9.1 The Legendre Symbol and Its Properties

Note Title 5/31/2006

1. Find the value of the following Legendre symbols:

(a) $(19/23)$

$19 \equiv -4 \pmod{23}$.

$\therefore (19/23) = (-4/23) = (-1 \cdot 2^2/23) = (-1/23)$
$= (-1)^{(23-1)/2} = \underline{-1}$

(b) $(-23/59)$

$-23 \equiv -23+59 \pmod{59} = 36 = 6^2$
$\therefore (-23/59) = (6^2/59) = \underline{1}$

(c) $(20/31) = (2^2 \cdot 5/31) = (5/31)$
$5 \equiv 36 \pmod{31}$
$\therefore (20/31) = (36/31) = (6^2/31) = \underline{1}$

(d) $(18/43) = (2 \cdot 3^2/43) = (2/43)$

$43 = 5 \cdot 8 + 3$, so by Th. 9.6, $(2/43) = \underline{-1}$

(e) $(-72/131) = (-3^2 \cdot 2^2 \cdot 2/131) = (-1/131)(2/131)$

$(-1/131) = (-1)^{(131-1)/2} = -1$. $\therefore (-72/131) = -(2/131)$

$131 = (16)\cdot 8 + 3$, so by Th. 9.6, $(2/131) = -1$

$\therefore (-72/131) = (-1)(-1) = \underline{1}$

2. Use Gauss' lemma to compute each of the Legendre symbols below (that is, in each case obtain the integer n for which $(a/p) = (-1)^n$):

(a) $(8/11)$

$$(p-1)/2 = 5, \quad p/2 = 5.5$$

$$\therefore S = \{8, 16, 24, 32, 40\} = \{1\cdot 8, 2\cdot 8, \ldots, 5\cdot 8\}$$

$$\equiv \{8, 5, 2, 9, 7\} \pmod{11}$$

$$\therefore 8, 9, 7 > p/2, \text{ so } n = 3$$

$$\therefore (8/11) = (-1)^3 = -1$$

(b) $(7/13)$ $\quad (p-1)/2 = 6, \quad p/2 = 6.5$

$$\therefore S = \{7, 14, 21, 28, 35, 42\}$$

$$\equiv \{7, 1, 8, 2, 9, 3\} \pmod{13}$$

$\therefore$ $7, 8, 9 > p/2$, so $n = 3$

$\therefore$ $(8/13) = (-1)^3 = -1$

(c) $(5/19)$ $\quad (p-1)/2 = 9$, $p/2 = 9.5$

$\therefore$ $S = \{5, 10, 15, 20, 25, 30, 35, 40, 45\}$

$\equiv \{5, 10, 15, 1, 6, 11, 16, 2, 7\} \pmod{19}$

$\therefore$ $10, 15, 11, 16 > 9.5$, so $n = 4$

$\therefore$ $(-1)^4 = 1$

(d) $(11/23)$ $\quad (p-1)/2 = 11$, $p/2 = 11.5$

$\therefore$ $S = \{11, 22, 33, 44, 55, 66, 77, 88, 99, 110, 121\}$

$\equiv \{11, 22, 10, 21, 9, 20, 8, 19, 7, 18, 6\}$

$\therefore$ $22, 21, 20, 19, 18 > 11.5$, so $n = 5$

$\therefore$ $(-1)^5 = -1$

(e) $(6, 31)$ $(p-1)/2 = 15$, $p/2 = 15.5$

$\therefore S = \{6, 12, 18, 24, 30, 36, 42, 48, 54, 60, 66, 72, 78, 84, 90\}$

$\equiv \{6, 12, 18, 24, 30, 5, 11, 17, 23, 29, 4, 10, 16, 22, 28\} \pmod{31}$

$\therefore 18, 24, 30, 17, 23, 29, 16, 22, 28 > 15.5$, so $n = 9$

$\therefore (-1)^9 = -1$

3. For an odd prime p, prove there are $\frac{p-1}{2} - \phi(p-1)$ quadratic non-residues of p that are not primitive roots of p.

Pf: By Th. 9.4, there are $\frac{p-1}{2}$ quadratic residues of p and $\frac{p-1}{2}$ quadratic nonresidues of p.

If a is a quadratic residue of p, it cannot be a primitive root, because $a^{(p-1)/2} \equiv 1 \pmod{p}$ by Th. 9.1, and $\frac{p-1}{2} < p-1 = \phi(p)$.

$\therefore$ if r is a primitive root of p, it must be congruent to a quadratic nonresidue of p.

Let S be the set of quadratic nonresidues of p. There are thus $\frac{p-1}{2}$ elements of S.

$\therefore$ All the primitive roots of p are congruent to some of the $\frac{p-1}{2}$ elements of S!

By the corollary to Th. 8.6 (p. 165), there are $\phi(p-1)$ primitive roots of p, and so $\phi(p-1)$ elements of S are primitive roots.

