Introduction to Analytic Number Theory

George Voutsadakis[1]

[1]Mathematics and Computer Science
Lake Superior State University

LSSU Math 500

1. Primitive Roots
   - The Exponent of a Number mod m. Primitive roots
   - Primitive Roots and Reduced Residue Systems
   - The Nonexistence of Primitive Roots mod 2^α for $\alpha \geq 3$
   - The Existence of Primitive Roots mod p for Odd Primes p
   - Primitive Roots and Quadratic Residues
   - The Existence of Primitive Roots mod p^α
   - The Existence of Primitive Roots mod $2p^\alpha$
   - The Nonexistence of Primitive Roots in the Remaining Cases
   - The Number of Primitive Roots mod m
   - The Index Calculus
   - Primitive Roots and Dirichlet Characters
   - Real-Valued Dirichlet Characters mod p^α
   - Primitive Dirichlet Characters mod p^α

Subsection 1

The Exponent of a Number mod m. Primitive roots

Introducing Exponents and Primitive Roots

- Let a and m be relatively prime integers, with $m > 1$.
- Consider all the positive powers of a:

$$a, a^2, a^3, \ldots.$$

- We know, from the Euler-Fermat Theorem, that

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

- However, there may be an earlier power a^f, such that

$$a^f \equiv 1 \pmod{m}.$$

Exponents and Primitive Roots

Definition

The smallest positive integer f such that

$$a^f \equiv 1 \pmod{m}$$

is called the **exponent of a modulo m**, and is denoted by writing

$$f = \exp_m(a).$$

If $\exp_m(a) = \varphi(m)$, then a is called a **primitive root** mod m.

- The Euler-Fermat Theorem tells us that

$$\exp_m(a) \leq \varphi(m).$$

Properties of Exponents

Theorem

Given $m \geq 1$, $(a, m) = 1$, let $f = \exp_m(a)$. Then we have:

(a) $a^k \equiv a^h \pmod{m}$ if, and only if, $k \equiv h \pmod{f}$.

(b) $a^k \equiv 1 \pmod{m}$ if, and only if, $k \equiv 0 \pmod{f}$.
In particular $f \mid \varphi(m)$.

(c) The numbers $1, a, a^2, \ldots, a^{f-1}$ are incongruent mod m.

- Parts (b) and (c) follow at once from Part (a).
  So we need only prove Part (a).
  Assume, first, $a^k \equiv a^h \pmod{m}$. Then $a^{k-h} \equiv 1 \pmod{m}$.
  Write $k - h = qf + r$, where $0 \leq r < f$.
  Then $1 \equiv a^{qf+r} \equiv a^r \pmod{m}$. So $r = 0$ and $k \equiv h \pmod{f}$.
  Conversely, assume $k \equiv h \pmod{f}$. Then $k - h = qf$.
  So $a^{k-h} \equiv 1 \pmod{m}$. Hence, $a^k \equiv a^h \pmod{m}$.

Subsection 2

Primitive Roots and Reduced Residue Systems

Primitive Roots and Reduced Residue Systems

Theorem

Let $(a, m) = 1$. Then a is a primitive root mod m if and only if the numbers

$$a, a^2, \ldots, a^{\varphi(m)}$$

form a reduced residue system mod m.

- Suppose a is a primitive root. Then the numbers in the list are incongruent mod m, by Part (c) of the preceding theorem.

  But there are $\varphi(m)$ such numbers.

  So they form a reduced residue system mod m.

  Conversely, suppose the numbers in the list form a reduced residue system. Then $a^{\varphi(m)} \equiv 1 \pmod{m}$. But no smaller power is congruent to 1. So a is a primitive root.

Remark

- We saw that the reduced residue classes mod m form a group.
- Suppose m has a primitive root a.
- Then the theorem shows that this group is the cyclic group generated by the residue class $\widehat{a}$.

Moduli with Primitive Roots

- Suppose m has a primitive root.
- Then each reduced residue system mod m can be expressed as a geometric progression.
- Unfortunately, not all moduli have primitive roots.
- In the next few sections we will prove that primitive roots exist only for the following moduli:

$$m = 1, 2, 4, p^\alpha \text{ and } 2p^\alpha,$$

  where p is an odd prime and $\alpha \geq 1$.
- The first three cases are easily settled.
  - The case $m = 1$ is trivial.
  - For $m = 2$ the number 1 is a primitive root.
  - For $m = 4$, we have $\varphi(4) = 2$ and $3^2 \equiv 1 \pmod{4}$. So 3 is a primitive root.

Subsection 3

The Nonexistence of Primitive Roots mod 2^α for $\alpha \geq 3$

Nonexistence of Primitive Roots mod 2^α, $\alpha \geq 3$

Theorem

Let x be an odd integer. If $\alpha \geq 3$, we have

$$x^{\varphi(2^\alpha)/2} \equiv 1 \pmod{2^\alpha}.$$

So there are no primitive roots mod 2^α.

- If $\alpha = 3$, the claimed congruence is

$$x^2 \equiv 1 \pmod{8}, \quad \text{for } x \text{ odd}.$$

  This is verified by testing $x = 1, 3, 5, 7$.

  Alternatively, we note that

$$(2k+1)^2 = 4k^2 + 4k + 1 = 4k(k+1) + 1.$$

  Then observe that $k(k+1)$ is even.

Nonexistence of Primitive Roots mod 2^α, $\alpha \geq 3$ (Cont'd)

- Now we prove the theorem by induction on α.

  We assume the conclusion holds for α.

  We prove that it also holds for $\alpha + 1$.

