8.2 Primitive Roots for Primes

Note Title 2/16/2006

1. If p is an odd prime, prove:

(a) The only incongruent solutions of $x^2 \equiv 1 \pmod{p}$ are 1 and $p-1$.

Pf: Since p is odd prime, $2 \mid p-1$.
$\therefore$ By Corollary to Lagrange Th. 8.5, The congruence $x^2-1 \equiv 0 \pmod{p}$ has exactly 2 solutions.

Clearly, 1 is a solution since $1 \equiv 1 \pmod{p}$

$p-1$ is also a solution since
$(p-1)^2 = p^2-2p+1 \equiv 1 \pmod{p}$

$\therefore$ 1 and $p-1$ are solutions and They are incongruent mod p.
$(1 \equiv p-1 \pmod{p} \Rightarrow 1 \equiv -1 \pmod{p})$.

(b) The congruence $x^{p-2} + \cdots + x^2 + x + 1 \equiv 1 \pmod{p}$ has exactly $p-2$ incongruent solutions, and they are $2, 3, \ldots, p-1$.

Pf: By Fermat's Th., when $\gcd(x, p) = 1$, Then $x^{p-1} \equiv 1 \pmod{p}$.

$\gcd(x, p) = 1$ for $x = 1, 2, 3, \ldots, p-1$, and these are all incongruent mod p.

$\therefore$ $x^{p-1} - 1 \equiv 0$ has exactly $p-1$ solutions and they are $1, 2, 3, \ldots, p-1$.

$$x^{p-1} - 1 = (x-1)(x^{p-2} + x^{p-3} + \cdots + x^2 + x + 1)$$

Since p is odd, $p \geq 3$, so $p-2$ is a valid exponent.

Since $x - 1 \equiv 0 \pmod{p}$ has exactly one solution ($x \equiv 1$), then $x^{p-2} + \cdots + x + 1$ has exactly $(p-1) - 1 = p-2$ solutions. Since $x \not\equiv 1 \pmod{p}$ for $x = 2, \ldots, p-1$, and $x^{p-1} - 1 \equiv 0$ for $x = 2, \ldots, p-1$, then $x^{p-2} + \cdots + x + 1 \equiv 0$ for $x = 2, \ldots, p-1$.

Thus, the $p-2$ solutions for $x^{p-2} + \cdots + x + 1 \equiv 0 \pmod{p}$ are $x = 2, 3, \ldots, p-1$.

2. Verify that each of the congruences:

$$x^2 \equiv 1 \pmod{15}$$
$$x^2 \equiv -1 \pmod{65}$$
$$x^2 \equiv -2 \pmod{33}$$

has four incongruent solutions; hence Lagrange's Theorem need not hold if the modulus is a composite number.

Pf: By Corollary 2 to Th. 2.4 (p. 24), if p and q are primes, $p \neq q$, and $p \mid c$ and $q \mid c$, then $pq \mid c$.

In problems above, if p, q are prime, $p \neq q$, then if $x_1^2 \equiv a \pmod{p}$, and
$x_1^2 \equiv a \pmod{q}$

Then $x_1^2 \equiv a \pmod{pq}$

Pf: $p \mid x_1^2 - a$, $q \mid x_1^2 - a$, and so $pq \mid x_1^2 - a$ by above statement.

$\therefore$ Strategy is to break up the congruence into two parts, solve each part, find common congruent solutions

$x^2 \equiv 1 \pmod{15} \Leftrightarrow x^2 \equiv 1 \pmod 3,\ x^2 \equiv 1 \pmod 5$