$\therefore$ $\frac{p-1}{2} - \phi(p-1)$ elements of S are not primitive roots of p.

4. (a) Let p be an odd prime. Show that the Diophantine equation $x^2 + py + a = 0$, $\gcd(a, p) = 1$, has an integral solution if and only if $(-a/p) = 1$!

(1) If $x^2 + py + a = 0$ has a solution, then $x^2 + a = -yp \Rightarrow x^2 + a \equiv 0 \pmod{p} \Rightarrow x^2 \equiv -a \pmod{p} \Rightarrow (-a)$ is a quadratic residue of $p \Rightarrow (-a/p) = 1$.

(2) If $(-a/p) = 1$, then $(-a)$ is a quadratic residue of $p \Rightarrow x^2 \equiv -a \pmod{p}$ has a

solution in $x \Rightarrow$ There is an integer k s.t. $x^2 = -a + kp$, or $x^2 + a - kp = 0$, or letting $y = -k$, $x^2 + py + a = 0$

(b) Determine whether $x^2 + 7y - 2 = 0$ has a solution in integers.

$\gcd(-2, 7) = 1$. By (a), since $(2/7) = 1$ by Th. 9.6, Then there is a solution.

5. Prove That 2 is not a primitive root of any prime of the form $p = 3 \cdot 2^n + 1$, except when $p = 13$.

Pf: Strategy: show 2 is a quadratic residue of p, and so cannot be a primitive root.

For $p-1 = 3 \cdot 2^n$, $p - 1 \equiv 0 \pmod 8$ when $n \geq 3$

$\therefore$ For $n \geq 3$, $p \equiv 1 \pmod 8$, so by Th. 9.6, $(2/p) = 1$

$\therefore$ For $n \geq 3$, 2 is a quadratic residue and $\therefore$ not a primitive root.

$\therefore$ Consider $n=1,2$

$n=1$: $p = 3\cdot 2+1 = 7$. $\therefore p \equiv 7 \pmod 8$

$\therefore$ By Th. 9.6, $(2/p)=1$, so 2 is a quad. residue, and so 2 is not a prim. root.

$n=2$: $p = 3\cdot 2^2+1 = 13$. $\therefore p \equiv 5 \pmod 8$

$\therefore (2/p) = -1$, so 2 is a quad. nonresidue, and 2 is a know primitive root of 13.

$\therefore$ For $n \geq 1, n \neq 2$, if $p = 3\cdot 2^n+1$ is prim, then 2 is not a primitive root of p.

C. (a) If p is an odd prime, and $\gcd(ab,p)=1$, prove that at least one of a, b, or ab is a quadratic residue of p.

Pf: $(ab/p) = (a/p)(b/p)$

(ab/p), (a/p), and (b/p) are each equal to 1 or -1.

$\therefore$ if $(ab/p) = 1$, by def., ab is a quadratic residue of p.

$\therefore$ Suppose $(ab/p) = -1$.

$\therefore (a/p)(b/p) = -1$.

(a/p) and (b/p) cannot both be -1, since $(-1)\cdot(-1) \neq -1$.

$\therefore$ Either $(a/p) = 1$ or $(b/p) = 1$.

$\therefore$ either a or b is a quadratic residue of p.

(5) Given a prime p, show that for some choice of $n > 0$, p divides $(n^2-2)(n^2-3)(n^2-6)$

Pf: $p = 2$: Let $n = 3$. Then $(n^2-2)(n^2-3)(n^2-6) = (9-2)(9-3)(9-6) = 7\cdot 6\cdot 3$

$\therefore p \mid 7\cdot 6\cdot 3$

$p=3$: Let $n=3$, as above, $p \mid 7\cdot 6\cdot 3$

$p>3$: $\therefore \gcd(2\cdot 3, p)=1$

$\therefore$ By (a), one of 2, 3, or $2\cdot 3$ is a quadratic residue of p.

$\therefore$ By def., there must be an n s.t. $n^2 \equiv 2 \pmod p$, or
$n^2 \equiv 3 \pmod p$, or
$n^2 \equiv 6 \pmod p$.

$\therefore$ $n^2-2 \equiv 0 \pmod p$, or
$n^2-3 \equiv 0 \pmod p$, or
$n^2-6 \equiv 0 \pmod p$.

$\therefore (n^2-2)(n^2-3)(n^2-6) \equiv 0 \pmod p$.

$\therefore$ There is an n s.t. $p \mid (n^2-2)(n^2-3)(n^2-6)$

7. If p is an odd prime, show that

$$\sum_{a=1}^{p-2} (a(a+1)/p) = -1 \qquad [(\ /\ ) \text{ is Legendre symbol}]$$

Pf: Use the hint. Let a' be defined by

$aa' \equiv 1 \pmod{p}$. Note that since $\gcd(a,p)=1$, then a' exists, by Th. 4.7, for each $1 \le a \le p-2$.

