# 8.4 The Theory of Indices

Note Title 4/3/2006

1. Find The index of 5 relative to each of the primitive roots of 13.

There are $\phi(\phi(13)) = \phi(12) = 4$ prim. roots of 13. 2 is a primitive root as $2^{12} \equiv 1 \pmod{13}$ and $2^1, 2^2, 2^3, 2^4, 2^5, 2^6 \not\equiv 1 \pmod{13}$.
$\therefore$ Other prim. roots are found from $2^K$, $1 \le K \le 12$, s.t. $\gcd(K, 12) = 1$, by Th. 8.3 and 8.4.

$\gcd(K, 12) = 1 \Rightarrow K = 1, 5, 7, 11.$

$2^1 \equiv 2,\ 2^5 \equiv 6,\ 2^7 \equiv 11,\ 2^{11} \equiv 7 \pmod{13}.$

$\therefore$ Prim. roots of 13 are: 2, 6, 7, 11.

Construct powers of roots till get 5.

2: $2^1 \equiv 2,\ 2^2 \equiv 4,\ 2^3 \equiv 8,\ 2^4 \equiv 3,\ 2^5 \equiv 6,\ 2^6 \equiv 12,\ 2^7 \equiv 11,\ 2^8 \equiv 9,$
$\underline{2^9 \equiv 5}$

6: $6^1 \equiv 6,\ 6^2 \equiv -3 \equiv 10,\ 6^3 \equiv -18 \equiv 8,\ 6^4 \equiv 48 \equiv 9,\ 6^5 \equiv 2,$
$6^6 \equiv 12 \equiv -1,\ 6^7 \equiv -6 \equiv 7,\ 6^8 \equiv -36 \equiv 3,\ \underline{6^9} \equiv 18 \equiv 5$

7: $7^1 \equiv 7,\ 7^2 \equiv 10 \equiv -3,\ \underline{7^3} \equiv -21 \equiv 5$

$11: 11^1 \equiv 11 \equiv -2,\ 11^2 \equiv -22 \equiv 4,\ \underline{11^3} \equiv 44 \equiv 5$

$\therefore\ ind_2 5 = 9,\ ind_6 5 = 9,\ ind_7 5 = 3,\ ind_{11} 5 = 3$

2. Use a table of indices for a prim. root of 11, solve the following congruences:
(a) $7x^3 \equiv 3 \pmod{11}$
(b) $3x^4 \equiv 5 \pmod{11}$
(c) $x^8 \equiv 10 \pmod{11}$

By table on p. 166, 2 is a prim. root of 11.

$2^1 \equiv 2,\ 2^2 \equiv 4,\ 2^3 \equiv 8,\ 2^4 \equiv 5,\ 2^5 \equiv 10 \equiv -1,\ 2^6 \equiv -2 \equiv 9$
$2^7 \equiv 7,\ 2^8 \equiv 3,\ 2^9 \equiv 6,\ 2^{10} \equiv 1$

| $a$ | 1 | 2 | 3 | 4 | 5 | 6 | 7 | 8 | 9 | 10 |
|---|---|---|---|---|---|---|---|---|---|---|
| $ind_2 a$ | 10 | 1 | 8 | 2 | 4 | 9 | 7 | 3 | 6 | 5 |

(a) $7x^3 \equiv 3 \pmod{11}$
gcd$(3,11) = 1$, and 11 has a prim. root

$7x^3 \equiv 3 \pmod{11} \iff ind_2 7 + 3\, ind_2 x \equiv ind_2 3 \pmod{10}$

$\iff 7 + 3\, ind_2 x \equiv 8 \pmod{10}$

$\iff 3\, ind_2 x \equiv 1 \pmod{10}$

Since $\gcd(3,10)=1$, and $1 \mid 1$,
Then by Th. 4.7, There is one incongruent solution.
$ind_2 x \equiv 7 \pmod{10}$ is a solution.

From table, $x = 7$

$\therefore$ $\underline{x \equiv 7 \pmod{11}}$

(b) $3x^4 \equiv 5 \pmod{11}$

$\gcd(5,11)=1$, and 11 has a prim. root.

$3x^4 \equiv 5 \pmod{11} \Leftrightarrow ind_2 3 + 4\, ind_2 x \equiv ind_2 5 \pmod{10}$

$\Leftrightarrow 8 + 4\, ind_2 x \equiv 4 \pmod{10}$

$\Leftrightarrow 4\, ind_2 x \equiv 6 \pmod{10}$

$\gcd(4,10)=2$, and $2 \mid 6$, so
2 incongruent solutions.