  The induction hypothesis is that

  $$x^{\varphi(2^\alpha)/2} = 1 + 2^\alpha t,$$

  where t is an integer.

  Squaring both sides and taking into account $2\alpha > \alpha + 1$,

  $$x^{\varphi(2^\alpha)} = 1 + 2^{\alpha+1} t + 2^{2\alpha} t^2 \equiv 1 \pmod{2^{\alpha+1}}.$$

  Note that

  $$\varphi(2^\alpha) = 2^{\alpha-1} = \varphi(2^{\alpha+1})/2.$$

  So the proof is complete.

Subsection 4

The Existence of Primitive Roots mod p for Odd Primes p

Exponents of Powers

Lemma

Given $(a, m) = 1$, let $f = \exp_m(a)$. Then

$$\exp_m(a^k) = \frac{\exp_m(a)}{(k, f)}.$$

In particular, $\exp_m(a^k) = \exp_m(a)$ if, and only if, $(k, f) = 1$.

- $\exp_m(a^k)$ is the smallest $x > 0$, such that $a^{xk} \equiv 1 \pmod{m}$.
  This is also the smallest $x > 0$ such that $kx \equiv 0 \pmod{f}$.
  The latter is equivalent to $x \equiv 0 \pmod{\frac{f}{d}}$, where $d = (k, f)$.
  The smallest positive solution of this congruence is $\frac{f}{d}$.
  So $\exp_m(a^k) = \frac{f}{d}$.

Primitive Roots Modulo a Prime

Theorem

Let p be an odd prime. Let d be any positive divisor of $p-1$. Then in every reduced residue system mod p there are exactly $\varphi(d)$ numbers a, such that

$$\exp_p(a) = d.$$

In particular, when $d = \varphi(p) = p-1$, there are exactly $\varphi(p-1)$ primitive roots mod p.

- The numbers $1, 2, \ldots, p-1$ are distributed into disjoint sets $A(d)$, each set corresponding to a divisor d of $p-1$, where

$$A(d) = \{x : 1 \leq x \leq p-1 \text{ and } \exp_p(x) = d\}.$$

  Let $f(d)$ be the number of elements in $A(d)$.
  Then $f(d) \geq 0$, for each d.
  Our goal is to prove that $f(d) = \varphi(d)$.

Primitive Roots Modulo a Prime (Cont'd)

- Note that:
  - The sets $A(d)$ are disjoint;
  - Each $x = 1, 2, \ldots, p-1$ falls into some $A(d)$.

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

  But we also have $\sum_{d|p-1} \varphi(d) = p-1$.

  So
  $$\sum_{d|p-1} \{\varphi(d) - f(d)\} = 0.$$

  To show that each term is zero, it suffices to show $f(d) \leq \varphi(d)$.

  We do this by showing that either $f(d) = 0$ or $f(d) = \varphi(d)$.

  Equivalently, we show $f(d) \neq 0$ implies $f(d) = \varphi(d)$.

Primitive Roots Modulo a Prime (Cont'd)

- Suppose that $f(d) \neq 0$. Then $A(d)$ is nonempty.
  So $a \in A(d)$, for some a. Therefore, $\exp_p(a) = d$.
  Hence $a^d \equiv 1 \pmod{p}$.
  But every power of a satisfies the same congruence.
  So the d numbers $a, a^2, \ldots, a^d$ are solutions of the congruence

$$x^d - 1 \equiv 0 \pmod{p}.$$

  These solutions are incongruent mod p since $d = \exp_p(a)$.
  But the congruence has at most d solutions, since p is prime.
  So the d powers must be all its solutions.
  Hence, each number in $A(d)$ must be of the form a^k, for some $k = 1, 2, \ldots, d$.
  By a previous lemma, $\exp_p(a^k) = d$ if, and only if, $(k, d) = 1$.
  In other words, among the d powers there are $\varphi(d)$ which have exponent d modulo p. So $f(d) = \varphi(d)$ if $f(d) \neq 0$.

Subsection 5

Primitive Roots and Quadratic Residues

Primitive Roots and Quadratic Residues

Theorem

Let g be a primitive root mod p, where p is an odd prime. Then the even powers

$$g^2, g^4, \ldots, g^{p-1}$$

are the quadratic residues mod p, and the odd powers

$$g, g^3, \ldots, g^{p-2}$$

are the quadratic nonresidues mod p.

- Suppose n is even, say $n = 2m$. Then $g^n = (g^m)^2$.
  So $g^n \equiv (g^m)^2 \pmod{p}$. Hence $g^n R p$.
  But there are $\frac{p-1}{2}$ distinct even powers $g^2, \ldots, g^{p-1}$ modulo p and the same number of quadratic residues mod p.
  Therefore, the even powers are the quadratic residues and the odd powers are the nonresidues.

Subsection 6

The Existence of Primitive Roots mod p^α

Primitive Roots mod p^α

- We turn to the case $m = p^\alpha$, where p is an odd prime and $\alpha \geq 2$.
- In seeking primitive roots mod p^α it is natural to consider as candidates the primitive roots mod p.
- Let g be a primitive root mod p.
- We ask whether g might also be a primitive root mod p^2.
- Now $g^{p-1} \pmod{p}$.
- Moreover, $\varphi(p^2) = p(p-1) > p-1$.
- So g will not be a primitive root mod p^2 if $g^{p-1} \equiv 1 \pmod{p^2}$.
- Therefore, the relation $g^{p-1} \not\equiv 1 \pmod{p^2}$ is a necessary condition for a primitive root g mod p to also be a primitive root mod p^2.
- Remarkably, this condition is also sufficient for g to be a primitive root mod p^2 and, more generally, mod p^α, for all powers $a \geq 2$.