$(x+1)(x-1) \equiv 0 \qquad (x+1)(x-1) \equiv 0$

$x \equiv 1, 4, 7, 10, 13 \qquad x \equiv 1, 6, 11, 16$

$x \equiv -1, 2, 5, 8, 11, 14 \qquad x \equiv -1, 4, 9, 14$

$\therefore x \equiv \underline{1, 4, 11, 14} \pmod{15}$

$x^2 \equiv -1 \pmod{65} \Leftrightarrow$

$x^2 \equiv -1 \pmod 5 \qquad x^2 \equiv -1 \pmod{13}$

$x^2 \equiv 4 \qquad x^2 \equiv 12,\ x^2 \equiv 25$

$(x+2)(x-2) \equiv 0 \qquad (x+5)(x-5) \equiv 0$

$x \equiv -2, 3, 8, 13, 18, 23, 28, 33, 38, 43 \qquad x \equiv -5, 8, 21, 34, 47, 60$

$x \equiv 2, 7, 12, 17, 22, 27, 32, 37, 42, 47, 52, 57 \qquad x \equiv 5, 18, 31, 44, 57$

$\therefore x \equiv \underline{8, 18, 47, 57} \pmod{65}$

$x^2 \equiv -2 \pmod{33} \Leftrightarrow$

$x^2 \equiv -2 \pmod 3 \qquad x^2 \equiv -2 \pmod{11}$

$x^2 \equiv 1 \qquad x^2 \equiv 9$

$(x+1)(x-1) \equiv 0 \qquad (x+3)(x-3) \equiv 0$

$x \equiv -1, 2, 5, 8, 11, 14, 17, 20, 23, 26, 29 \qquad x \equiv -3, 8, 19, 30$

$x \equiv 1, 4, 7, 10, 13, 16, 19, 22, 25, 28, 31 \qquad x \equiv 3, 14, 25$

$\therefore x \equiv \underline{8, 14, 19, 25} \pmod{33}$

3. Determine all the primitive roots of the primes $p = 11, 19,$ and 23, expressing each as a power of some one of the roots.

11: There are $\phi(10) = (5-1)(2-1) = 4$ primitive roots

Try 2: $2^5 \equiv 10$, $\therefore 2^{10} \equiv 100 \equiv 1 \pmod{11}$

Divisors of 10: 1, 2, 5. $2^1 = 2$, $2^2 = 4$, $2^5 \equiv 10$

$\therefore$ 2 is a primitive root of 11.

Any integer relatively prime to 11 is congruent mod 11 to 2^k, $1 \leq k \leq 10$, since there are $\phi(11) = 10$ such numbers, and 2^k, $1 \leq k \leq 10$, are incongruent by Th. 8.4.
$\therefore$ Other primitive roots must be among the 2^k!
By Th. 8.3, these integers, 2^k, will have order 10 also if $\gcd(k, 10) = 1$.
$\therefore k = 1, 3, 7, 9$

$\therefore$ Primitive roots of 11 are: $\underline{2^1, 2^3, 2^7, 2^9}$
or 2, 6 ($\equiv 2^9$), 7 ($\equiv 2^7$), 8

19: There are $\phi(18) = (2-1)(3^2-3^1) = 6$ primitive roots

Try 2: $2^5 \equiv 13$, $2^6 \equiv 26 \equiv 7$, $\therefore 2^{11} \equiv 91 \equiv -4$

$\therefore 2^{17} \equiv (7)(-4) = -28 \equiv 10$, $2^{18} \equiv 20 \equiv 1 \pmod{19}$

Divisors of 18: 1, 2, 3, 6, 9, 18

$2^1, 2^2, 2^3 \not\equiv 1$. $2^6 \equiv 7 \not\equiv 1$, $2^9 \equiv 2^6 \cdot 2^3 \equiv 7 \cdot 8 = 56 \equiv 18$

$\therefore$ 2 is a primitive root of 19

Other primitive roots are congruent to 2^k, $1 \le k \le 18$

By Th. 8.3, need to select k s.t. $\gcd(k, 18) = 1$.

$\therefore k = 1, 5, 7, 11, 13, 17$

$\therefore$ Primitive roots are $\underline{2^1, 2^5, 2^7, 2^{11}, 2^{13}, 2^{17}}$

or $2, 13 (\equiv 2^5), 14 (\equiv 2^7), 15 (\equiv 2^{11}), 3 (\equiv 2^{13}), 10 (\equiv 2^{17})$

23: There are $\phi(22) = (2-1)(11-1) = 10$ primitive roots.