Note that as a runs from 1 to $p-2$, a' also runs from 1 to $p-2$ (not $p-1$, for if $a' = p-1$, then $a(p-1) \equiv 1$, $ap - a \equiv 1$, $-a \equiv 1$, $0 \equiv 1+a$, $p \equiv 1+a$, $p-1 \equiv a \Rightarrow p-1 = a$, a contradiction). Also, if $a_1 a' \equiv 1$ and $a_2 a' \equiv 1$, then $a_1 a' \equiv a_2 a' \Rightarrow a_1 \equiv a_2 \Rightarrow a_1 = a_2$.
$\therefore$ As a runs through 1 to $p-2$, each a' from 1 to $p-2$ is represented only once.

$\therefore$ as a runs through 1 to $p-a$, $1+a'$ runs through 2 to $p-1$.

$$\therefore aa' \equiv 1 \pmod{p} \Rightarrow a + aa' \equiv a+1$$
$$\Rightarrow a(1+a') \equiv a+1$$

$$\therefore a(a+1) \equiv a^2(1+a') \pmod{p}$$

$$\therefore (a(a+1)/p) = (a^2(1+a')/p) = ((1+a')/p)$$

$$\therefore \sum_{a=1}^{p-2} (a(a+1)/p) = \sum_{1+a'=2}^{p-1} ((1+a')/p)$$

$$= \sum_{a'=2}^{p-1} (a'/p) = \sum_{a=2}^{p-1} (a/p)$$

$$= \sum_{a=1}^{p-1} (a/p) - (1/p)$$

But by Th. 9.4, $\sum_{a=1}^{p-1} (a/p) = 0$

and $(1/p) = 1$.

$$\therefore \sum_{a=1}^{p-2} (a(a+1)/p) = -1$$

8. Prove the statements below:

(a) If p and $q = 2p+1$ are both odd primes, then -4 is a primitive root of q.

Pf: Since $-4 = -2^2$ and $\gcd(2,q)=1$, then $\gcd(-4,q)=1$. Since $\phi(q) = q-1 = 2p$, then order of -4 must be $1, 2, p$, or $2p$ by Th. 8.1.

(1) If $-4 \equiv 1 \pmod{q}$, then $5 \equiv 0 \pmod{q} \Rightarrow q \mid 5$. But $q > 5$ since p is odd. $\therefore$ order of -4 mod q is not 1.

(2) If $(-4)^2 \equiv 1 \pmod{q}$, then $15 \equiv 0 \pmod{q}$, or $q \mid 15 \Rightarrow q = 3$ or 5, again contradicting $q > 5$. $\therefore$ order of -4 mod q is not 2.

(3) Suppose $(-4)^p \equiv 1 \pmod q$

Since $(-4)^p = (-4)^{\frac{q-1}{2}}$, Then $(-4)^{\frac{q-1}{2}} \equiv 1 \pmod q$

But $(-4/q) \equiv (-4)^{\frac{q-1}{2}} \pmod q$

$\therefore (-4/q) \equiv 1 \pmod q \Rightarrow (-4/q) = 1$ [1]

However, $(-4/q) = (-1/q)(2/q)(2/q)$

$(-1/q) = (-1)^{\frac{q-1}{2}} = (-1)^{\frac{2p}{2}} = (-1)^p = -1$ as p is odd

$(2/q) \equiv 2^{\frac{q-1}{2}} = 2^p \pmod q$

if $p \equiv 1 \pmod 4$, Then $p = 1 + 4k$, some k, so $q = 2p + 1 = 3 + 8k$, so $q \equiv 3 \pmod 8$, so by Th. 9.6, $(2/q) = 1$.

$\therefore (-4/q) = (-1)(1)(1) = -1$

This contradicts [1]

if $p \equiv 3 \pmod 4$ Then, as above, $q \equiv 7 \pmod 8$, so by Th. 9.6, $(2/q) = 1$

$\therefore (-4/q) = (-1)(1)(1) = -1$, contradicting [1].

$\therefore (-4)^p \not\equiv 1 \pmod q$, so order of $-4 \bmod q$ is not p.

(1), (2), (3) $\Rightarrow$ order of $(-4) \bmod q$ is $2p = q-1 = \phi(q)$.

$\therefore -4$ is a primitive root of $q = 2p+1$.

(6) If $p \equiv 1 \pmod 4$ is a prime, then -4 and $(p-1)/4$ are quadratic residues of p.

Pf: (1) $(-4/p) = (-1/p)(2/p)(2/p)$

By corollary to Th. 9.2 (p. 187), $(-1/p) = 1$

$(2/p) = \pm 1$, so $(2/p)(2/p) = 1$.

$\therefore (-4/p) = 1 \Rightarrow -4$ is a quadratic residue of p

(2) Since $\gcd(4, p) = 1$, then

$$x^2 \equiv \frac{p-1}{4} \pmod p \iff 4x^2 \equiv p-1 \pmod p$$
$$\iff 4x^2 \equiv -1 \pmod p$$
$$\iff (2x)^2 \equiv -1 \pmod p$$

Let $y = 2x$.