Existence of Primitive Roots mod p^α

Theorem

Let p be an odd prime. Then we have:

(a) If g is a primitive root mod p, then g is also a primitive root mod p^α, for all $\alpha \geq 1$ if, and only if,

$$g^{p-1} \not\equiv 1 \pmod{p^2}.$$

(b) There is at least one primitive root g mod p which satisfies

$$g^{p-1} \not\equiv 1 \pmod{p^2}.$$

Hence, there exists at least one primitive root mod p^α, if $\alpha \geq 2$.

Existence of Primitive Roots mod p^α (Part (b))

(b) Let g be a primitive root mod p.

If $g^{p-1} \not\equiv 1 \pmod{p^2}$, there is nothing to prove.

If $g^{p-1} \equiv 1 \pmod{p^2}$, we can show that $g_1 = g + p$, which is another primitive root modulo p, satisfies the condition $g_1^{p-1} \not\equiv 1 \pmod{p^2}$.

In fact, we have

$$\begin{aligned} g_1^{p-1} &= (g+p)^{p-1} \\ &= g^{p-1} + (p-1)g^{p-2}p + tp^2 \\ &\equiv g^{p-1} + (p^2-p)g^{p-2} \pmod{p^2} \\ &\equiv 1 - pg^{p-2} \pmod{p^2}. \end{aligned}$$

But we cannot have $pg^{p-2} \equiv 0 \pmod{p^2}$ for this would imply $g^{p-2} \equiv 0 \pmod{p}$, contradicting the primitivity of g mod p.

Hence, $g_1^{p-1} \not\equiv 1 \pmod{p^2}$.

Existence of Primitive Roots mod p^α (Part (a))

(a) Let g be a primitive root modulo p.

If g is a primitive root mod p^α, for all $\alpha \geq 1$, then, in particular, it is a primitive root mod p^2.

As we have already shown, this implies the condition.

Conversely, let g is a primitive root mod p, such that

$$g^{p-1} \not\equiv 1 \pmod{p^2}.$$

We must show that g is also a primitive root mod p^α, for all $\alpha \geq 2$.

Let t be the exponent of g modulo p^α.

We wish to show that $t = \varphi(p^\alpha)$.

Now $g^t \equiv 1 \pmod{p^\alpha}$. Hence, $g^t \equiv 1 \pmod{p}$.

So $\varphi(p) \mid t$. We can write $t = q\varphi(p)$.

Existence of Primitive Roots mod p^α (Part (a) Cont'd)

- Now $t \mid \varphi(p^\alpha)$. So $q\varphi(p) \mid \varphi(p^\alpha)$.
  But $\varphi(p^\alpha) = p^{\alpha-1}(p-1)$. Hence, $q(p-1) \mid p^{\alpha-1}(p-1)$.
  This means $q \mid p^{\alpha-1}$. Therefore, $q = p^\beta$, where $\beta \leq \alpha - 1$.
  We conclude $t = p^\beta(p-1)$.
  Claim: $\beta = \alpha - 1$, whence $t = \varphi(p^\alpha)$.
  Suppose, on the contrary, that $\beta < \alpha - 1$. Then $\beta \leq \alpha - 2$.
  We have
  $$t = p^\beta(p-1) \mid p^{\alpha-2}(p-1) = \varphi(p^{\alpha-1}).$$
  Thus, $\varphi(p^{\alpha-1})$ is a multiple of t.
  This implies $g^{\varphi(p^{\alpha-1})} \equiv 1 \pmod{p^\alpha}$.
  Now we make use of the following Lemma which shows that this congruence is a contradiction.

Existence of Primitive Roots mod p^α (Lemma)

Lemma

Let g be a primitive root modulo p such that

$$g^{p-1} \not\equiv 1 \pmod{p^2}.$$

Then for every $\alpha \geq 2$, we have

$$g^{\varphi(p^{\alpha-1})} \not\equiv 1 \pmod{p^\alpha}.$$

- We use induction on α.

  For $\alpha = 2$, the conclusion is immediate.

  Suppose that the conclusion holds for α.

  By the Euler-Fermat Theorem, $g^{\varphi(p^{\alpha-1})} \equiv 1 \pmod{p^{\alpha-1}}$.

  So $g^{\varphi(p^{\alpha-1})} = 1 + kp^{\alpha-1}$, where $p \nmid k$ because of the hypothesis.

Existence of Primitive Roots mod p^α (Lemma Cont'd)

- We obtained $g^{\varphi(p^{\alpha-1})} = 1 + kp^{\alpha-1}$, where $p \nmid k$.

  Raise both sides to the p-th power,

$$g^{\varphi(p^\alpha)} = (1 + kp^{\alpha-1})^p = 1 + kp^\alpha + k^2 \frac{p(p-1)}{2} p^{2(\alpha-1)} + rp^{3(\alpha-1)}.$$

  We have, since $\alpha \geq 2$:
  - $2\alpha - 1 \geq \alpha + 1$;
  - $3\alpha - 3 \geq \alpha + 1$.

  Hence, the last equation gives us the congruence

$$g^{\varphi(p^\alpha)} \equiv 1 + kp^\alpha \pmod{p^{\alpha+1}}.$$

  Since $p \nmid k$,

$$g^{\varphi(p^\alpha)} \not\equiv 1 \pmod{p^{\alpha+1}}.$$

  So the conclusion holds for $\alpha + 1$.