From table on p. 166, 5 is the smallest primitive root.

All primitive roots are congruent to 5^k, $1 \le k \le 22$

By Th. 8.3, need to select k s.t. $\gcd(22, k) = 1$.

$\therefore k = 1, 3, 5, 7, 9, 13, 15, 17, 19, 21$

$\therefore$ Primitive roots are $\underline{5^1, 5^3, 5^5, 5^7, 5^9, 5^{13}, 5^{15}, 5^{17}, 5^{19}, 5^{21}}$

Note $5^2 = 25 \equiv 2$

$\therefore$ $5 \ (\equiv 5^1)$ $\quad$ $21 \ (\equiv -2 \equiv 5^{13})$

$10 \ (\equiv 5^3)$ $\quad$ $19 \ (\equiv -4 \equiv 5^{15})$

$20 \ (\equiv 5^5)$ $\quad$ $15 \ (\equiv -8 \equiv 5^{17})$

$17 \ (\equiv 5^7)$ $\quad$ $7 \ (\equiv 5^{19})$

$11 \ (\equiv 5^9)$ $\quad$ $14 \ (\equiv 5^{21})$

4. Given that 3 is a primitive root of 43, find the following:

(a) All positive integers less than 43 having order 6 mod 43.

3^k, $1 \le k \le 42$ are incongruent by Th. 8.2

$\therefore$ All integers < 43 are congruent to 3^k.

3^k has order $42/\gcd(k, 42)$ mod 43 by Th. 8.3

$$\frac{42}{\gcd(k,42)} = 6 \Rightarrow \gcd(k, 42) = 7$$

$\therefore k = 7, 35$

$\therefore 3^7, 3^{35}$ have order 6 mod 43.

$3^3 = 27$, $3^4 = 81 \equiv -5$, $\therefore 3^7 \equiv -135 \equiv -135 + 3\cdot 43 \equiv -6 \equiv 37$

$3^7 \cdot 3^7 \equiv (-6)(-6) \equiv 36 \equiv (-7)$, $3^{18} \equiv (-7)(-5) \equiv 35 \equiv -8$

$3^{32} = 3^{14}\cdot 3^{18} \equiv (-7)(-8) = 56 \equiv 13$

$3^{33} \equiv 39 \equiv -4$, $\therefore 3^{35} \equiv 9(-4) = -36 \equiv 7$

$\therefore$ Only $\underline{7\ (\equiv 3^{35})}$ and $\underline{37\ (\equiv 3^7)}$ have order 6 mod 43.

(6). All positive integers less than 43 having order 21 mod 43.

As in (a), all such integers are congruent to 3^k, $1 \le k \le 42$

$$\therefore \frac{42}{\gcd(42,k)} = 21 \Rightarrow \gcd(42,k) = 2$$

$42 = 2\cdot 3\cdot 7$

$\therefore 2, 2^2, 2^3, 2^4, 2^5$ $(= 2, 4, 8, 16, 32)$

$2\cdot 5, 2\cdot 11, 2\cdot 13, 2\cdot 17, 2\cdot 19$ $(= 10, 22, 26, 34, 38)$

$2^2\cdot 5$ $(= 20)$

$2^3\cdot 5$ $(= 40)$

$\therefore 3^2, 3^4, 3^8, 3^{10}, 3^{16}, 3^{20}, 3^{22}, 3^{26}, 3^{32}, 3^{34}, 3^{38}, 3^{40}$

$3^2 \equiv 9$
$3^4 \equiv 81 \equiv -5 \equiv 38$
$3^8 \equiv 25$
$3^{10} \equiv 225 \equiv 10$

$3^{16} \equiv 25^2 \equiv 23$
$3^{20} \equiv 23 \cdot 38 \equiv 14$
$3^{22} \equiv 40$
$3^{26} \equiv 3^{10} \cdot 3^{16} \equiv 230 \equiv 15$

$3^{32} \equiv 400 \equiv 13$
$3^{34} \equiv 31$
$3^{38} \equiv 31 \cdot 38 \equiv 17$
$3^{40} \equiv 9 \cdot 17 \equiv 24$

$\therefore$ $\underline{9, 10, 13, 14, 15, 17, 23, 24, 25, 31, 38, 40}$

all have order 21 mod 43.

