exist integers m, m' satisfying $mn' + m'n = 1$.
  - Suppose for some prime $p > 1$, $p \mid bm$ and $p \mid n$. Then, since, by $mn' + m'n = 1$, $p \nmid m$. So $p \mid b$. But, then $p \mid (b, nn')$, contradicting $(b, nn') = 1$.

    We conclude $(bm, n) = 1$. So $a \equiv bm \pmod{n}$, for some a.
  - Similarly, $a' \equiv bm' \pmod{n'}$, for some a',

  These a, a' have the required property.

Fermat's Theorem and Euler's Theorem

(Theorem (Euler's Theorem)

If a, n are natural numbers with $(a, n) = 1$, then

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

- Since $(a, n) = 1$, as x runs through a reduced set of residues $\pmod{n}$, so also does ax.

  Hence, $\prod(ax) \equiv \prod(x) \pmod{n}$, where the products are taken over all x in the reduced set.

  Upon canceling $\prod(x)$ from both sides, we get the result.

Corollary (Fermat's Theorem)

If a is any natural number and if p is any prime then $a^p \equiv a \pmod{p}$.

- In particular, if $(a, p) = 1$, then $a^{p-1} \equiv 1 \pmod{p}$.

Subsection 4

Wilson's Theorem

Wilson's Theorem

- The result is attributed to Wilson, but the statement was first published by Waring in 1770 and a proof was by Lagrange.

Theorem (Wilson's Theorem)

$(p-1)! \equiv -1 \pmod{p}$, for any prime p.

- Being obvious for $p=2$, we assume that p is odd.

  For every a, with $0<a<p$, there is a unique a', with $0<a'<p$, such that $aa' \equiv 1 \pmod{p}$.

  Further, if $a=a'$, then $a^2 \equiv 1 \pmod{p}$, whence $a=1$ or $a=p-1$.

  Thus, the set $2,3,\ldots,p-2$ can be divided into $\frac{1}{2}(p-3)$ pairs a,a', with $aa' \equiv 1 \pmod{p}$.

  Hence, we have $2 \cdot 3 \cdots (p-2) \equiv 1 \pmod{p}$.

  So $(p-1)! \equiv p-1 \equiv -1 \pmod{p}$.

A Converse to Wilson's Theorem

Theorem (Converse to Wilson's Theorem)

An integer $n > 1$ is a prime if and only if $(n-1)! \equiv -1 \pmod{n}$.

- If n is a prime, the congruence holds by Wilson's Theorem.

  Suppose n is not a prime, e.g., $n = k\ell$, with $k, \ell < n$.

  Assume to the contrary that $(n-1)! \equiv -1 \pmod{n}$.

  Then $k \mid n \mid (n-1)! + 1$.

  But $k \mid (n-1)!$.

  These give $k \mid 1$, a contradiction.

A Solution to a Congruence

Theorem

If p is a prime, with $p \equiv 1 \pmod 4$, then the congruence $x^2 \equiv -1 \pmod p$ has solutions $x = \pm(r!)$, where $r = \frac{1}{2}(p-1)$.

All following congruences are taken $\pmod p$:

$$\begin{array}{rcl}(\pm(r!))^2 & \equiv & (\pm\frac{p-1}{2}!)^2 \equiv \frac{p-1}{2}!\frac{p-1}{2}! \\ & \equiv & 1 \cdot 2 \cdots \frac{p-1}{2}(-\frac{p-1}{2}) \cdots (-2)(-1) \\ & \equiv & 1 \cdot 2 \cdots \frac{p-1}{2}(\frac{p-1}{2}+1)(\frac{p-1}{2}+2) \cdots (\frac{p-1}{2}+\frac{p-1}{2}) \\ & \equiv & 1 \cdot 2 \cdots (p-1) \equiv (p-1)! \equiv -1.\end{array}$$

- Note that the congruence has no solutions when $p \equiv 3 \pmod 4$. Otherwise we would have
$$x^{p-1} = x^{2r} \equiv (-1)^r = -1 \pmod p,$$
contradicting Fermat's Theorem.