$4\, ind_2 x \equiv 6 \pmod{10} \Rightarrow$
$2\, ind_2 x \equiv 3 \pmod{5} \Rightarrow$
$ind_2 x = 4, 9$

$\therefore\ x \equiv 5, 6 \pmod{11}$

(c) $x^8 \equiv 10 \pmod{11}$

$\gcd(10, 11) = 1$, and 11 has a prim. root

$x^8 \equiv 10 \pmod{11} \Leftrightarrow 8\,\mathrm{ind}_2 x \equiv \mathrm{ind}_2 10 \pmod{10}$

$\Leftrightarrow 8\,\mathrm{ind}_2 x \equiv 5 \pmod{10}$

But $\gcd(8, 10) = 2$ and $2 \nmid 5$

$\therefore$ by Th. 4.7, no solution to $8\,\mathrm{ind}_2 x \equiv 5 \pmod{10}$

$\therefore$ no solution to $x^8 \equiv 10 \pmod{11}$

3. The following is a table of indices for the prime 17 relative to the primitive root 3:

| $a$ | 1 | 2 | 3 | 4 | 5 | 6 | 7 | 8 | 9 | 10 | 11 | 12 | 13 | 14 | 15 | 16 |
|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|
| $\mathrm{ind}_3\, a$ | 16 | 14 | 1 | 12 | 5 | 15 | 11 | 10 | 2 | 3 | 7 | 13 | 4 | 9 | 6 | 8 |

With the aid of this table, solve the following congruences:

(a) $x^{12} \equiv 13 \pmod{17}$.
(b) $8x^5 \equiv 10 \pmod{17}$.
(c) $9x^8 \equiv 8 \pmod{17}$.
(d) $7^x \equiv 7 \pmod{17}$.

(a) $x^{12} \equiv 13 \pmod{17}$ $\qquad \gcd(13, 17) = 1$

$\therefore\ 12\,\mathrm{ind}_3 x \equiv \mathrm{ind}_3 13 \pmod{16}$, $\mathrm{ind}_3 13 = 4$

$\therefore\ 12\,\mathrm{ind}_3 x \equiv 4 \pmod{16}$, $\gcd(12,16) = 4$

$\therefore$ 4 incongruent solutions.

Dividing by 4,

$3\,\mathrm{ind}_3 x \equiv 1 \pmod 4$

$\therefore\ \mathrm{ind}_3 x = 3, 7, 11, 15$

$\therefore\ x = 10, 11, 7, 6$ from table

$\therefore\ x \equiv 6, 7, 10, 11 \pmod{17}$

(b) $8x^5 \equiv 10 \pmod{17}$ $\quad \gcd(10,17) = 1$

$\therefore\ \mathrm{ind}_3 8 + 5\,\mathrm{ind}_3 x \equiv \mathrm{ind}_3 10 \pmod{16}$

$\therefore\ 10 + 5\,\mathrm{ind}_3 x \equiv 3 \pmod{16}$

$5\,\mathrm{ind}_3 x \equiv -7 \pmod{16}$ $\quad \gcd(5,16) = 1$

$\therefore$ 1 solution

$\therefore\ 15\,\mathrm{ind}_3 x \equiv -21$

$-\mathrm{ind}_3 x \equiv -21$

$\mathrm{ind}_3 x \equiv 21 \equiv 5$, $\therefore\ x = 5$ (from table).

$\therefore\ x \equiv 5 \pmod{17}$

(c) $9x^8 \equiv 8 \pmod{17}$ $\quad \gcd(8,17)=1$

$\mathrm{ind}_3 9 + 8\,\mathrm{ind}_3 x \equiv \mathrm{ind}_3 8 \pmod{16}$

$\therefore\ 2 + 8\,\mathrm{ind}_3 x \equiv 10 \pmod{16}$

$8\,\mathrm{ind}_3 x \equiv 8 \pmod{16}$ $\quad \gcd(8,16)=8$

$\therefore$ 8 incongruent solutions

$\therefore\ \mathrm{ind}_3 x \equiv 1 \pmod{2}$

$\therefore\ \mathrm{ind}_3 x = 1, 3, 5, 7, 9, 11, 13, 15$

$\therefore\ x \equiv 3, 10, 5, 11, 14, 7, 12, 6 \pmod{17}$

(d) $7^x \equiv 7 \pmod{17}$ $\quad \gcd(7,17)=1$

$\therefore\ x\,\mathrm{ind}_3 7 \equiv \mathrm{ind}_3 7 \pmod{16}$

$11x \equiv 11 \pmod{16}$, $\gcd(11,16)=1$, so just one solution

$\therefore\ x \equiv 1 \pmod{16}$ [don't need table at this point].

4. Find the remainder when $3^{24} \cdot 5^{13}$ is divided by 17.

$3^{24} \cdot 5^{13} \equiv x \pmod{17}$. $\gcd(1,17)=1$, so just 1 solution

Use 3 as a prim. root of 17, and use table in #3 above.