Subsection 7

The Existence of Primitive Roots mod $2p^\alpha$

The Existence of Primitive Roots mod $2p^\alpha$

Theorem

If p is an odd prime and $\alpha \geq 1$, there exist odd primitive roots g modulo p^α. Each such g is also a primitive root modulo $2p^\alpha$.

- If g is a primitive root modulo p^α, so is $g + p^\alpha$. But one of g or $g + p^\alpha$ is odd. So odd primitive roots mod p^α always exist.

  Let g be an odd primitive root mod p^α.

  Let f be the exponent of g mod $2p^\alpha$.

  We wish to show that $f = \varphi(2p^\alpha)$.
  - We have $f \mid \varphi(2p^\alpha)$, and $\varphi(2p^\alpha) = \varphi(2)\varphi(p^\alpha) = \varphi(p^\alpha)$. So $f \mid \varphi(p^\alpha)$.
  - We also have $g^f \equiv 1 \pmod{2p^\alpha}$. So $g^f \equiv 1 \pmod{p^\alpha}$. Hence, $\varphi(p^\alpha) \mid f$, since g is a primitive root mod p^α.

  Therefore, $f = \varphi(p^\alpha) = \varphi(2p^\alpha)$. So g is primitive mod $2p^\alpha$.

Subsection 8

The Nonexistence of Primitive Roots in the Remaining Cases

Nonexistence of Primitive Roots

Theorem

Let $m \geq 1$ be not of the form $m = 1, 2, 4, p^\alpha$ or $2p^\alpha$, where p is an odd prime. Then for any a, with $(a, m) = 1$, we have

$$a^{\varphi(m)/2} \equiv 1 \pmod{m}.$$

So there are no primitive roots mod m.

- We have seen that there are no primitive roots mod 2^α if $\alpha \geq 3$. Therefore, we can assume

$$m = 2^\alpha p_1^{\alpha_1} \cdots p_s^{\alpha_s},$$

where the p_i are odd primes, $s \geq 1$, and $\alpha \geq 0$.
By hypothesis, m is not of the form $1, 2, 4, p^\alpha$ or $2p^\alpha$.
So $\alpha \geq 2$, if $s = 1$, and $s \geq 2$, if $\alpha = 0$ or 1.
Note that $\varphi(m) = \varphi(2^\alpha)\varphi(p_1^{\alpha_1}) \cdots \varphi(p_s^{\alpha_s})$.

Nonexistence of Primitive Roots (Cont'd)

- Now let a be any integer relatively prime to m.

  We wish to prove that $a^{\varphi(m)/2} \equiv 1 \pmod{m}$.

  Let g be a primitive root mod $p_1^{\alpha_1}$.

  Choose k so that

$$a \equiv g^k \pmod{p_1^{\alpha_1}}.$$

  Then we have

$$\begin{aligned} a^{\varphi(m)/2} &\equiv g^{k\varphi(m)/2} \pmod{p_1^{\alpha_1}} \\ &\equiv g^{k\varphi(2^\alpha)\varphi(p_1^{\alpha_1})\cdots\varphi(p_s^{\alpha_s})/2} \pmod{p_1^{\alpha_1}} \\ &\equiv g^{t\varphi(p_1^{\alpha_1})} \pmod{p_1^{\alpha_1}}, \end{aligned}$$

  where

$$t = k\varphi(2^\alpha)\varphi(p_2^{\alpha_2})\cdots\varphi(p_s^{\alpha_s})/2.$$

Nonexistence of Primitive Roots (Cont'd)

Claim: $t = k\varphi(2^{\alpha})\varphi(p_2^{\alpha_2})\cdots\varphi(p_s^{\alpha_s})/2$ is an integer.

If $\alpha \geq 2$, the factor $\varphi(2^{\alpha})$ is even. Hence t is an integer.

If $\alpha = 0$ or 1, then $s \geq 2$ and the factor $\varphi(p_2^{\alpha_2})$ is even.

So t is an integer in this case as well.

Hence we get

$$a^{\varphi(m)/2} \equiv 1 \pmod{p_1^{\alpha_1}}.$$

In the same way we find, for all $i = 1, 2, \ldots, s$,

$$a^{\varphi(m)/2} \equiv 1 \pmod{p_i^{\alpha_i}}.$$

Nonexistence of Primitive Roots (Conclusion)

Claim: We also have $a^{\varphi(m)/2} \equiv 1 \pmod{2}$

Suppose $\alpha \geq 3$. The condition $(a, m) = 1$ requires a to be odd.

By a previous theorem, $a^{\varphi(2^\alpha)/2} \equiv \pmod{2^\alpha}$.

But $\varphi(2^\alpha) \mid \varphi(m)$. Hence, $a^{\varphi(m)/2} \equiv 1 \pmod{2^\alpha}$, for $\alpha \geq 3$.

Suppose $\alpha \leq 2$. Then $a^{\varphi(2^\alpha)} \equiv 1 \pmod{2^\alpha}$.

But $s \geq 1$. Hence,

$$\varphi(m) = \varphi(2^\alpha)\varphi(p_1^{\alpha_1}) \cdots \varphi(p_s^{\alpha_s}) = 2r\varphi(2^\alpha), \quad r \text{ an integer.}$$

It follows that $\varphi(2^\alpha) \mid \varphi(m)/2$.

We conclude that $a^{\varphi(m)/2} \equiv 1 \pmod{2^\alpha}$, for all α.

Multiplying all these congruences, we get $a^{\varphi(m)/2} \equiv 1 \pmod{m}$.

So a cannot be a primitive root mod m.