Subsection 5

Lagrange's Theorem

Lagrange's Theorem

Theorem (Lagrange's Theorem)

Let $f(x)$ be a polynomial, with integer coefficients and with degree n. Suppose p is a prime and the leading coefficient of f is not divisible by p. The congruence $f(x) \equiv 0 \pmod{p}$ has at most n solutions $\pmod{p}$.

- The theorem holds for $n = 1$, by a previous result.
  We assume that it is valid for polynomials with degree $n - 1$.
  We prove the theorem for polynomials with degree n.
  Not that, for any integer a, $f(x) - f(a) = (x - a)g(x)$, where g is a polynomial with:
  - degree $n - 1$;
  - integer coefficients;
  - the same leading coefficient as f.

  By hypothesis, $g(x) \equiv 0 \pmod{p}$ has $\leq n - 1$ solutions $\pmod{p}$.
  But, if $f(x) \equiv 0 \pmod{p}$ has a solution $x = a$, then all solutions of the congruence satisfy $(x - a)g(x) \equiv 0 \pmod{p}$.

Factorization, Fermat's and Wilson's Theorems

- We write $f(x) \equiv g(x) \pmod{p}$ to signify that the coefficients of like powers of x in the polynomials f, g are congruent $\pmod{p}$.
- It is clear that if the congruence $f(x) \equiv 0 \pmod{p}$ has its full complement $a_1, \ldots, a_n$ of solutions $\pmod{p}$, then

$$f(x) \equiv c(x - a_1) \cdots (x - a_n) \pmod{p},$$

  where c is the leading coefficient of f.
- In particular, by Fermat's theorem, we have

$$x^{p-1} - 1 \equiv (x - 1) \cdots (x - p + 1) \pmod{p}.$$

- On comparing constant coefficients, we obtain another proof of Wilson's theorem.

Lagrange's Theorem Using $\mathbb{F}_p$

Theorem (Lagrange's Theorem)

The number of zeros in $\mathbb{F}_p$ of a polynomial defined over this field cannot exceed its degree.

- We assume the result is valid for polynomials with degree $n-1$.

  We prove the theorem for polynomials with degree n.

  Supposing that $f(x)$ is a polynomial over $\mathbb{F}_p$ with degree n and with at least one zero a in $\mathbb{F}_p$.

  Then

  $$f(x) = f(x) - f(a) = (x-a)g(x)$$

  where $g(x)$ is a polynomial over $\mathbb{F}_p$ with degree $n-1$.

  Since, by the hypothesis, $g(x)$ has at most $n-1$ roots, $f(x)$ has at most n roots.

Corollary

Corollary

The polynomial $x^d - 1$ has precisely d zeros in $\mathbb{F}_p$, for each divisor d of $p-1$.

- Note that
$$x^{p-1} - 1 = (x^d - 1)g(x),$$
where $g(x)$ has degree $p-1-d$.
  - By Fermat's theorem, $x^{p-1} - 1$ has $p-1$ zeros in $\mathbb{F}_p$.
  - by Lagrange's theorem, $g(x)$ has at most $p-1-d$ zeros in $\mathbb{F}_p$.

  It follows that $x^d - 1$ has at least $(p-1)-(p-1-d) = d$ zeros in $\mathbb{F}_p$.

  Example: Taking $d = 4$, we deduce that $x^2 + 1$ has precisely two zeros in $\mathbb{F}_p$, when $p \equiv 1 \pmod 4$.

Prime Power and Composite Moduli

- Lagrange's theorem is false for prime power moduli.
  E.g., $x^2 \equiv 1 \pmod 8$ has four solutions.
- Lagrange's theorem does not remain true for composite moduli.
  Let $m_1, \ldots, m_k$ be such that $(m_i, m_j) = 1$, $1 \le i < j \le k$.
  Let $f(x)$ be a polynomial with integer coefficients.
  Assume $f(x) \equiv 0 \pmod{m_j}$ has s_j solutions $\pmod{m_j}$.
  Then, by the Chinese Remainder Theorem, if $m = m_1 \cdots m_k$,

$$f(x) \equiv 0 \pmod m$$

has $s = s_1 \cdots s_k$ solutions $\pmod m$.