5. Find all positive integers less than 61 having order 4 mod 61.

Table p. 166 indicates 2 is a primitive root of 61.

$\therefore 2^k$, $1 \le k \le 60$ are incongruent

$$\therefore \frac{60}{\gcd(60,k)} = 4 \Rightarrow \gcd(60,k) = 15 \text{ by Th. 8.3}$$

$60 = 2^2 \cdot 3 \cdot 5$. $\therefore$ $3 \cdot 5$, $3^2 \cdot 5 \Rightarrow 15, 45$

$\therefore 2^{15}, 2^{45}$ have order 4 mod 61.

$2^6 = 64 \equiv -3$, $2^{12} \equiv 9$, $2^{15} \equiv 9 \cdot 8 = 72 \equiv 11$
$2^{30} \equiv 121 \equiv -1$, $2^{45} \equiv (-1)(11) = -11 \equiv 50$

$\therefore$ Only <u>11, 50</u> have order 4 mod 61.

6. Assuming that r is a primitive root of the odd prime p, establish the following facts:

(a) The congruence $r^{(p-1)/2} \equiv -1 \pmod{p}$ holds.

Pf: We know $r^{p-1} \equiv 1 \pmod{p}$ by Fermat's Th.

As $\frac{p-1}{2}$ is an integer, $r^{\frac{p-1}{2}}$ exists,

$\therefore r^{p-1} - 1 \equiv 0 \Rightarrow \left(r^{\frac{p-1}{2}} - 1\right)\left(r^{\frac{p-1}{2}} + 1\right) \equiv 0$

If $r^{\frac{p-1}{2}} - 1 \equiv 0 \pmod{p}$ then since $\frac{p-1}{2} < p-1$, r wouldn't have order $p-1$.

$\therefore r^{\frac{p-1}{2}} + 1 \equiv 0 \Rightarrow r^{\frac{p-1}{2}} \equiv -1 \pmod{p}$

(b) If r' is any other primitive root of p, then rr' is not a primitive root of p.

If rr' were a primitive root, its order would be $p-1$.

But by (a), $r^{\frac{p-1}{2}} \equiv -1$ and $(r')^{\frac{p-1}{2}} \equiv -1$, so $\left(r^{\frac{p-1}{2}}\right)\left((r')^{\frac{p-1}{2}}\right) \equiv (-1)(-1) \pmod{p}$, or

$(rr')^{\frac{p-1}{2}} \equiv 1 \pmod{p}$. Since $\frac{p-1}{2} < p-1$, This contradicts assumption of order of rr'.

$\therefore$ rr' not a primitive root of p.

(c) If The integer r' is such That $rr' \equiv 1 \pmod{p}$, Then r' is a primitive root of p.

Pf: We can assume $1 \le r' \le p-1$.
For if $r' = p$, Then $r' \equiv 0$, so $rr' \not\equiv 1$.
If $r' > p$, Then by Div. Alg.,
$r' = qp + s$, $0 \le s \le p-1$, so $r' \equiv s \pmod{p}$
and $\therefore$ r' and s have same order.

$\therefore$ $\gcd(r', p) = 1$.

Consider $(r')^k$, $1 \le k \le p-1$.

If $k < p-1$ and $(r')^k \equiv 1 \pmod{p}$, then

$1 = 1^k \equiv (rr')^k = r^k (r')^k \equiv r^k \pmod{p}$

contradicting order of $r = p-1$.

$\therefore\ 1 = 1^{p-1} \equiv (rr')^{p-1} = r^{p-1}(r')^{p-1} \equiv (r')^{p-1} \pmod p$

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

$(r')^k \not\equiv 1 \pmod p$ for $1 \le k < p-1$, and

$\gcd(r', p) = 1$.