$\therefore 24 \, \mathrm{ind}_3 3 + 13 \, \mathrm{ind}_3 5 \equiv \mathrm{ind}_3 x \pmod{16}$

$\therefore 24(1) + 13(5) \equiv \mathrm{ind}_3 x \pmod{16}$

$89 \equiv 9 \equiv \mathrm{ind}_3 x \pmod{16}$, $x = 14$ from table

$\therefore x \equiv 14 \pmod{17}$

$\therefore$ remainder $= \underline{14}$

5. If $r$ and $r'$ are both primitive roots of the odd prime $p$, show that for $\gcd(a, p) = 1$

$$\mathrm{ind}_{r'}\, a \equiv (\mathrm{ind}_r\, a)(\mathrm{ind}_{r'}\, r) \pmod{p-1}$$

This corresponds to the rule for changing the base of logarithms.

Pf: Let $x = \mathrm{ind}_{r'} a \pmod{p}$

$y = \mathrm{ind}_r a \pmod{p}$

$z = \mathrm{ind}_{r'} r \pmod{p}$

$\therefore$ By def., $(r')^x \equiv a \pmod p$,

$r^y \equiv a \pmod p$, and

$(r')^z \equiv r \pmod p \Rightarrow (r')^{zy} \equiv r^y \pmod p$

$\therefore (r')^x \equiv r^y \equiv (r')^{zy} \pmod p$

By Th. 8.2, $x \equiv zy \pmod{p-1}$

$\therefore \text{ind}_{r'} a \equiv (\text{ind}_r a)(\text{ind}_{r'} r) \pmod{p-1}$

6. (a) Construct a table of indices for the prime 17 with respect to the primitive root 5 [*Hint:* By the previous problem, $\text{ind}_5\, a \equiv 13\, \text{ind}_3\, a \pmod{16}$.]
(b) Solve the congruences in Problem 3, using the table in part (a).

(a) By #5, $\text{ind}_5 a = (\text{ind}_5 3)(\text{ind}_3 a) \pmod{16}$

Let $\text{ind}_5 3 = x$. $\therefore 5^x \equiv 3 \pmod{17}$

$\therefore x \,\text{ind}_3 5 \equiv \text{ind}_3 3 \equiv 1 \pmod{16}$

From table in #3, $\text{ind}_3 5 = 5$

$\therefore 5x \equiv 1 \pmod{16}$, $\gcd(5,16) = 1$, so just one solution (mod 16). $\therefore 15x \equiv 3$, $-x \equiv 3$, $x \equiv 13$

$\therefore \operatorname{ind}_5 3 = 13$

$\therefore \operatorname{ind}_5 a \equiv 13 \operatorname{ind}_3 a \pmod{16}$

| $a$ | 1 | 2 | 3 | 4 | 5 | 6 | 7 | 8 | 9 | 10 | 11 | 12 | 13 | 14 | 15 | 16 |
|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|
| $\operatorname{ind}_3 a$ | 16 | 14 | 1 | 12 | 5 | 15 | 11 | 10 | 2 | 3 | 7 | 13 | 4 | 9 | 6 | 8 |
| $13 \operatorname{ind}_3 a$ | 208 | 182 | 13 | 156 | 65 | 195 | 143 | 130 | 26 | 39 | 91 | 169 | 52 | 117 | 78 | 104 |
| $\operatorname{ind}_5 a$ | 16 | 6 | 13 | 12 | 1 | 3 | 15 | 2 | 10 | 7 | 11 | 9 | 4 | 5 | 14 | 8 |

(6) $x^{12} \equiv 13 \pmod{17}$

$12 \operatorname{ind}_5 x \equiv \operatorname{ind}_5 13 \pmod{16}$,

$12 \operatorname{ind}_5 x \equiv 4 \pmod{16}$, $\gcd(12,16) = 4$ solutions

$3 \operatorname{ind}_5 x \equiv 1 \pmod 4$, $\operatorname{ind}_5 x = 3, 7, 11, 15$

$\therefore x \equiv 6, 10, 11, 7 \pmod{17}$ as in #3

$8x^5 \equiv 10 \pmod{17}$

$\operatorname{ind}_5 8 + 5 \operatorname{ind}_5 x \equiv \operatorname{ind}_5 10 \pmod{16}$

$2 + 5 \operatorname{ind}_5 x \equiv 7$

$5 \operatorname{ind}_5 x \equiv 5 \pmod{16}$ $\gcd(5,16) = 1$ solution

$\therefore \operatorname{ind}_5 x \equiv 1 \pmod{16}$

$x \equiv 5 \pmod{17}$, as in #3

$9x^8 \equiv 8 \pmod{17}$

$\operatorname{ind}_5 9 + 8 \operatorname{ind}_5 x \equiv \operatorname{ind}_5 8 \pmod{16}$