$\therefore y^2 \equiv -1 \pmod{p}$ has a solution

by corollary to Th. 9.2 (p. 187)
since $p \equiv 1 \pmod{4}$

$\therefore x^2 \equiv \frac{p-1}{4} \pmod{p}$ has a solution,

and so $\frac{p-1}{4}$ is a quadratic residue of p.

9. For a prime $p \equiv 7 \pmod{8}$, show that $p \mid 2^{\frac{p-1}{2}} - 1$

Pf: By Th. 9.2, $(2/p) \equiv 2^{\frac{p-1}{2}} \pmod{p}$

By Th. 9.6, $(2/p) = 1$ since $p \equiv 7 \pmod{8}$.

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

$\Rightarrow p \mid 2^{\frac{p-1}{2}} - 1$

10. Use Problem 9 to confirm that the numbers $2^n - 1$ are composite for $n = 11, 23, 83, 131, 179, 183, 239, 251$.

Need to show $n = \frac{p-1}{2}$ for p of form $7+8k$.

Then, by #9, $p \mid 2^n - 1$, so $2^n - 1$ is composite.

11: $11 = \frac{p-1}{2}$, $p = 23 = 7 + (2)8$

23: $23 = \frac{p-1}{2}$, $p = 47 = 7 + (5)8$

83: $83 = \frac{p-1}{2}$, $p = 167 = 7 + (20)8$

131: $131 = \frac{p-1}{2}$, $p = 263 = 7 + (32)8$

179: $179 = \frac{p-1}{2}$, $p = 359 = 7 + (44)8$

183: $183 = \frac{p-1}{2}$, $p = 367 = 7 + (45)8$

239: $231 = \frac{p-1}{2}$, $p = 463 = 7 + 456 = 7 + (57)8$

251: $251 = \frac{p-1}{2}$, $p = 503 = 7 + 496 = 7 + (62)8$

All the "p" numbers above are prime.

11. Given that p and $q = 4p+1$ are both prime, prove the following:

(a) Any quadratic nonresidue of q is either a primitive root of q or has order 4 mod q.

Pf: Let a be a quadratic non-residue of q. It is assumed that $\gcd(a, q) = 1$.

$\therefore -1 = (a/q) \equiv a^{(q-1)/2} = a^{4p/2} = a^{2p} \pmod{q}$

$\therefore a^{4p} \equiv 1 \pmod{q}$

$\therefore$ order of a mod q is $1, 2, 4, p, 2p,$ or $4p$

(1) If order of a mod q is $4p = \phi(q)$, then a is a primitive root of q!

(2) $\therefore$ Assume order of a mod q is not $4p$.

1: Order of $a \neq 1$, for if $a^1 \equiv 1 \pmod{q}$, then $x^2 \equiv a \equiv 1 \pmod{q}$ would have a solution $(x = 1)$, which contradicts a as a quadratic non-residue.

2: If $a^2 \equiv 1 \pmod{q}$, then $a^{2p} \equiv 1 \pmod{q}$. But $-1 \equiv a^{2p} \pmod{q} \Rightarrow -1 \equiv 1$, or $q \mid 2$, an impossibility. $\therefore$ order of

$a \bmod q$ is not 2

p: Suppose $a^p \equiv 1 \pmod q$. $\therefore a^{2p} \equiv 1 \pmod q$, and since $a^{2p} \equiv -1 \pmod q$, then $1 \equiv -1 \pmod q \Rightarrow q \mid 2$, an impossibility. $\therefore$ order of a is not p.

$2p$: As above $a^{2p} \equiv 1 \pmod q$ contradicts $a^{2p} \equiv -1 \pmod q$, so order of a can't be $2p$.

$\therefore$ Since order can't be $1, 2, p, 2p, 4p$, order of $a \bmod q$ must be 4.

$\therefore$ (1) & (2) $\Rightarrow$ order of $a \bmod q$ is either $4p$ or 4. If $4p = \phi(q)$, then a is a primitive root of q.

(b) The integer 2 is a primitive root of q; in particular, 2 is a prim. root of the primes 13, 29, 53, and 173.

Pf: $\phi(q) = q - 1 = 4p + 1 - 1 = 4p$.

$\therefore$ Need to show $2^{4p} \equiv 1 \pmod q$, and order of 2 mod q can't be $1, 2, 4, p, 2p$.

Note $p \equiv 1 \pmod 4 \Rightarrow p = 1+4k$, so
$q = 4p+1 = 4+16k+1 = 5+16k = 5+8(2k)$
$\therefore p \equiv 1 \pmod 4 \Rightarrow q \equiv 5 \pmod 8$

$p \equiv 3 \pmod 4 \Rightarrow p = 3+4k$, so
$q = 12+16k+1 = 13+16k = 5+8(1+2k)$
$\therefore p \equiv 3 \pmod 4 \Rightarrow q \equiv 5 \pmod 8$.