Subsection 9

The Number of Primitive Roots mod m

Number of Primitive Roots

Theorem

If m has a primitive root g, then m has exactly $\varphi(\varphi(m))$ incongruent primitive roots and they are given by the numbers in the set

$$S = \{g^n : 1 \leq n \leq \varphi(m) \text{ and } (n, \varphi(m)) = 1\}.$$

- Since g is a primitive root of m,

$$\exp_m(g) = \varphi(m).$$

  By a previous lemma,

$$\exp_m(g^n) = \exp_m(g) \quad \text{if and only if} \quad (n, \varphi(m)) = 1.$$

  Therefore, each element of S is a primitive root mod m.

Number of Primitive Roots (Cont'd)

- Conversely, suppose a is a primitive root mod m.

  Then

  $$a \equiv g^k \pmod{m}, \quad \text{for some } k = 1, 2, \ldots, \varphi(m).$$

  Hence,

  $$\exp_m(g^k) = \exp_m(a) = \varphi(m).$$

  The lemma used above implies $(k, \varphi(m)) = 1$.

  Therefore every primitive root is a member of S.

  But S contains $\varphi(\varphi(m))$ incongruent members mod m.

  This completes the proof.

Subsection 10

The Index Calculus

The Index

- Suppose m has a primitive root g.
- The numbers
$$1, g, g^2, \dots, g^{\varphi(m)-1}$$
form a reduced residue system mod m.
- If $(a, m) = 1$, there is a unique integer k, $0 \leq k \leq \varphi(m) - 1$, such that
$$a \equiv g^k \pmod{m}.$$
- This integer is called the **index of** a **to the base** $g \pmod{m}$.
- We write
$$k = \mathrm{ind}_g a$$
or simply $k = \mathrm{ind} a$ if the base g is understood.

Properties of Indices

- Indices have properties analogous to those of logarithms.

Theorem

Let g be a primitive root mod m. If $(a,m)=(b,m)=1$, we have:

(a) $\text{ind}(ab) \equiv \text{ind} a + \text{ind} b \pmod{\varphi(m)}$.

(b) $\text{ind} a^n \equiv n \text{ind} a \pmod{\varphi(m)}$ if $n \geq 1$.

(c) $\text{ind} 1 = 0$ and $\text{ind} g = 1$.

(d) $\text{ind}(-1) = \varphi(m)/2$ if $m > 2$.

(e) Suppose g' is also a primitive root mod m.

Then $\text{ind}_g a \equiv \text{ind}_{g'} a \cdot \text{ind}_g g' \pmod{\varphi(m)}$.

- The proof is relatively easy.

Linear Congruences and Indices

- Suppose m has a primitive root.
- Let $(a, m) = (b, m) = 1$.
- The linear congruence $ax \equiv b \pmod{m}$ is equivalent to

$$\text{ind} a + \text{ind} x \equiv \text{ind} b \pmod{\varphi(m)}.$$

- So the unique solution of the former satisfies the congruence

$$\text{ind} x \equiv \text{ind} b - \text{ind} a \pmod{\varphi(m)}.$$

Example

- Consider the linear congruence

$$9x \equiv 13 \pmod{47}.$$

The corresponding index relation is

$$\mathrm{ind}x \equiv \mathrm{ind}13 - \mathrm{ind}9 \pmod{46}.$$

Using index tables, we find, for $p = 47$,

$$\begin{array}{rcl} \mathrm{ind}13 & = & 11, \\ \mathrm{ind}9 & = & 40. \end{array}$$

So

$$\mathrm{ind}x \equiv 11 - 40 \equiv -29 \equiv 17 \pmod{46}.$$

Again from a table we find $x \equiv 38 \pmod{47}$.

Example: Binomial Congruences and Index Tables

- A congruence of the form
$$x^n \equiv a \pmod{m}$$
is called a **binomial congruence**.
- If m has a primitive root and if $(a, m) = 1$ it is equivalent to the congruence
$$n\text{ind}x \equiv \text{ind}a \pmod{\varphi(m)}.$$
- The latter is linear in the unknown ind$x$.
- The linear congruence has a solution if, and only if,
$$\text{ind}a \text{ is divisible by } d = (n, \varphi(m)).$$
- Moreover, if this holds, it has exactly d solutions.

Example

- Consider the binomial congruence

$$x^8 \equiv a \pmod{17}.$$

The corresponding index relation is

$$8\text{ind}x \equiv \text{ind}a \pmod{16}.$$

In this example $d = (8, 16) = 8$.

An index table shows that 1 and 16 are the only numbers mod 17 whose index is divisible by 8.

  - $\text{ind}1 = 0$;
  - $\text{ind}16 = 8$.

Hence there are no solutions if $a \not\equiv 1$ or $a \not\equiv 16 \pmod{17}$.

Example (Cont'd)

- We look at the two cases, where a solution exists.
  - Suppose $a = 1$.
    We get
    $$8\text{ind}x \equiv 0 \pmod{16}.$$
    This has exactly eight solutions mod 16.
    They are those x whose index is even,
    $$x \equiv 1, 2, 4, 8, 9, 13, 15, 16 \pmod{17}.$$
    These, of course, are the quadratic residues of 17.
  - Suppose $a = 16$.
    We get
    $$8\text{ind}x \equiv 8 \pmod{16}.$$
    This has also exactly eight solutions mod 16.
    They are those x whose index is odd.
    That is, they are the quadratic nonresidues of 17,
    $$x \equiv 3, 5, 6, 7, 10, 11, 12, 14 \pmod{17}.$$

Exponential Congruences and Index Tables

- An exponential congruence is one of the form
$$a^x \equiv b \pmod{m}.$$
- Suppose m has a primitive root.
- If $(a, m) = (b, m) = 1$, this is equivalent to the linear congruence
$$x \text{ind} a \equiv \text{ind} b \pmod{\varphi(m)}.$$
- Let $d = (\text{ind} a, \varphi(m))$.
- Then the linear congruence has a solution if, and only if,
$$d \mid \text{ind} b.$$
- In that case, there are exactly d solutions.