$10 + 8\,\mathrm{ind}_5 x \equiv 2 \pmod{16}$

$8\,\mathrm{ind}_5 x \equiv -8 \equiv 8 \pmod{16}$ gcd(8, 16) = 8 solutions

$\mathrm{ind}_5 x \equiv 1 \pmod{2}$

$\mathrm{ind}_5 x = 1, 3, 5, 7, 9, 11, 13, 15$

$\therefore x \equiv 5, 6, 14, 10, 12, 11, 3, 7 \pmod{17}$, as in #3

$7^x \equiv 7 \pmod{17}$

$x\,\mathrm{ind}_5 7 \equiv \mathrm{ind}_5 7 \pmod{16}$

$15x \equiv 15 \pmod{16}$, gcd(15, 16) = 1 solution

$x \equiv 1 \pmod{16}$, same as in #3

7. If $r$ is a primitive root of the odd prime $p$, verify that

$$\mathrm{ind}_r\,(-1) = \mathrm{ind}_r\,(p-1) = \frac{1}{2}(p-1)$$

Pf: (a) Since $-1 \equiv p-1 \pmod{p}$, then

$$\underline{\mathrm{ind}_r(-1) = \mathrm{ind}_r(p-1)}$$

(b) Let $x = \mathrm{ind}_r(p-1)$. Then $r^x \equiv p-1 \pmod{p}$

As $p$ is odd, $p-1$ is even and $\therefore \frac{p-1}{2}$ exists.

$\therefore r^{p-1} \equiv 1 \equiv p^2 - 2p + 1 = (p-1)^2 \pmod{p}$

$\therefore r^{p-1} \equiv (p-1)^2 \pmod{p}$

$\therefore\ r^{\frac{p-1}{2}} \equiv p-1$ or $-(p-1) = -p+1$

if $r^{\frac{p-1}{2}} \equiv -p+1 \equiv 1 \pmod{p}$, Then since $\frac{p-1}{2} < p-1$, $r$ wouldn't have order $p-1$.

$\therefore\ r^{\frac{p-1}{2}} \not\equiv -p+1$

$\therefore\ r^{\frac{p-1}{2}} \equiv p-1 \pmod{p}$

$\therefore$ By def., $\underline{\underline{\operatorname{ind}_r(p-1) = \frac{p-1}{2}}}$

8. (a) Determine the integers $a$ $(1 \le a \le 12)$ s.t. the congruence $ax^4 \equiv b \pmod{13}$ has a solution for $b = 2, 5, 6$.

Note That $\gcd(b, 13) = 1$

$\therefore\ \operatorname{ind} a + 4 \operatorname{ind} x \equiv \operatorname{ind} b \pmod{12}$

$\therefore\ 4 \operatorname{ind} x \equiv \operatorname{ind} b - \operatorname{ind} a \pmod{12}$

$\gcd(4, 12) = 4$, so for a solution to exist,

$4 \mid (\operatorname{ind} b - \operatorname{ind} a)$

$\therefore$ ind $b$ - ind $a$ $= 0, 4$ (or $-4$), $8$ (or $-8$)

(1) ind $b$ - ind $a = 0$, $\therefore$ ind $b =$ ind $a$
$\therefore b \equiv a$, and with $1 \le a \le 12$, $\therefore b = a$
$\therefore a = 2, 5, 6$ when $b = 2, 5, 6$, respectively

(2) ind $b$ - ind $a$ $= 4$ (or $-4$)
Using table of indices for prim. root 2 of 13 (p. 175), $\text{ind}_2 2 = 1$, $\text{ind}_2 5 = 9$, $\text{ind}_2 6 = 5$

$\therefore 1 - \text{ind}_2 a = -4 \Rightarrow \text{ind}_2 a = 5 \Rightarrow a = 6$
$9 - \text{ind}_2 a = 4 \Rightarrow \text{ind}_2 a = 5 \Rightarrow a = 6$
$5 - \text{ind}_2 a = 4, -4 \Rightarrow \text{ind}_2 a = 1, 9 \Rightarrow a = 2, 5$

$\therefore b = 2 : a = 6$
$b = 5 : a = 6$
$b = 6 : a = 2$ or $5$

(3) ind $b$ - ind $a$ $= 8$ (or $-8$)
Using table as in (2) above,

$1 - \text{ind}_2 a = -8$, $\text{ind}_2 a = 9 \Rightarrow a = 5$
$9 - \text{ind}_2 a = 8$, $\text{ind}_2 a = 1 \Rightarrow a = 2$
$5 - \text{ind}_2 a = -8$, $\text{ind}_2 a = 13 \Rightarrow$ no solution

$\therefore$ when $b = 2$, $a = 2, 6$, or $5$

$b = 5$, $a = 5, 6$, or $2$

$b = 6$, $a = 6, 2$, or $5$

(b) Determine the integers $a$ $(1 \le a \le p-1)$ s.t. the congruence $x^4 \equiv a \pmod{p}$ has a solution for $p = 7, 11, 13$.