Subsection 6

Primitive Roots

Order

- Let a, n be natural numbers with $(a, n) = 1$.

  The least natural number d, such that $a^d \equiv 1 \pmod{n}$, is called the **order** of $a \pmod{n}$, and a is said to **belong to** $d \pmod{n}$.

Proposition

The order d of $a \pmod{n}$ divides every integer k, such that $a^k \equiv 1 \pmod{n}$.

- By the division algorithm, $k = dq + r$, with $0 \leq r < d$.

  Thus, $a^r \equiv a^k \equiv 1 \pmod{n}$, whence, $r = 0$.
- By Euler's theorem, the order d exists and it divides $\varphi(n)$.

Primitive Roots

- By a **primitive root** $\pmod{n}$ we mean a number that belongs to $\varphi(n) \pmod{n}$.
- Thus, for a prime p, a primitive root $\pmod{p}$ is an integer g, such that:
  - g is not divisible by p;
  - $p-1$ is the smallest exponent with $g^{p-1} \equiv 1 \pmod{p}$.
- I.e., a primitive root $\pmod{p}$ can be defined as a generator g of the multiplicative group of the field $\mathbb{F}_p$.

  Example: Take $p = 17$.

  The smallest primitive root is $g = 3$.

  The respective powers of 3 (mod 17) are

$$3, 9, 10, 13, 5, 15, 11, 16, 14, 8, 7, 4, 12, 2, 6, 1.$$

Number of Primitive Roots

Theorem

For every odd prime p, there exists a primitive root $\pmod{p}$. More precisely, there are exactly $\varphi(p-1)$ primitive roots $\pmod{p}$.

- Each of $1,2,\ldots,p-1$ belongs $\pmod{p}$ to some divisor d of $p-1$.
  Let $\psi(d)$ be the number that belongs to $d \pmod{p}$.
  Clearly, $\sum_{d|(p-1)} \psi(d) = p-1$.
  By a previous result, we have $\sum_{d|(p-1)} \varphi(d) = p-1$.
  So, it suffices to prove that, if $\psi(d) \neq 0$, then $\psi(d) = \varphi(d)$.
  This would imply that $\psi(d) \neq 0$, for all d,
  and, therefore, that $\psi(p-1) = \varphi(p-1)$.

Number of Primitive Roots (Cont'd)

Claim: if $\psi(d) \neq 0$, then $\psi(d) = \varphi(d)$.

Suppose that $\psi(d) \neq 0$.

Let a be a number that belongs to $d \pmod{p}$.

Then $a, a^2, \ldots, a^d$ are mutually incongruent solutions of $x^d \equiv 1 \pmod{p}$.

By Lagrange's theorem, they represent all the solutions (in fact we showed that the congruence has precisely d solutions $\pmod{p}$).

Subclaim: The numbers a^m, with $1 \leq m \leq d$ and $(m, d) = 1$ represent all the numbers that belong to $d \pmod{p}$.

Each of these has order d: If $a^{md'} \equiv 1$, then $d \mid md'$, whence $d \mid d'$.

If b belongs to $d \pmod{p}$, then $b \equiv a^m$, for some m, $1 \leq m \leq d$.

But $b^{d/(m,d)} \equiv (a^d)^{m/(m,d)} \equiv 1 \pmod{p}$. So $(m, d) = 1$.

We conclude that $\psi(d) = \varphi(d)$.

Working in $\mathbb{F}_p$

- By a **primitive root** $\pmod{p}$ we mean a generator g of the multiplicative group of $\mathbb{F}_p$.
- By the **order** of a non-zero element a of $\mathbb{F}^p$ we mean the least positive integer d such that $a^d = 1$.

Proposition

Let $\psi(d)$ be the number of elements in $\mathbb{F}_p$, with order d. If $\psi(d) \neq 0$, then $\psi(d) = \varphi(d)$.