$\therefore p$ prime and $q = 4p+1$ prime $\Rightarrow$
$q \equiv 5 \pmod 8$.

$\therefore (2/q) = -1$ by Th. 9.6

$\therefore -1 = (2/q) \equiv 2^{(q-1)/2} \pmod q = 2^{2p} \pmod q$

$\therefore 2^{2p} \equiv -1 \pmod q$ [1]

(a) Squaring [1], $2^{4p} \equiv 1 \pmod q$

(b) $2p$: Order of 2 can't be $2p$ by [1], for
$2^{2p} \equiv 1 \Rightarrow 1 \equiv -1 \pmod q \Rightarrow q | 2$.

p: Order of 2 can't be p, for $2^p \equiv 1 \Rightarrow$

$2^{2p} \equiv 1 \pmod q$ by squaring [1].

1: $2^1 \equiv 1 \pmod q \Rightarrow 1 \equiv 0 \Rightarrow q \mid 1$, so order can't be 1.

2: $2^2 \equiv 1 \pmod q \Rightarrow 3 \equiv 0 \Rightarrow q \mid 3$, and impossibility since $q = 4p+1$.

4: $2^4 \equiv 1 \pmod q \Rightarrow 15 \equiv 0 \Rightarrow q \mid 15 \Rightarrow$ $q = 3, 5,$ or 15 also an impossibility since $q = 4p+1$ and p is prime!

$\therefore$ Order of 2 mod q is not $1, 2, 4, p, 2p$ and so must be $4p$.

$\therefore$ (a) & (b) $\Rightarrow$ 2 is a primitive root of q

$13 = 1 + 4(3)$
$29 = 1 + 4(7)$
$53 = 1 + 4(13)$
$173 = 1 + 4(43)$

$\therefore$ 13, 29, 53, and 173 satisfy condition and so 2 is a prim. root for each.

12. If r is a primitive root of the odd prime p, prove that the product of the quadratic residues of p is congruent mod p to $r^{(p^2-1)/4}$ and the product of the nonresidues of p is congruent mod p to $r^{(p-1)^2/4}$.

Pf: (a) Product of quadratic residues is congruent to $r^{(p^2-1)/4}$

The quadratic residues are congruent to the even powers of r (corollary to Th. 9.4).

Let $a_1, a_2, \ldots, a_{\frac{p-1}{2}}$ be the $(p-1)/2$ quadratic residues of p.

$$\therefore a_1 a_2 \cdots a_{\frac{p-1}{2}} \equiv r^2 \cdot r^4 \cdots r^{p-1} \pmod{p}$$

$$\equiv (r^1)^2 \cdot (r^2)^2 \cdots (r^{\frac{p-1}{2}})^2 \pmod{p}$$

$$\equiv \left[r^1 \cdot r^2 \cdots r^{\frac{p-1}{2}}\right]^2 \pmod{p}$$

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

But $1+2+\cdots+\frac{p-1}{2} = \frac{p-1}{2}\left[\frac{p-1}{2}+1\right]/2$

$$= \frac{p-1}{2}\left(\frac{p+1}{2}\right)/2 = \left(\frac{p^2-1}{4}\right)/2$$

$$\therefore a_1 a_2 \cdots a_{\frac{p-1}{2}} \equiv \left(r^{1+2+\cdots+\frac{p-1}{2}}\right)^2 \pmod{p}$$

$$= \left[r^{\left(\frac{p^2-1}{4}\right)/2}\right]^2 \pmod{p}$$

$$= r^{\frac{p^2-1}{4}} \pmod{p}$$

$\therefore$ product of quadratic residues is congruent mod p to $r^{(p^2-1)/4}$.

(6) Product of quadratic nonresidues is congruent to $r^{(p-1)^2/4}$

The quadratic nonresidues are congruent to the odd powers of r (corollary p. 188)

$\therefore$ Let $a_1, a_2, \ldots, a_{\frac{p-1}{2}}$ be the quadratic nonresiduis

$$\therefore a_1 \cdot a_2 \cdots a_{\frac{p-1}{2}} \equiv r^1 \cdot r^3 \cdots r^{p-2} \pmod{p}$$

$$= r^{1+3+\cdots+p-2} \pmod{p}$$

But $1+3+\cdots+p-2 = \frac{p-1}{2}(p-1)/2$, as

There are $\frac{p-1}{2}$ terms.

$\therefore 1+3+\cdots+p-2 = \frac{(p-1)^2}{4}$.

$\therefore a_1 \cdot a_2 \cdots a_{\frac{p-1}{2}} \equiv r^{(p-1)^2/4} \pmod{p}$.

13. Establish that the product of the quadratic residues of the odd prime p is congruent mod p to 1 or -1 according as $p \equiv 3 \pmod 4$ or $p \equiv 1 \pmod 4$.

Pf: Let r be a primitive root of p.