Example

- Consider the exponential congruence

$$25^x \equiv 17 \pmod{47}.$$

We have:
  - $\text{ind}25 = 2$;
  - $\text{ind}17 = 16$;
  - $d = (2, 46) = 2$.

Therefore, the linear congruence is

$$2x \equiv 16 \pmod{46}.$$

It has two solutions, $x \equiv 8$ and $31 \pmod{46}$.

These are also the solutions of the given exponential congruence.

Subsection 11

Primitive Roots and Dirichlet Characters

Primitive Roots and Dirichlet Characters (p^α)

- Primitive roots and indices can be used to construct explicitly all the Dirichlet characters mod m.
- We start with modulus p^α, where p is an odd prime and $\alpha \geq 1$.
- By a previous theorem, we may find g, which is:
  - A primitive root mod p;
  - A primitive root mod p^β, for all $\beta \geq 1$.
- Suppose $(n, p) = 1$.
- Let

$$b(n) = \text{ind}_g n \pmod{p^\alpha}.$$

- Then $b(n)$ is the unique integer satisfying

$$n \equiv g^{b(n)} \pmod{p^\alpha}, \quad 0 \leq b(n) < \varphi(p^\alpha).$$

Primitive Roots and Dirichlet Characters (p^α Cont'd)

- For $h = 0, 1, 2, \ldots, \varphi(p^\alpha) - 1$, define χ_h by the relations

$$\chi_h(n) = \begin{cases} e^{2\pi i h b(n)/\varphi(p^\alpha)}, & \text{if } p \nmid n \\ 0, & \text{if } p \mid n \end{cases}.$$

- Using the properties of indices, we may verify that:
  - χ_h is completely multiplicative;
  - χ_h is periodic with period p^α.
- So χ_h is a Dirichlet character mod p^α.
- Moreover, χ_0 is the principal character.

Primitive Roots and Dirichlet Characters (p^α Cont'd)

- Note that
$$\chi_h(g) = e^{2\pi i h/\varphi(p^\alpha)}.$$
- The characters
$$\chi_0, \chi_1, \cdots, \chi_{\varphi(p^\alpha)-1}$$
take distinct values at g.
- Therefore,
$$\chi_0, \chi_1, \cdots, \chi_{\varphi(p^\alpha)-1}$$
are distinct characters.
- But there are $\varphi(p^\alpha)$ such functions.
- So they represent all the Dirichlet characters mod p^α.
- The same construction works for the modulus 2^α if $a = 1$ or $a = 2$, using $g = 3$ as the primitive root.

Primitive Roots and Dirichlet Characters (Odd)

- Suppose, now, that
$$m = p_1^{\alpha_1} \cdots p_r^{\alpha_r},$$
where the p_i are distinct odd primes.
- Let χ_i be a Dirichlet character mod p.
- Then the product
$$\chi = \chi_1 \cdots \chi_r$$
is a Dirichlet character mod m.
- We have $\varphi(m) = \varphi(p_1^{\alpha_1}) \cdots \varphi(p_r^{\alpha_r})$.
- So we get $\varphi(m)$ such characters as each χ_i runs through the $\varphi(p_i^{\alpha_i})$ characters mod $p_i^{\alpha_i}$.
- In this way, one has an explicit construction of all characters mod m, for every odd modulus m.

Primitive Roots and Dirichlet Characters ($2^\alpha, \alpha \geq 3$)

Theorem

Assume $\alpha \geq 3$. Then for every odd integer n, there is a uniquely determined integer $b(n)$, with $1 \leq b(n) \leq \varphi(2^\alpha)/2$, such that

$$n \equiv (-1)^{(n-1)/2} 5^{b(n)} \pmod{2^\alpha}.$$

- Let $f = \exp_{2^\alpha}(5)$.
  We have
  $$5^f \equiv 1 \pmod{2^\alpha}.$$
  We will show that $f = \varphi(2^\alpha)/2$.
  We have $f \mid \varphi(2^\alpha) = 2^{\alpha-1}$. So $f = 2^\beta$, for some $\beta \leq \alpha - 1$.
  By a previous theorem, $5^{\varphi(2^\alpha)/2} \equiv 1 \pmod{2^\alpha}$.
  Hence, $f \leq \varphi(2^\alpha)/2 = 2^{\alpha-2}$. Therefore, $\beta \leq \alpha - 2$.
  We will show that $\beta = \alpha - 2$.

Primitive Roots and Dirichlet Characters (2^α Cont'd)

Claim: $\beta = \alpha - 2$.

Raise both sides of $5 = 1 + 2^2$ to the $f = 2^\beta$ power,

$$5^f = (1+2^2)^{2^\beta} = 1 + 2^{\beta+2} + r2^{\beta+3} = 1 + 2^{\beta+2}(1+2r),$$

where r is an integer.

Hence,

$$5^f - 1 = 2^{\beta+2}t, \quad \text{with } t \text{ is odd.}$$

On the other hand, $2^\alpha \mid (5^f - 1)$.

So $\alpha \leq \beta + 2$.