- Let a be in $\mathbb{F}_p$, with order d. We show that the $\varphi(d)$ elements a^m, with $1 \leq m \leq d$ and $(m,d) = 1$ are precisely those with order d.
  The a^m, with $1 \leq m \leq d$, are distinct zeros of the polynomial $x^d - 1$, and, thus, by Lagrange's theorem, they are all the zeros. Hence, any element with order d is given by a^m, for some m.
  - We have $(a^m)^{d/(m,d)} = (a^d)^{m/(m,d)} = 1$. So $(m,d) = 1$.
  - Suppose $(m,d) = 1$. Then $a^{md} = 1$ and md is the smallest multiple of m divisible by d. So a^m has order d.

The Prime Power Property

Theorem

Let g be a primitive root $\pmod{p}$. There exists an integer x, such that $g' = g + px$ is a primitive root $\pmod{p^j}$, for all prime powers p^j.

- We have $g^{p-1} = 1 + py$, for some integer y.

  By the binomial theorem,

  $$g'^{p-1} = 1 + pz, \text{ where } z \equiv y + (p-1)g^{p-2}x \pmod{p}.$$

  The coefficient of x is not divisible by p.

  So, we can choose x, such that $(z, p) = 1$.

  Then g' has the required property.

The Prime Power Property (Cont'd)

- Suppose that g' belongs to $d \pmod{p^j}$.
  Then d divides $\varphi(p^j) = p^{j-1}(p-1)$.
  But $g' = g + px$ is a primitive root $\pmod{p}$.
  Therefore, $p-1$ divides d.
  Hence,
  $$d = p^k(p-1), \text{ for some } k < j.$$
  Now, we get $\pmod{p^j}$:
  $$\begin{array}{rcl} 1 & \equiv & g'^d = g'^{p^k(p-1)} = (1+pz)^{p^k} \\ & \overset{p \text{ odd}}{=} & 1 + p^{k+1}z_k, \text{ where } (z_k, p) = 1. \end{array}$$
  So, $p^{k+1}z_k \equiv 0 \pmod{p^j}$ and $(z_k, p) = 1$.
  These give $j = k+1$ and $d = \varphi(p^j)$.

Existence of Primitive Roots Modulo n

Theorem

For any natural number n, there exists a primitive root $\pmod{n}$ if and only if n has the form 2, 4, p^j or $2p^j$, where p is an odd prime.

- We show, first, that, if n has the form 2, 4, p^j or $2p^j$, where p is an odd prime, then there exists a primitive root $\bmod n$.
  - 1 is a primitive root $\pmod{2}$.
  - 3 is a primitive root $\pmod{4}$.
  - A primitive root $\pmod{p^j}$ exists by the preceding theorem.
  - Suppose g is a primitive root $\pmod{p^j}$.
    Let g' be the odd element of the pair $g, g+p^j$.
    Then, we have

$$\begin{array}{rcl} g'^{\varphi(2p^j)} & = & g'^{\varphi(p^j)} \equiv 1 \pmod{p^j}; \\ g'^{\varphi(2p^j)} & \equiv & 1 \pmod{2}. \end{array}$$

    Therefore, $g'^{\varphi(2p^j)} \equiv 1 \pmod{2p^j}$.

Existence of Primitive Roots Modulo n (Converse)

- We show the necessity of the assertion.

  Suppose $n = n_1 n_2$, where $(n_1, n_2) = 1$ and $n_1 > 2, n_2 > 2$.

  Let a be a natural number.

  We have that $\varphi(n_1)$ and $\varphi(n_2)$ are even and

$$a^{\frac{1}{2}\varphi(n)} = (a^{\varphi(n_1)})^{\frac{1}{2}\varphi(n_2)} \equiv 1 \pmod{n_1}.$$

  Similarly,

$$a^{\frac{1}{2}\varphi(n)} \equiv 1 \pmod{n_2}.$$

  Hence

$$a^{\frac{1}{2}\varphi(n)} \equiv 1 \pmod{n}.$$

Existence of Primitive Roots Modulo n (Conclusion)