Construct table of indices for 7, 11

3 is a prim. root of 7, 2 is a prim. root of 11.

$3^1 \equiv 3,\ 3^2 \equiv 2,\ 3^3 \equiv 6,\ 3^4 \equiv 4,\ 3^5 \equiv 5,\ 3^6 \equiv 1 \pmod{7}$

$2^1 \equiv 2,\ 2^2 \equiv 4,\ 2^3 \equiv 8,\ 2^4 \equiv 5,\ 2^5 \equiv 10,\ 2^6 \equiv 9,\ 2^7 \equiv 7,\ 2^8 \equiv 3,$
$2^9 \equiv 6,\ 2^{10} \equiv 1 \pmod{11}$

| $a$ | 1 | 2 | 3 | 4 | 5 | 6 |
|---|---|---|---|---|---|---|
| $ind_3 a$ | 6 | 2 | 1 | 4 | 5 | 3 |

| $a$ | 1 | 2 | 3 | 4 | 5 | 6 | 7 | 8 | 9 | 10 |
|---|---|---|---|---|---|---|---|---|---|---|
| $ind_2 11$ | 10 | 1 | 8 | 2 | 4 | 9 | 7 | 3 | 6 | 5 |

$p = 7$: $x^4 \equiv a \pmod{7}$

$4\, ind\, x \equiv ind\, a \pmod{6}$, $\gcd(4,6) = 2$

$\therefore 2 \mid ind\, a \Rightarrow ind\, a = 2, 4, 6$

$\therefore\ a \equiv 2, 4, 1$

$p = 11$: $x^4 \equiv a \pmod{11}$

$4 \operatorname{ind} x \equiv \operatorname{ind} a \pmod{10}$, $\gcd(4,10) = 2$

$\therefore 2 \mid \operatorname{ind} a$, $\therefore \operatorname{ind} a = 2, 4, 6, 8, 10$

$\therefore\ a \equiv 4, 5, 9, 3, 1$

$p = 13$: $x^4 \equiv a \pmod{13}$

$4 \operatorname{ind} x \equiv \operatorname{ind} a \pmod{12}$, $\gcd(4,12) = 4$

$\therefore 4 \mid \operatorname{ind} a \Rightarrow \operatorname{ind} a = 4, 8, 12$

Use table on p. 175

$\therefore\ a \equiv 3, 9, 1$

9. Employ the corollary to Th. 8.12 to establish that if $p$ is an odd prime, then

(a) $x^2 \equiv -1 \pmod{p}$ is solvable $\Leftrightarrow p \equiv 1 \pmod{4}$

Since $-1 \equiv p-1 \pmod{p}$, and $\gcd(p-1, p) = 1$, then $\gcd(-1, p) = 1$.

Using corollary to Th. 8.12, $x^2 \equiv -1 \pmod{p}$ is

solvable $\iff (-1)^{\frac{p-1}{2}} \equiv 1 \pmod{p}$, as
$2 = \gcd(2, p-1)$ since $p$ is odd.

$(-1)^{\frac{p-1}{2}} = 1$ if $\frac{p-1}{2}$ is even
$-1$ if $\frac{p-1}{2}$ is odd

So, $(-1)^{\frac{p-1}{2}} \equiv 1 \iff (-1)^{\frac{p-1}{2}} = 1 \iff \frac{p-1}{2}$ is even

$\therefore \frac{p-1}{2} = 2k$, some $k$, so $p = 1 + 4k$, or
$p \equiv 1 \pmod{4}$

$\therefore x^2 \equiv 1 \pmod{p}$ solvable $\iff p \equiv 1 \pmod{4}$

(b) $x^4 \equiv -1 \pmod{p}$ is solvable $\iff p \equiv 1 \pmod{8}$

As in (a), $\gcd(-1, p) = 1$. Using corollary to Th. 8.12,

$x^4 \equiv -1 \pmod{p}$ solvable $\iff (-1)^{\frac{p-1}{d}} \equiv 1 \pmod{p}$,
where $d = \gcd(4, p-1)$

If $d = 2$, then as in (a), $p = 1 + 4k$, some $k$,
so $p \equiv 1 \pmod{4}$ and $\therefore p \equiv 1 \pmod{8}$

If $d = 4$, then $\frac{p-1}{4} = 2k$, $p = 1 + 8k$, some $k$,
so $p \equiv 1 \pmod{8}$

$\therefore$ if $(-1)^{\frac{p-1}{d}} \equiv 1 \pmod p$ Then $p \equiv 1 \pmod 8$

But if $p \equiv 1 \pmod 8$, Then $p-1 = 8k$, some $k$,
so
$$(-1)^{\frac{p-1}{d}} = (-1)^{\frac{8k}{d}} = 1 \text{ whether } d = 2 \text{ or } 4,$$
so $(-1)^{\frac{p-1}{d}} \equiv 1 \pmod p$, so $x^4 \equiv -1 \pmod p$ is solvable.