$\therefore$ By def., r' is a primitive root of p.

7. For a prime $p > 3$, prove that the primitive roots of p occur in incongruent pairs r, r' where $rr' \equiv 1 \pmod p$.

Pf: By Th. 7.4, for $n > 2$, $\phi(n)$ is an even integer, so that $\phi(n) \ge 2$.

Let r be one primitive root of p.
By Th. 8.4, $r, r^2, \ldots, r^{p-1}$ are congruent to $1, 2, \ldots, p-1$ in some order, and so $r, r^2, \ldots, r^{p-1}$ are incongruent. Since $p > 3$, there are at least 3 members in this list.
Let $r' = r^{p-2}$. $\therefore$ r and r' are incongruent, and $rr' = r \cdot r^{p-2} = r^{p-1} \equiv 1 \pmod p$.

By 6(c) above, r' is a primitive root.

$\therefore$ If r is a primitive root of p, $p > 3$, we can always find an r' incongruent to r s.t. $rr' \equiv 1 \pmod{p}$.

8. Let r be a primitive root of the odd prime p. Prove the following:

(a) If $p \equiv 1 \pmod 4$, then $-r$ is also a primitive root of p.

Pf: Let k be s.t. $p-1 = 4k$

r a primitive root of $p \Rightarrow r^{p-1} \equiv 1 \pmod{p}$

$\therefore r^{4k} \equiv 1 \pmod{p}$

$\therefore (-r)^{p-1} = (-r)^{4k} = r^{4k} \equiv 1 \pmod{p}$

Let $1 \leq s < p-1$, and consider $(-r)^s$

s even: $(-r)^s = r^s \not\equiv 1 \pmod{p}$ as r is a primitive root, and by def., $r^s \not\equiv 1$ if for $1 \leq s < p-1$.

s odd: $(-r)^s = -r^s$

For s to be odd, $s = 4k-3$ or $4k-1$ for some k.

$4k-1$: Assume $-r^{4k-1} \equiv 1 \pmod{p}$

$\therefore (-r)(-r^{4k-1}) = r^{4k} \equiv -r$

But $r^{4k} = r^{p-1} \equiv 1$, so

$-r \equiv 1 \Rightarrow r^2 \equiv 1$ contradicting r having order $p-1$.

$4k-3$: Assume $-r^{4k-3} \equiv 1 \pmod{p}$

$\therefore (-r^3)(-r^{4k-3}) = r^{4k} \equiv -r^3$

But $r^{4k} = r^{p-1} \equiv 1$, so

$-r^3 \equiv 1$, or $r^3 + 1 \equiv 0 \pmod{p}$

$\therefore (r+1)(r^2+r+1) \equiv 0$

$\therefore r+1 \equiv 0$ or $r^2+r+1 \equiv 0$

If $r+1 \equiv 0$, then $r \equiv -1 \Rightarrow r^2 \equiv 1$, contradicting order of r as $p-1$.

If $r^2+r+1 \equiv 0$, then

$(r^{p-1})(r^2+r+1) \equiv 0$

$r^{p+1} + r^p + r^{p-1} \equiv r^{p+1} + r^p \equiv 0$

$\therefore$ Since $\gcd(r,p)=1$, $\gcd(r^p,p)=1$, dividing by r^p,

$r+1 \equiv 0 \Rightarrow r \equiv -1$, $r^2 \equiv 1$, contradicting $p-1$ as order of r.

$\therefore$ for $1 \le s < p-1$, $(-r)^s \not\equiv 1 \pmod p$

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

$\therefore$ $-r$ is a primitive root of p.

(b). If $p \equiv 3 \pmod 4$, Then $-r$ has order $(p-1)/2 \mod p$

Pf: $p = 3 + 4k$, some $k \ge 0$. $\therefore$ $p-1 = 2+4k$,

$\therefore$ $\frac{p-1}{2} = 1 + 2k$, some $k \ge 0$.