Since $r^{p-1} \equiv 1 \pmod{p}$, then

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

As r is a prim. root of p, $r^{\frac{p-1}{2}}-1 \not\equiv 0 \pmod{p}$

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

$$r^{\frac{p-1}{2}} \equiv -1 \pmod{p}. \quad [1]$$

Let $a_1, a_2, \ldots, a_{\frac{p-1}{2}}$ be the quadratic residues of p.

$\therefore$ By prob. #12 above,

$$a_1 \cdot a_2 \cdots a_{\frac{p-1}{2}} \equiv r^{(p^2-1)/4} \pmod{p}.$$
$$\equiv \left(r^{\frac{p-1}{2}}\right)^{\left(\frac{p+1}{2}\right)} \pmod{p}$$
$$\equiv (-1)^{\frac{p+1}{2}} \pmod{p} \text{ by [1]}$$

If $p \equiv 1 \pmod 4$, then $p = 1 + 4K$, some k,
so $\frac{p+1}{2} = \frac{2+4k}{2} = 1 + 2k$, and odd integer.

$\therefore (-1)^{\frac{p+1}{2}} = -1$.

$\therefore p \equiv 1 \pmod 4 \Rightarrow a_1 \cdot a_2 \cdots a_{\frac{p-1}{2}} \equiv -1 \pmod p$

If $p \equiv 3 \pmod 4$, then $p = 3 + 4k$, some k,
so $\frac{p+1}{2} = \frac{4+4k}{2} = 2 + 2k$, an even integer.

$\therefore (-1)^{\frac{p+1}{2}} = 1$.

$\therefore p \equiv 3 \pmod 4 \Rightarrow a_1 \cdot a_2 \cdots a_{\frac{p-1}{2}} \equiv 1 \pmod p$.

14. (a) If the prime $p > 3$, show that p divides the sum of its quadratic residues.

pf: Let r be a primitive root of p.

Let $a_1, a_2, \ldots, a_{\frac{p-1}{2}}$ be the quadratic residues of p.

By corollary to Th. 9.4 (p. 188), $r^2, r^4, \ldots, r^{p-1}$ are congruent to the quadratic residues of p.

$$\therefore a_1 + a_2 + \cdots + a_{\frac{p-1}{2}} \equiv r^2 + r^4 + \cdots + r^{p-1} \pmod{p}$$

But $r^2 + r^4 + \cdots + r^{p-1} = r^2 \left(1 + r^2 + \cdots + r^{p-3}\right)$, for $p > 3$.

$$\therefore a_1 + a_2 + \cdots + a_{\frac{p-1}{2}} \equiv r^2 (1 + r^2 + \cdots + r^{p-3}) \pmod{p}, \quad [1]$$

for $p > 3$.

But $r^{p-1} \equiv 1 \pmod{p}$, as r is a prim. root.

$$\therefore r^2 + r^4 + \cdots + r^{p-1} \equiv 1 + r^2 + r^4 + \cdots + r^{p-3} \pmod{p},$$

for $p > 3$.

$$\therefore a_1 + a_2 + \cdots + a_{\frac{p-1}{2}} \equiv 1 + r^2 + r^4 + \cdots + r^{p-3} \pmod{p}, \quad [2]$$

for $p > 3$

Equating [1] and [2], for $p > 3$,

$$r^2(1+r^2+\dots+r^{p-3}) \equiv (1+r^2+\dots+r^{p-3}) \pmod{p} \quad [3]$$

But p must divide $(1+r^2+\dots+r^{p-3})$, for if not, then we cancel it on both sides of [3], and obtain $r^2 \equiv 1 \pmod{p}$. This is a contradiction since r is a primitive root of $p > 3$, so that $p-1 > 2$ and $r^{p-1} \equiv 1 \pmod{p}$.

Since $p \mid (1+r^2+\dots+r^{p-3})$, then from [1] or [2], $p \mid (a_1+a_2+\dots+a_{\frac{p-1}{2}})$

Note: Since $1+2+\dots+p-1 = \left(\frac{p-1}{2}\right)p$, then $p \mid (1+2+\dots+p-1)$.
$\therefore$ p also divides the sum of the quadratic nonresidues of p, for $p > 3$.

(b) If the prime $p > 5$, show that p divides the sum of the squares of its quadratic nonresidues.

Pf: Let r be a prim. root of p, and let $a_1, a_2, \dots, a_{\frac{p-1}{2}}$ be the quadratic nonresidues of p.

By corollary to Th. 9.4 (p. 188), $r^1, r^3, \ldots, r^{p-2}$ are congruent to the quadratic nonresidues of p.

$$\therefore\ a_1^2 + a_2^2 + \ldots + \left(a_{\frac{p-1}{2}}\right)^2 \equiv r^2 + r^6 + \ldots + r^{2(p-2)} \pmod p \quad [1]$$

Each term on the right side of [1] is described by r^{4k-2}, $1 \le k \le \frac{p-1}{2}$

And all terms on the right of [1] are incongruent mod p.