$\therefore x^4 \equiv -1 \pmod p$ solvable $\Leftrightarrow p \equiv 1 \pmod 8$

10. Given The congruence $x^3 \equiv a \pmod p$, where $p \geq 5$ is a prime and $\gcd(a, p) = 1$, prove The following:

(a) If $p \equiv 1 \pmod 6$, Then The congruence has either no solutions or 3 incongruent solutions mod $p$.

Pf: If $p \equiv 1 \pmod 6$, Then $p-1 = 6k$, some $k$.
$\therefore \gcd(3, 6k) = 3$.

Since $p$ is prime, it has a prim. root, so
$$x^3 \equiv a \pmod p \Leftrightarrow 3 \,\text{ind}\, x \equiv \text{ind}\, a \pmod{6k}$$

By Th. 4.7, if $3 \nmid \text{ind}\, a$, there is no solution. If $3 \mid \text{ind}\, a$, then there are 3 incongruent solutions.

(b) If $p \equiv 5 \pmod 6$, then the congruence has a unique solution mod $p$.

Pf: If $p \equiv 5 \pmod 6$, then $p-5 = 6k$, some $k$.
$\therefore p-1 = 6k+4 = 2(3k+2)$

$\therefore \gcd(3, p-1) = \gcd(3, 2(3k+2)) = 1$.
since $\gcd(3, 3k+2) = 1$ for all $k$.

$\therefore x^3 \equiv a \pmod p \Leftrightarrow 3\,\text{ind}\, x \equiv \text{ind}\, a \pmod{p-1}$

$\Leftrightarrow 3\,\text{ind}\, x \equiv \text{ind}\, a \pmod{2(3k+2)}$

Since $1 \mid \text{ind}\, a$, by Th. 4.7, the latter congruence has a unique solution mod $p-1$, and so $x^3 \equiv a \pmod p$ has a unique solution mod $p$.

11. Show that the congruence $x^3 \equiv 3 \pmod{19}$ has no solutions, whereas $x^3 \equiv 11 \pmod{19}$ has three incongruent solutions.

(1) $x^3 \equiv 3 \pmod{19}$, $\gcd(3,19)=1$

Since $\gcd(3, \phi(19)) = \gcd(3,18) = 3$, by Th. 8.12,

since $3^{\frac{18}{3}} = 3^6 = 3^3 \cdot 3^3 \equiv 8 \cdot 8 \equiv 7 \not\equiv 1 \pmod{19}$,

Then $x^3 \equiv 3 \pmod{19}$ has no solutions.

(2) $x^3 \equiv 11 \pmod{19}$, $\gcd(11,19)=1$

Since $\gcd(3, \phi(19)) = 3$, by Th. 8.12, since

$11^{\frac{18}{3}} = 11^6 \equiv (-8)^6 \equiv (64)^3 \equiv 7^3 \equiv 49 \cdot 7 \equiv 11 \cdot 7 \equiv 1 \pmod{19}$,

Then there are $3 = \gcd(3, \phi(19))$ incongruent solutions.

12. Determine whether the two congruences $x^5 \equiv 13 \pmod{23}$ and $x^7 \equiv 15 \pmod{29}$ are solvable.

(1) $x^5 \equiv 13 \pmod{23}$

Using Th. 8.12, $\gcd(13,23)=1$, and $\gcd(5,22)=1$

$\therefore$ solvable $\Leftrightarrow$ $13^{22} \equiv 1 \pmod{23}$

$13^2 = 169 \equiv 8$, $13^4 \equiv 64 \equiv -5$, $13^8 \equiv 25 \equiv 2$,

$13^{16} \equiv 4$, $13^{20} \equiv -20 \equiv 3$, $13^{22} \equiv 8 \cdot 3 = 24 \equiv 1$

$\therefore\ 13^{22} \equiv 1 \pmod{23}$, and so $x^5 \equiv 13 \pmod{23}$ is solvable.

(2) $x^7 \equiv 15 \pmod{29}$

$\gcd(15, 29) = 1$, $\gcd(7, 28) = 7$.

$\therefore$ By Th. 8.12, solvable $\iff 15^{\frac{28}{7}} \equiv 1 \pmod{29}$

$15^2 = 225 \equiv 22$, $15^4 \equiv 22^2 = 484 \equiv 20 \not\equiv 1 \pmod{29}$

$\therefore$ not solvable.