$\therefore$ $\frac{p-1}{2}$ is odd. $\therefore$ $(-r)^{\frac{p-1}{2}} = -r^{\frac{p-1}{2}}$

(a) Since $r^{p-1} \equiv 1 \pmod p$ [r a prim. root],

Then $r^{p-1} - 1 \equiv 0 \Rightarrow (r^{\frac{p-1}{2}}+1)(r^{\frac{p-1}{2}}-1) \equiv 0$

But $r^{\frac{p-1}{2}} - 1 \not\equiv 0$. If so, $r^{\frac{p-1}{2}} \equiv 1$, contradicting order of r as $p-1$.

$\therefore$ $r^{\frac{p-1}{2}} + 1 \equiv 0 \Rightarrow r^{\frac{p-1}{2}} \equiv -1 \Rightarrow$

$(-r)^{\frac{p-1}{2}} = -r^{\frac{p-1}{2}} \equiv 1 \pmod p$.

(b) Now suppose $-r$ has order s, $1 \le s < \frac{p-1}{2}$

s can't be even. If so, then $(-r)^s = r^s \equiv 1$, so order of r would be less than $p-1$, a contradiction.

$\therefore$ s is odd, $2s < p-1$

$\therefore$ $(-r)^s \equiv 1 \Rightarrow (-r)^{2s} = r^{2s} \equiv 1$

This contradicts order of r as $p-1$.

$\therefore$ order of $-r$ can't be $< \frac{p-1}{2}$.

(a) + (b) $\Rightarrow$ order of $-r$ is $\frac{p-1}{2}$.

9. Give a different proof of Th. 5.5 by showing that if r is a primitive root of the prime $p \equiv 1 \pmod 4$, then $r^{(p-1)/4}$ satisfies the quadratic congruence $x^2 + 1 \equiv 0 \pmod p$

Pf: r a primitive root $\Rightarrow r^{p-1} \equiv 1 \pmod p$
Since $p-1 = 4k$, some k, then

$(p-1)/4 = k$, some integer.

Consider $x^4 \equiv 1 \pmod{p}$.

$r^{\frac{p-1}{4}}$ is a solution.

$\therefore x^4 - 1 = (x^2+1)(x^2-1) \equiv 0 \pmod{p}$

If $r^{\frac{p-1}{4}}$ is a solution to $x^2 - 1 \equiv 0$,
Then $r^{\frac{p-1}{2}} \equiv 1$, contradicting order of r as $p-1$.

$\therefore r^{\frac{p-1}{4}}$ is a solution to $x^2+1 \equiv 0 \pmod{p}$.

Th. 5.5 says $x^2+1 \equiv 0 \pmod{p}$, p odd, has a solution $\Leftrightarrow p \equiv 1 \pmod{4}$.

(a) if $p \equiv 1 \pmod{4}$, p has a primitive root, since p is prime. Call it r. Above shows $r^{(p-1)/4}$ is a solution.

(b) Suppose $x^2+1 \equiv 0 \pmod{p}$ has a solution
Proof is same as given in text on p. 99.

10. Use The fact That each prime p has a primitive root to give a different proof of Wilson's Theorem.

Pf: Let r be a primitive root of p.

$1, 2, 3, \ldots, p-1$ are the positive integers less than p that are relatively prime to p. Also, $\phi(p) = p-1$.

$\therefore$ By Th. 8.4, $r, r^2, \ldots, r^{p-1}$ are congruent mod p to $1, 2, \ldots, p-1$, in some order.