For if $r^{4k_1-2} \equiv r^{4k_2-2} \pmod p$, then by Th. 8.2, $4k_1-2 \equiv 4k_2-2 \pmod{p-1} \Leftrightarrow$

$4k_1 \equiv 4k_2 \pmod{p-1} \Leftrightarrow$

$k_1 \equiv k_2 \pmod{p-1}$

since $p > 5$, $p-1 > 4$, $\therefore \gcd(4, p-1) = 1$.

But $1 \le k_1, k_2 \le \frac{p-1}{2}$, so that $k_1, k_2 < p-1$.

$\therefore k_1 = k_2$

$\therefore r^{4k_1-2} \equiv r^{4k_2-2} \pmod p \Leftrightarrow k_1 = k_2$, so all terms on right side of [1] are incongruent mod p.

All the terms on the right side of [1]

are even, and there are $\frac{p-1}{2}$ such terms. Since they are incongruent, then the terms are congruent to $r^2, r^4, \dots, r^{p-1}$, in some order.

$$\therefore r^2 + r^6 + \dots + r^{2(p-2)} \equiv r^2 + r^4 + \dots + r^{p-1} \pmod{p} \quad [2]$$

By (a), the right side of [2] is divisible by p, and $\therefore$ so is the left side of [2], and $\therefore$ so is the left side of [1].

15. Prove that for any prime $p > 5$ there exist integers $1 \le a, b \le p-1$ for which $(a/p) = (a+1/p) = 1$ and
$(b/p) = (b+1/p) = -1$

That is, there are consecutive quadratic residues of p and consecutive nonresidues.

Pf: Since $x^2 \equiv 1$, $x^2 \equiv 4$, and $x^2 \equiv 9$ have solutions for all $p > 5$, then consider $x^2 \equiv 2$, $x^2 \equiv 5$, $x^2 \equiv 10$.

Now use 6(a).

For $p > 5$: $\gcd(2,p) = 1$, $\gcd(5,p) = 1$, so $\gcd(10,p) = 1$. By 6(a) one of 2, 5, or 10 must be a quadratic residue of p.

If $(2/p) = 1$, then 1, 2 are consecutive residues

If $(5|p)=1$, then 4 and 5 are consecutive residues

If $(10|p)=1$, then 9 and 10 are consecutive residues.

Since the above showed at least one pair of consecutive residues for $p>5$, then consider the remaining $p-3$ terms (there are $p-1$ residues + nonresidues, so subtract out the 2 consecutive residues). Let a_k, a_{k+1} be the consecutive residues.

$\therefore$ Consider the terms:

$$1, 2, \dots, a_k, a_{k+1}, \dots, a_{p-1}$$

If 2, 3 are consecutive nonresidues, then we're done.

So suppose 2, 3 are not consecutive nonresidues.
$\therefore$ Since 1 and 4 are always residues, then in the list, there are at least 3 residues among 1, 2, 3, 4.
Suppose the remaining even number of terms $5, 6, \dots, p-1$ alternate with

respect to residue/nonresidue.
Then in the remaining terms $5, 6, \ldots, p-1$, the number of residues = number of nonresidues, and so overall, the number of residues is at least 2 greater than the number of nonresidues.

$\therefore$ There must be consecutive nonresidues in the list $1, 2, \ldots, p-1$.

16. (a) Let p be an odd prime and $\gcd(a,p) = \gcd(k,p) = 1$. Show that if the equation $x^2 - ay^2 = kp$ admits a solution, then $(a/p) = 1$; for example, $(2/7) = 1$ because $6^2 - 2\cdot 2^2 = 4\cdot 7$.

Pf: Suppose x, y solve $x^2 - ay^2 = kp$.

(1) $\gcd(p, y) = 1$

For if $\gcd(p,y) = n > 1$, then since p is prime, then $y = np$.

$\therefore x^2 = a(np)^2 + kp = an^2p^2 + kp$.
$\therefore p \mid x$, so $x = mp$, some $m \geq 1$.

$\therefore\ m^2p^2 = an^2p^2 + kp$, or

$m^2p - an^2p = p(m^2 - an^2) = k \Rightarrow p \mid k$

But $\gcd(k,p) = 1$. $\therefore \gcd(p,y) = 1$

(2) By (1), $y^{p-1} \equiv 1 \pmod{p}$ by Euler's Th.

$\therefore\ x^2 - ay^2 = kp \Leftrightarrow x^2 \equiv ay^2 \pmod{p}$

$\therefore\ x^2 y^{p-1} \equiv ay^2 \pmod{p}$.

p is odd, so $p-1 \geq 2$, so $y^{p-1} \geq y^2$.
Using (1) again to divide by y^2,

$$x^2 y^{p-3} \equiv a \pmod{p}$$

$$\therefore\ x^2 y^{p-3} \cdot y^{p-1} \equiv a \pmod{p}$$

$$x^2 y^{2p-4} = (xy^{p-2})^2 \equiv a \pmod{p}$$

$\therefore$ Let $z = xy^{p-2}$, so $z^2 \equiv a \pmod{p}$

$\therefore\ (a/p) = 1$

Incidentally, $\gcd(x,p)=1$

For if $x=np$, then $(np)^2-ay^2=kp$, or

$n^2p^2-kp=ay^2$, $p(np-k)=ay^2$.