13. If $p$ is a prime and $\gcd(k, p-1) = 1$, prove that the integers $1^k, 2^k, 3^k, \dots, (p-1)^k$ form a reduced set of residues mod $p$.

Pf: $1, 2, \dots, p-1$ form a reduced set of residues mod $p$.

Thus, each of $1^k, 2^k, \dots, (p-1)^k$ must be congruent to one of $1, 2, \dots, p-1$.

Let $1 \le a \le p-1$, $1 \le b \le p-1$, and $a \ne b$.

Suppose $a^k \equiv b^k \pmod{p}$.

$\therefore$ ind $a^k$ = ind $b^k$, so

$k(\text{ind } a) \equiv k(\text{ind } b) \pmod{p-1}$

Since $\gcd(k, p-1) = 1$, Then

$\text{ind}\, a \equiv \text{ind}\, b \pmod{p-1}$

By def., $1 \le \text{ind}\, a \le p-1$, $1 \le \text{ind}\, b \le p-1$.

$\therefore \text{ind}\, a = \text{ind}\, b$

If $r$ is a prim. root of $p$, Then

$r^{\text{ind}\, a} = r^{\text{ind}\, b}$. But by def.,

$a \equiv r^{\text{ind}\, a} \pmod{p}$, $b \equiv r^{\text{ind}\, b} \pmod{p}$

$\therefore a \equiv b \pmod{p} \Rightarrow a = b$ a contradiction.

$\therefore a \not\equiv b \pmod{p}$, so each of The $p-1$ integers

$1^k, 2^k, \ldots, (p-1)^k$ is incongruent to The other mod $p$.

$\therefore 1^k, 2^k, \ldots, (p-1)^k$ form a complete set of residues mod $p$.

Now need to prove $\gcd(a^k, p-1) = 1$ for $1 \le a \le p-1$.

Consider $x^k \equiv a \pmod{p}$.

Clearly $\gcd(a, p) = 1$.

Since $\gcd(k, p-1) = 1$, Then by Th. 8-12, since $a^{p-1} \equiv 1 \pmod{p}$ by Fermat's Th., Then $x^k \equiv a \pmod{p}$ has exactly $\gcd(x, p-1) = 1$

solution mod $p$.

$\therefore$ The solution $x$ must be among $1, 2, \ldots, p-1$ since the solution is mod $p$.

$\therefore$ since $\gcd(a, p) = 1$, then $\gcd(x^k, p) = 1$ as $x^k \equiv a$ (and using prob. #3, sec. 4.2).

$\therefore$ each of $1^k, 2^k, \ldots, (p-1)^k$ is relatively prime to $p$.

$\therefore$ $1^k, 2^k, \ldots, (p-1)^k$ forms a reduced set of residues mod $p$.

14. Let $r$ be a prim. root of the odd prime $p$, and let $d = \gcd(k, p-1)$. Prove that the values of $a$ for which the congruence $x^k \equiv a \pmod{p}$ is solvable are $r^d, r^{2d}, \ldots, r^{[(p-1)/d]d}$.

Pf: (1) Let $s = 1, 2, \ldots, \frac{p-1}{d}$, let $a = r^{sd}$

Since $(r^{sd})^{\frac{\phi(p)}{d}} = (r^{\phi(p)})^s \equiv 1^s = 1 \pmod{p}$, as $r$ is a prim. root, then by Th. 8.12, $x^k \equiv a \pmod{p}$ has a solution when $a = r^d, r^{2d}, \ldots, r^{(\frac{p-1}{d})d}$, or $a = r^d, r^{2d}, \ldots, r^{p-1}$

(2) If $x^k \equiv a \pmod{p}$ has a solution, then, if $r$ is a prim. root of $p$,

$\text{ind}_r x^k = \text{ind}_r a$, so $k\,\text{ind}_r x \equiv \text{ind}_r a \pmod{p-1}$

Let $d = \gcd(k, p-1)$. Note $1 \le d \le p-1$

$\therefore$ By Th. 4.7, $d \mid \text{ind}_r a$. By def., $1 \le \text{ind}_r a \le p-1$

Let $m$ be s.t. $dm = \text{ind}_r a$. By def., $r^{dm} \equiv a \pmod{p}$

Since $1 \le d \le p-1$ and $1 \le \text{ind}_r a \le p-1$, then it must be true that $1 \le m \le p-1$.

$\therefore$ (1) shows that when $a = r^d, r^{2d}, \ldots, r^{p-1}$, then $x^k \equiv a \pmod{p}$ is solvable, and
(2) shows that if $x^k \equiv a \pmod{p}$ is solvable, $a$ must be congruent mod $p$ to $r^{dm}$, where $m = 1, 2, \ldots, p-1$.