$\therefore$ $1 \cdot 2 \cdot 3 \cdot \cdots (p-1) \equiv r \cdot r^2 \cdot r^3 \cdots r^{p-1} \pmod{p}$, or

$$(p-1)! \equiv r^{1+2+\cdots+(p-1)} \pmod{p}$$

But $1+2+\cdots+(p-1) = \dfrac{(p-1)p}{2}$

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

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

But, since r is a primitive root of p,

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

$\therefore$ $[(p-1)!]^2 \equiv 1 \pmod{p}$

$\therefore [(p-1)!]^2 - 1 \equiv 0 \pmod{p}$, so

$[(p-1)! + 1][(p-1)! - 1] \equiv 0 \pmod{p}$

If $(p-1)! - 1 \equiv 0$, Then $r^{\frac{(p-1)(p)}{2}} \equiv (p-1)! \equiv 1$

But $r^{p-1} \equiv 1$, so $r^p \equiv r$

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

which contradicts order of $r = p-1$, since $\frac{p-1}{2} < p-1$.

$\therefore (p-1)! + 1 \equiv 0 \pmod{p}$, so $\underline{(p-1)! \equiv -1 \pmod{p}}$

11. If p is a prime, show that the product of the $\phi(p-1)$ primitive roots of p is congruent mod p to $(-1)^{\phi(p-1)}$

Pf: By Th. 8.4, since r is a primitive root, Then $r^1, r^2, \ldots, r^{p-1}$ are congruent to $1, 2, \ldots, p-1$ in some order.

If s is any other primitive root, it must be congruent to one of $1, 2, \ldots, p-1$, and $\therefore$ is congruent to one of $r^1, r^2, \ldots, r^{p-1}$.

$\therefore$ All primitive roots of p are of the form r^k, where $1 \leq k \leq p-1$.

By Th. 8.3, the r^k will have order $p-1$ if $\gcd(k, p-1) = 1$. Clearly, $k \neq p-1$ for this to be true, so k must be of the form $1 \leq k < p-1$.

Call these $\phi(p-1)$ integers $k_1, k_2, \ldots, k_{\phi(p-1)}$, where $1 \leq k_i < p-1$.

$\therefore$ The product of these primitive roots

is $r^{k_1} \cdot r^{k_2} \cdots r^{k_{\phi(p-1)}} = r^{k_1 + k_2 + \cdots + k_{\phi(p-1)}}$

By Th. 7.7, $k_1 + k_2 + \cdots + k_{\phi(p-1)} = \frac{1}{2}(p-1)\phi(p-1)$

$\therefore r^{k_1 + k_2 + \cdots k_{\phi(p-1)}} = r^{\frac{1}{2}(p-1)\phi(p-1)}$

For $p > 2$, $\phi(p-1)$ is even by Th. 7.4, so $2 \mid \phi(p-1)$

$$\therefore\ r^{\frac{1}{2}(p-1)\phi(p-1)} = \left(r^{p-1}\right)^{\frac{1}{2}\phi(p-1)}$$

$$\equiv (1)^{\frac{1}{2}\phi(p-1)} \equiv 1 \pmod{p}$$

since $\frac{1}{2}\phi(p-1) \geq 1$ for $p > 2$.
Since $\phi(p-1)$ is even, $(-1)^{\phi(p-1)} = 1$,
so

$$r^{k_1 + k_2 + \cdots + k_{\phi(p-1)}} \equiv (-1)^{\phi(p-1)} \pmod{p}$$

For $p = 2$, the only primitive root is 1,
$\phi(2) = 1$, and so,

$$r^{k_1 + \cdots + r_{\phi(p-1)}} = 1 \equiv (-1)^{\phi(2-1)} = -1 \pmod{2}$$

since $1 \equiv -1 \pmod{2}$.

$\therefore$ The formula holds for $p = 2$.

12. For an odd prime p, verify that the sum

$$1^n + 2^n + 3^n + \cdots + (p-1)^n \equiv \begin{cases} 0 \pmod{p} & \text{if } (p-1) \nmid n \\ -1 \pmod{p} & \text{if } (p-1) \mid n \end{cases}$$

Pf: p odd means $p \neq 2$, so sum doesn't reduce to $1^n = 1$. But for $p=2$, $p-1 \mid n$ for all n, and so $1^n = 1 \equiv -1 \pmod{2}$, so formula works even for $p = 2$.