$\therefore p \mid a$ or $p \mid y$. This contradicts (1) and $\gcd(a,p)=1$.

(b) By considering the equation $x^2+5y^2=7$, demonstrate that the converse of the result in part (a) need not hold.

$(-5/7)=1$, for $(-5)^{(7-1)/2}=-5^3=-125=-7\cdot 18+1$
so $(-5)^{(7-1)/2}\equiv 1 \pmod 7$

But there is no integer solution to $x^2+5y^2=7$.

Only possibilities are $x=0,1,2$, $y=0,1$ and these don't work.

(c) Show that for any prime $p\equiv \pm 3 \pmod 8$, the equation $x^2-2y^2=p$ has no solution.

Pf: Suppose $x^2-2y^2=p$ has a solution.

Since p is odd, $\gcd(2,p)=1$ and clearly $\gcd(1,p)=1$.

$\therefore$ By (a), $(2/p)=1$.

But $p \equiv \pm 3 \pmod 8 \Leftrightarrow$
$p \equiv 3 \pmod 8$ or $p \equiv 5 \pmod 8$,

and by Th. 9.6, $(2/p)=-1$.

$\therefore$ $x^2-2y^2=p$ can't have a solution.

17. Prove that the odd prime divisors p of the integers 9^n+1 are of the form $p \equiv 1 \pmod 4$

Pf: Let p be an odd prime divisor of 9^n+1

$\therefore$ $9^n+1 \equiv 0 \pmod p$, or

$(3^2)^n+1 \equiv 0 \pmod p$, or $(3^n)^2 \equiv -1 \pmod p$

Since p is odd, either $p \equiv 1 \pmod 4$ or $p \equiv 3 \pmod 4$.

By corollary to Th. 9.2 (p. 187) if $p \equiv 3 \pmod 4$,
There can be no solution to $x^2 \equiv -1 \pmod p$,
so that there is no n s.t. $(3^n)^2 \equiv -1 \pmod p$

$\therefore$ If p is to be a divisor of $9^n + 1$, it must be of the form $p \equiv 1 \pmod 4$.

18. For a prime $p \equiv 1 \pmod 4$, verify that the sum of the quadratic residues of p is equal to $p(p-1)/4$

Pf: (1) If $(a/p) = 1$, Then $(p-a/p) = 1$

For since $a^{\frac{p-1}{2}} \equiv 1 \pmod p$, and

$$(p-a)^n = p^n + \dots + (-a)^n = p^n + \dots + (-1)^n a^n,$$

$$\text{Then } (p-a)^{\frac{p-1}{2}} \equiv (-1)^{\frac{p-1}{2}} a^{\frac{p-1}{2}} \pmod p$$

For $p \equiv 1 \pmod 4$, $p - 1 = 4K$, some K,
so $(-1)^{\frac{p-1}{2}} = (-1)^{2K} = 1$.

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

$\therefore$ for $p \equiv 1 \pmod 4$, $p-a$ is also a quad. residue.

(2) Let $a_1, \ldots, a_r$ be the quadradic residues of p less than $p/2$.

$\therefore p-a_1, \ldots, p-a_r$ are quadratic residues of p, all less than p, and $p-a_i > p/2$ (since $a_i < p/2$,

then $-a_i > -p/2$, $p-a_i > p - p/2 = p/2$).

Since all these residues are less than p, they are all incongruent.

(3) The a_i and $p-a_i$ are all the quadratic residues of p.

For if a_x is a quadratic residue of p s.t. $p/2 < a_x < p$, then $p-a_x$ is a residue by (2), and $0 < p-a_x < p/2$, so $p-a_x$ must be one of the a_i, since that set consisted of <u>all</u> residues less than $p/2$.
$\therefore p-(p-a_x)$ must be one of the $p-a_i$.
But $p-(p-a_x) = a_x$, so a_x is one of a_i.

(4) Since there are a total of $\frac{p-1}{2}$ quadratic

residues (Th. 9.4), (3) $\Rightarrow$ There are $\frac{p-1}{4}$ residues $< p/2$ and $\frac{p-1}{4}$ residues $> p/2$.

$\therefore r = \frac{p-1}{4}$ in the sequence $a_1, \ldots, a_r$.

(5) $\therefore$ Sum $= (a_1 + \ldots + a_r) + [(p-a_1) + \ldots + (p-a_r)]$

$$= p + \ldots + p = rp = \left(\frac{p-1}{4}\right)p$$

Note that from (1), for $p \equiv 3 \pmod 4$,

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

so if a is a quadratic residue of p, $\underline{p-a}$ is a quadratic <u>nonresidue</u>.