$\therefore a = r^d, r^{2d}, \ldots, r^{p-1}$ are all the values, mod $p$, for which $x^k \equiv a \pmod{p}$ is solvable.

15. If $r$ is a prim. root of the odd prime $p$, show that

$$\operatorname{ind}_r(p-a) \equiv \operatorname{ind}_r a + \frac{(p-1)}{2} \pmod{p-1}$$

and consequently, that only half of an index table need be calculated to complete the table.

Pf: By def., $r^{\operatorname{ind}_r(p-a)} \equiv p-a \equiv (-a) \pmod p$

$\therefore \operatorname{ind}_r r^{\operatorname{ind}_r(p-a)} = \operatorname{ind}_r(-a)$. Since $\operatorname{ind}_r r = 1$,

$$\begin{aligned}\operatorname{ind}_r(p-a) &\equiv \operatorname{ind}_r(-a)\\ &\equiv \operatorname{ind}_r(-1) + \operatorname{ind}_r(a) \pmod{p-1}\end{aligned}$$

By prob. #7, $\operatorname{ind}_r(-1) = \frac{1}{2}(p-1)$.

$$\therefore \operatorname{ind}_r(p-a) = \tfrac{1}{2}(p-1) + \operatorname{ind}_r a \pmod{p-1}$$

16. (a) Let $r$ be a prim. root of the odd prime $p$. Establish that the exponential congruence

$a^x \equiv b \pmod p$ has a solution $\Leftrightarrow$

$d \mid \operatorname{ind}_r b$, where $d = \gcd(\operatorname{ind}_r a, p-1)$; in this case, there are $d$ incongruent solutions mod $p-1$.

Pf: $a^x \equiv b \pmod{p} \Leftrightarrow$

$$x \, \text{ind}_r a \equiv \text{ind}_r b \pmod{p-1} \quad [1]$$

By Th. 4.7, [1] has a solution $\Leftrightarrow$

$\gcd(\text{ind}_r a, p-1) = d \mid \text{ind}_r b$, in which

case there are $d$ incongruent solutions, mod $p-1$.

(b) Solve the exponential congruences
$4^x \equiv 13 \pmod{17}$ and $5^x \equiv 4 \pmod{19}$

(1) $4^x \equiv 13 \pmod{17}$ 3 is a prim. root of 17

$x \, \text{ind}_3 4 \equiv \text{ind}_3 13 \pmod{16}$

From table in prob. #3, $\text{ind}_3 4 = 12$,
$\text{ind}_3 13 = 4$

$\therefore 12x \equiv 4 \pmod{16}$ $\gcd(12, 16) = 4$
$4 \mid 4$, so 4 incongruent solutions mod 16

$\therefore 3x \equiv 1 \pmod{4}$, $9x \equiv 3$, $x \equiv 3 \pmod{4}$

$\therefore\ \underline{x \equiv 3, 7, 11, 15 \pmod{16}}$

(2) $5^x \equiv 4 \pmod{19}$ $\quad$ 2 is a prim. root of 19

$\therefore\ x \,\text{ind}_2 5 \equiv \text{ind}_2 4 \pmod{18}$

Develop table of indices for 19 relative to 2

| | | | | | | | | | | | | | | | | | | |
|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|
| $a$ | 1 | 2 | 3 | 4 | 5 | 6 | 7 | 8 | 9 | 10 | 11 | 12 | 13 | 14 | 15 | 16 | 17 | 18 |
| $\text{ind}_2 a$ | 18 | 1 | 13 | 2 | 16 | 14 | 6 | 3 | 8 | 17 | 12 | 15 | 5 | 7 | 11 | 4 | 10 | 9 |

$\therefore\ \text{ind}_2 5 = 16,\ \text{ind}_2 4 = 2$

$\therefore\ 16x \equiv 2 \pmod{18}$, $\gcd(16, 18) = 2$

$\therefore$ 2 incongruent solutions mod 18

$\therefore\ 8x \equiv 1 \pmod{9}$, $-8x \equiv -1$, $x \equiv -1 \equiv 8$

$\therefore\ \underline{x \equiv 8, 17 \pmod{18}}$

17. For which values of $b$ is the exponential congruence $9^x \equiv b \pmod{13}$ solvable.

2 is a prim. root of 13. Use table on p. 175

$\therefore x \, ind_2 9 \equiv ind_2 6 \pmod{12}$

$ind_2 9 = 8.$

$\therefore 8x \equiv ind_2 6 \pmod{12}$ $\quad gcd(8, 12) = 4$

$\therefore 4 \mid ind_2 6$, so $ind_2 6 = 4, 8, 12$

$\therefore 6$ (using table) $= 3, 9, 1$

$\therefore \underline{6 \equiv 1, 3, 9 \pmod{13}}$