- We finally show that there are no primitive roots $\pmod{2^j}$, for $j > 2$.
  By induction, we have, for all odd numbers a,
  $$a^{2^{j-2}} \equiv 1 \pmod{2^j}.$$
  Check that this is true for $j = 3$.
  Suppose that $a^{2^{k-2}} \equiv 1 \pmod{2^k}$, for some $k > 3$.
  Then, we have $a^{2^{k-2}} - 1 = 2^k m$, for some m.
  Now we get
  $$\begin{aligned} a^{2^{k-1}} &= a^{2^{k-2}+2^{k-2}} = a^{2^{k-2}} a^{2^{k-2}} = (2^k m + 1)^2 \\ &= 2^{2k} m^2 + 2 \cdot 2^k m + 1 = 2^{k+1}(2^{k-1} m^2 + m) + 1. \end{aligned}$$
  Therefore, $a^{2^{k-1}} \equiv 1 \pmod{2^{k+1}}$.

Subsection 7

Indices

Indices

- Let g be a primitive root $\pmod{n}$.
- The numbers
$$g^\ell, \quad \ell = 0, 1, \ldots, \varphi(n) - 1,$$
form a reduced set of residues $\pmod{n}$.
- For every integer a, with $(a, n) = 1$, there is a unique ℓ, such that
$$g^\ell \equiv a \pmod{n}.$$
The exponent ℓ is called the **index** of a with respect to g and it is denoted by $\mathrm{ind}_g a$.

Properties of Indices

Proposition

Let g be a primitive root $\pmod{n}$.

- $\operatorname{ind}_g a + \operatorname{ind}_g b \equiv \operatorname{ind}_g(ab) \pmod{\varphi(n)}$;
- $\operatorname{ind}_g 1 = 0$;
- $\operatorname{ind}_g g = 1$.

- Suppose $\ell = \operatorname{ind}_g a$ and $m = \operatorname{ind}_g b$.
  Then $g^\ell \equiv a \pmod{n}$ and $g^m \equiv b \pmod{n}$.
  It follows that $g^{\ell+m} \equiv ab \pmod{n}$.
  Thus, $\operatorname{ind}_g(ab) = \ell + m \pmod{\varphi(n)}$.
- $g^0 \equiv 1 \pmod{n}$.
- $g^1 \equiv g \pmod{n}$.

Power Rule for Indices

Proposition

Let g be a primitive root $\pmod{n}$. For every natural m, we have

$$\text{ind}_g(a^m) \equiv m \text{ ind}_g a \pmod{\varphi(n)}.$$

- Let $\ell = \text{ind}_g a$. So $g^\ell \equiv a \pmod{n}$.
  Then $g^{m\ell} = (g^\ell)^m \equiv a^m \pmod{n}$.
  It follows that $m \text{ ing}_g a = m\ell \equiv \text{ind}_g(a^m) \pmod{\varphi(n)}$.

Index of -1

Proposition

If g is a primitive root $\pmod{n}$, then $\text{ind}_g(-1) = \frac{1}{2}\varphi(n)$, for $n > 2$.

- Suppose $\ell = \text{ind}_g(-1)$.
  Then $g^{\ell} \equiv -1 \pmod{n}$ and $0 \le \ell < \varphi(n)$.
  Thus, $g^{2\ell} \equiv 1 \pmod{n}$ and $0 \le 2\ell < 2\varphi(n)$.
  It follows that $2\ell = \varphi(n)$.
  Therefore, $\text{ind}_g(-1) = \frac{\varphi(n)}{2}$.

Using Indices

Example: Consider $x^n \equiv a \pmod{p}$, where p is a prime.

We have $n \operatorname{ind}_g x \equiv \operatorname{ind}_g a \pmod{p-1}$.

Thus, if $(n, p-1) = 1$, then there is just one solution.

- Consider $x^5 \equiv 2 \pmod{7}$.

  Let $g = 3$, a primitive root $\pmod{7}$.

  $5 \operatorname{ind}_3 x \equiv \operatorname{ind}_3 2 \pmod{6}$

  $5 \operatorname{ind}_3 x \equiv 2 \pmod{6}$

  $\operatorname{ind}_3 x \equiv 4 \pmod{6}$

  $x \equiv 3^4 \equiv 4 \pmod{7}$