Equivalently, $\beta \geq \alpha - 2$.

Hence, $\beta = \alpha - 2$ and $f = 2^{\alpha-2} = \varphi(2^\alpha)/2$.

Primitive Roots and Dirichlet Characters (2^α Cont'd)

- We conclude that the numbers
$$5, 5^2, \ldots, 5^f$$
are incongruent mod 2^α.
Also each is $\equiv 1 \pmod 4$, since $5 \equiv 1 \pmod 4$.
Similarly, the numbers
$$-5, -5^2, \ldots, -5^f$$
are incongruent mod 2^α.
Moreover, each is $\equiv 3 \pmod 4$, since $-5 \equiv 3 \pmod 4$.
There are $2f = \varphi(2^\alpha)$ numbers in these lists combined.
Moreover, we cannot have $5^a = -5^b \pmod{2^\alpha}$, because this would imply $1 \equiv -1 \pmod 4$.
So the numbers represent $\varphi(2^\alpha)$ incongruent odd numbers mod 2^α.

Characters Modulo $2^\alpha, \alpha \geq 3$

- Let
$$f(n) = \begin{cases} (-1)^{(n-1)/2}, & \text{if } n \text{ is odd} \\ 0, & \text{if } n \text{ is even} \end{cases}$$
Let
$$g(n) = \begin{cases} e^{2\pi i b(n)/2^{\alpha-2}}, & \text{if } n \text{ is odd} \\ 0, & \text{if } n \text{ is even} \end{cases}$$
where $b(n)$ is the integer given by the preceding theorem.

Then it is easy to verify that each of f and g is a character mod 2^α.

So is each product
$$\chi_{a,c}(n) = f(n)^a g(n)^c,$$
where $a = 1, 2$ and $c = 1, 2, \ldots, \varphi(2^\alpha)/2$.

Moreover, these $\varphi(2^\alpha)$ characters are distinct so they represent all the characters mod 2^α.

Primitive Roots and Dirichlet Characters

- Finally, suppose
$$m = 2^\alpha Q,$$
where Q is odd.
- Form the products
$$\chi = \chi_1 \chi_2,$$
where:
  - χ_1 runs through the $\varphi(2^\alpha)$ characters mod 2^α;
  - χ_2 runs through the $\varphi(Q)$ characters mod Q.
- In this way, we obtain all the characters mod m.

Subsection 12

Real-Valued Dirichlet Characters mod p^α

Real-Valued Dirichlet Characters mod p^α

- Let χ be a real-valued Dirichlet character mod m.
- If $(n, m) = 1$, the number $\chi(n)$ is both a root of unity and real.
- It follows that $\chi(n) = \pm 1$.

Theorem

For an odd prime p and $\alpha \geq 1$, consider the $\varphi(p^\alpha)$ Dirichlet characters χ_h mod p^α given by

$$\chi_h(n) = \begin{cases} e^{2\pi i h b(n)/\varphi(p^\alpha)}, & \text{if } p \nmid n \\ 0, & \text{if } p \mid n \end{cases}$$

Then χ_h is real if, and only if, $h = 0$ or $h = \varphi(p^\alpha)/2$.
Hence, there are exactly two real characters mod p^α.

Real-Valued Dirichlet Characters mod p^α (Cont'd)

- In general, we have

$$e^{\pi iz} = \pm 1 \quad \text{if, and only if,} \quad z \text{ is an integer.}$$

If $p \nmid n$ we have

$$\chi_h(n) = e^{2\pi ihb(n)/\varphi(p^\alpha)}.$$

So $\chi_h(n) = \pm 1$ if, and only if, $\varphi(p^\alpha) \mid 2hb(n)$.

If $h = 0$ or $h = \varphi(p^\alpha)/2$, this condition is satisfied for all n.

Real-Valued Dirichlet Characters mod p^α (Cont'd)

- Conversely, suppose

$$\varphi(p^\alpha) \mid 2hb(n), \quad \text{for all } n.$$

Then, when $b(n) = 1$, we have

$$\varphi(p^\alpha) \mid 2h \quad \text{or} \quad \varphi(p^\alpha)/2 \mid h.$$

But 0 and $\varphi(p^\alpha)/2$ are the only multiples of $\varphi(p^\alpha)/2$ less than $\varphi(p^\alpha)$.
It follows that $h = 0$ or $h = \varphi(p^\alpha)/2$.

Note:

- The character corresponding to $h = 0$ is the principal character.
- When $\alpha = 1$, the quadratic character $\chi(n) = (n|p)$ is the only other real character mod p.

Real-Valued Dirichlet Characters mod 2^α

- For the moduli $m = 1, 2$ and 4, all the Dirichlet characters are real.
- Recall the definitions

$$f(n) = \begin{cases} (-1)^{(n-1)/2}, & n \text{ odd}, \\ 0, & n \text{ even}, \end{cases} \qquad g(n) = \begin{cases} e^{2\pi i b(n)/2^{\alpha-2}}, & n \text{ odd}, \\ 0, & n \text{ even}. \end{cases}$$

Theorem

If $\alpha \geq 3$, consider the $\varphi(2^\alpha)$ Dirichlet characters $\chi_{a,c}$ mod 2^α given by

$$\chi_{a,c}(n) = f(n)^a g(n)^c,$$

where $a = 1, 2$ and $c = 1, 2, \ldots, \varphi(2^\alpha)/2$.
Then $\chi_{a,c}$ is real if and only if, $c = \varphi(2^\alpha)/2$ or $c = \varphi(2^\alpha)/4$.
Hence, there are exactly four real characters mod 2^α if $\alpha \geq 3$.