$\therefore$ Let p be an odd prime, let r be a primitive root.

$\therefore$ $r, r^2, \ldots, r^{p-1}$ are congruent mod p to $1, 2, \ldots, p-1$ in some order by Th. 8.4

Since $r^k \equiv j \pmod{p}$, $1 \leq k \leq p-1$, $1 \leq j \leq p-1$,

Then $r^{kn} \equiv j^n \pmod{p}$

Thus, $r^n, r^{2n}, \ldots, r^{(p-1)n}$ are congruent mod p to $1^n, 2^n, \ldots, (p-1)^n$ in some order.

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

Since r is a primitive root of p, $r^{p-1} \equiv 1 \pmod{p}$, so $r^{(p-1)n} \equiv 1 \pmod{p}$.

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

Note since $p \geq 3$, $r^{(p-2)n}$ makes sense.

Suppose $(p-1) \mid n$. Then $n = (p-1)k$, some k.

$\therefore$ For $1 \leq s \leq p-2$, $r^{sn} = r^{(p-1)ks}$

$\therefore$ Since $r^{(p-1)ks} \equiv 1^{ks} = 1 \pmod p$, Then $r^{sn} \equiv 1$.

There are $(p-2)$ terms in $r^n + r^{2n} + \dots + r^{(p-2)n}$

$$\begin{aligned}\therefore 1 + r^n + r^{2n} + \dots + r^{(p-2)n} &\equiv 1 + [1 + 1 + \dots + 1] \\ &\equiv 1 + (p-2) \\ &\equiv p-1 \\ &\equiv -1 \pmod p\end{aligned}$$

$\therefore$ For $(p-1) \mid n$,

$$1^n + 2^n + \dots + (p-1)^n \equiv -1 \pmod p \qquad [1]$$

Suppose $(p-1) \nmid n$. $\therefore$ $n = a(p-1) + b$, $0 < b < (p-1)$ by Div. Alg.

$$\begin{aligned}\therefore r^n = r^{a(p-1)+b} &= [r^{(p-1)}]^a \cdot r^b \\ &\equiv 1^a \cdot r^b \equiv r^b \pmod p\end{aligned}$$

since r a prim. root of $p \Rightarrow r^{p-1} \equiv 1 \pmod p$.

$\therefore$ $r^b \not\equiv 1 \pmod p$ since $b < p-1$ and prim. root means $p-1$ is the smallest order for r.

$$\therefore r^n - 1 \equiv r^b - 1 \not\equiv 0 \pmod p \qquad [2]$$

$$\text{Let } S = 1 + r^n + r^{2n} + \dots + r^{(p-2)n} \qquad [3]$$

$\therefore\ r^n S = r^n + r^{2n} + r^{3n} + \ldots + r^{(p-2)n} + r^{(p-1)n}$ [4]

Subtracting [3] from [4],

$r^n S - S = (r^n - 1)S = r^{(p-1)n} - 1$, or

$(r^n - 1)(1 + r^n + r^{2n} + \ldots + r^{(p-2)n}) = r^{(p-1)n} - 1$

But $r^{(p-1)} \equiv 1 \pmod p$, so $r^{(p-1)n} - 1 \equiv 0 \pmod p$

$\therefore\ (r^n - 1)(1 + r^n + \ldots + r^{(p-2)n}) \equiv 0 \pmod p$

From [2], $r^n - 1 \not\equiv 0 \pmod p$.

$\therefore\ 1 + r^n + \ldots + r^{(p-2)n} \equiv 0 \pmod p$

$\therefore$ when $(p-1) \nmid n$,

$1^n + 2^n + \ldots + (p-1)^n \equiv 1 + r^n + \ldots + r^{(p-2)n} \equiv 0 \pmod p$ [5]

$\therefore$ [1] and [5] give

$$1^n + 2^n + \ldots + (p-1)^n \equiv \begin{cases} 0 \pmod p & \text{if } (p-1) \nmid n \\ -1 \pmod p & \text{if } (p-1) \mid n \end{cases}$$