Real-Valued Dirichlet Characters mod 2^α (Cont'd)

- If $\alpha \geq 3$ and n is odd we have

$$\chi_{a,c}(n) = f(n)^a g(n)^c,$$

where:

  - $f(n) = \pm 1$;
  - $g(n)^c = e^{2\pi i c b(n)/2^{\alpha-2}}$, with $1 \leq c \leq 2^{\alpha-2}$.

This is ± 1 if, and only if, $2^{\alpha-2} \mid 2cb(n)$ or $2^{\alpha-3} \mid cb(n)$.

But $\varphi(2^\alpha) = 2^{\alpha-1}$. So, if $c = \varphi(2^\alpha)/2 = 2^{\alpha-2}$ or $c = \varphi(2^\alpha)/4 = 2^{\alpha-3}$, the condition is satisfied.

Conversely, suppose $2^{\alpha-3} \mid cb(n)$, for all n.

Then $b(n) = 1$ requires $2^{\alpha-3} \mid c$.

So $c = 2^{\alpha-3}$ or $2^{\alpha-2}$, since $1 \leq c \leq 2^{\alpha-2}$.

Subsection 13

Primitive Dirichlet Characters mod p^α

Review on Primitive Characters

- We proved that every nonprincipal character χ mod p is primitive if p is prime.
- Now we determine all the primitive Dirichlet characters mod p^α.
- Recall that an induced modulus mod k is a divisor d of k, such that

$$\chi(n) = 1 \text{ whenever } (n, k) = 1 \text{ and } n \equiv 1 \pmod{d}.$$

- χ is primitive mod k if, and only if, χ has no induced modulus $d < k$.
- Suppose $k = p^\alpha$ and χ is imprimitive mod p^α.

  Then one of the divisors $1, p, \ldots, p^{\alpha-1}$ is an induced modulus.

  Hence $p^{\alpha-1}$ is an induced modulus.
- Therefore, χ is primitive mod p^α if, and only if, $p^{\alpha-1}$ is not an induced modulus for χ.

Primitive Dirichlet Characters mod p^α

Theorem

For an odd prime p and $\alpha \geq 2$, consider the $\varphi(p^\alpha)$ Dirichlet characters mod p^α,

$$\chi_h(n) = \begin{cases} e^{2\pi i h b(n)/\varphi(p^\alpha)}, & \text{if } p \nmid n \\ 0, & \text{if } p \mid n \end{cases}.$$

Then χ_h is primitive mod p^α if, and only if, $p \nmid h$.

- We will show that $p^{\alpha-1}$ is an induced modulus if, and only if, $p \mid h$.

  If $p \nmid n$, we have

  $$\chi_h(n) = e^{2\pi i h b(n)/\varphi(p^\alpha)},$$

  where $n \equiv g^{b(n)} \pmod{p^\alpha}$ and g is a primitive root mod p^β, for all $\beta \geq 1$. Therefore, $g^{b(n)} \equiv n \pmod{p^{\alpha-1}}$.

Primitive Dirichlet Characters mod p^α (Cont'd)

- If $n \equiv 1 \pmod{p^{\alpha-1}}$, then $g^{b(n)} \equiv 1 \pmod{p^{\alpha-1}}$.
  Since g is a primitive root of $p^{\alpha-1}$, $\varphi(p^{\alpha-1}) \mid b(n)$.
  So, for some integer t,
  $$b(n) = t\varphi(p^{\alpha-1}) = t\varphi(p^\alpha)/p.$$
  Therefore, $\chi_h(n) = e^{2\pi iht/p}$.
  - Suppose $p \mid h$. Then $\chi_h(n) = 1$.
    Hence χ_h is imprimitive mod p^α.
  - Suppose $p \nmid h$. Take $n = 1 + p^{\alpha-1}$.
    Then $n \equiv 1 \pmod{p^{\alpha-1}}$ but $n \not\equiv 1 \pmod{p^\alpha}$.
    So $0 < b(n) < \varphi(p^\alpha)$.
    Therefore, $p \nmid t$, $p \nmid ht$ and $\chi_h(n) \neq 1$.
    This shows that χ_h is primitive, if $p \nmid h$.

Remarks

- When $m = 1$ or 2, there is only one character χ mod m, the principal character.
- If $m = 4$, there are two characters mod 4:
  - The principal character;
  - The primitive character f given by

$$f(n) = \begin{cases} (-1)^{(n-1)/2}, & \text{if } n \text{ is odd,} \\ 0, & \text{if } n \text{ is even.} \end{cases}$$

Primitive Dirichlet Characters mod 2^α

Theorem

If $a \geq 3$, consider the $\varphi(2^\alpha)$ Dirichlet characters $\chi_{a,c}$ mod 2^a given by

$$\chi_{a,c}(n) = f(n)^a g(n)^c.$$

Then $\chi_{a,c}$ is primitive mod 2^α if, and only if, c is odd.

- The proof is similar to that of the preceding theorem.

Primitive Dirichlet Characters for Composite Modulus

- To determine the primitive characters for a composite modulus k we write
$$k = p_1^{\alpha_1} \cdots p_r^{\alpha_r}.$$
- Then every character χ mod k can be factored in the form
$$\chi = \chi_1 \cdots \chi_r,$$
where each χ_i is a character mod $p_i^{\alpha_i}$.
- Moreover, it turns out that χ is primitive mod k if, and only if, each χ_i is primitive mod $p_i^{\alpha_i}$.
- Therefore, we have a complete description of all primitive characters mod k.