9.3 Quadratic Reciprocity

Note Title 7/17/2006

1. Evaluate the following Legendre symbols:

(a) $(71/73)$

$71 \equiv -1 \pmod 4$, $73 \equiv 1 \pmod 4$. $\therefore (71/73) = (73/71)$

$(73/71) = (71+2/71) = (2/71)$

$71 = 7 + 8(8) \Rightarrow 71 \equiv 7 \pmod 8$, so $(2/71) = 1$

$\therefore (71/73) = 1$

(b) $(-219/383)$

$219 = 3 \cdot 73 \qquad 383 \equiv 3 \pmod 4$

$$\therefore (-219/383) = (-1/383)(3/383)(73/383)$$
$$= (-1)[-(383/3)](383/73)$$
$$= (2/3)(18/73)$$
$$= (-1)(2 \cdot 3^2/73) = -(2/73)$$
$$= -1 \quad \text{as } 73 \equiv 1 \pmod 4$$

$\therefore (-219/383) = -1$

(c) $(461/773)$

$461 \equiv 1 \pmod 4$

$\therefore (461/773) = (773/461)$
$= (312/461) = (2^3 \cdot 3 \cdot 13/461)$
$= (2 \cdot 3 \cdot 13/461)$
$= (2/461)(3/461)(13/461)$
$= (-1)(461/3)(461/13)$
$= (-1)(2/3)(6/13)$
$= (-1)(-1)(2/13)(3/13)$
$= (-1)(3/13) = (-1)(13/3)$, as $13 \equiv 1 \pmod 4$
$= (-1)(1/3)$
$= -1$

$\therefore (461/773) = -1$

(d) $(1234/4567)$ $1234 = 2 \cdot 617$

$4567 \equiv 3 \pmod 4$ $617 \equiv 1 \pmod 4$

$\therefore (1234/4567) = (2/4567)(617/4567)$

$= (1)(4567/617)$ as $4567 \equiv 7 \pmod 8$
$= (248/617)$

$= (2^3 \cdot 31 / 617) = (2/617)(31/617)$

$= (1)(31/617)$ as $617 \equiv 1 \pmod 8$

$= (617/31) = (28/31)$

$= (4 \cdot 7/31) = (7/31)$

$= -(31/7)$ as $7 \equiv 3 \pmod 4$, $31 \equiv 3 \pmod 4$

$= -(3/7) = (7/3) = (1/3) = 1$

$\therefore (1234/4567) = 1$

(e) $(3658/12703)$ $\quad 3658 = 2 \cdot 31 \cdot 59$

$12703 \equiv 7 \pmod 8$ $\quad \therefore (2/12703) = 1$

$\therefore (2/12703)(31/12703)(59/12703)$

$= (31/12703)(59/12703)$ $\quad 12703 \equiv 3 \pmod 4$

$31 \equiv 3 \pmod 4$

$= (12703/31)(12703/59)$ $\quad 59 \equiv 3 \pmod 4$

$= (24/31)(18/59)$

$= (6/31)(2/59) = -(6/31)$ as $59 \equiv 3 \pmod 8$

$= -(2/31)(3/31) = -(3/31)$ as $(2/31) = 1$

$= (31/3) = (1/3) = 1$

$\therefore (3658/12703) = 1$

2. Prove that 3 is a quadratic nonresidue of all primes of the form $2^{2n}+1$, and all primes of the form 2^p-1, where p is an odd prime.

Pf: (1) For all n, $4^n \equiv 4 \pmod{12}$

Clearly true for $n=1$

Assume true for n.

Then $4^{n+1} = 4^n \cdot 4 \equiv 4 \cdot 4 = 16 \equiv 4 \pmod{12}$

(2) $\therefore 2^{2n} = 4^n \equiv 4 \pmod{12}$

$\therefore 2^{2n}+1 \equiv 5 \pmod{12}$

(3) Let p be a prime of form $2^{2n}+1$.

$\therefore$ By Th. 9.10 and (2) above, $(3/p) = -1$, and so 3 is a quadratic nonresidue of prime $2^{2n}+1$!

(4) If p is an odd prime, $p = 2n+1$, some n.

$\therefore 2^p - 1 = 2^{2n+1} - 1 = 4^n \cdot 2 - 1$

By (1), $4^n \cdot 2 - 1 \equiv 4 \cdot 2 - 1 \pmod{12}$

$\equiv 7 \pmod{12}$

$\equiv -5 \pmod{12}$

$\therefore 2^p - 1 \equiv -5 \pmod{12}$

$\therefore$ By Th. 9.10, $\left(3/(2^p-1)\right) = -1$, so 3 is a quadradic nonresidue of prime 2^p-1.

3. Determine whether the following quadratic congruences are solvable:

(a) $x^2 \equiv 219 \pmod{419}$

419 is prime. $\therefore$ Consider $(219/419)$

$219 = 3 \cdot 73 \qquad 419 \equiv 3 \pmod 4, \quad 73 \equiv 1 \pmod 4$

$\therefore (219/419) = (3/419) \cdot (73/419)$

$(3/419) = -(419/3) = -(2/3) = -(-1) = 1$

$(73/419) = (419/73) = (5 \cdot 73 + 54/73)$
$= (54/73) = (2 \cdot 3^3/73) = (2 \cdot 3/73)$
$= (2/73) \cdot (3/73) = 1 \cdot (3/73)$
$= (73/3) = (1/3) = 1$

$\therefore (219/419) = 1$, so <u>solvable</u>

(b) $3x^2 + 6x + 5 \equiv 0 \pmod{89}$ $\qquad$ [1]

$\gcd(4, 89) = 1$, $\gcd(3, 89) = 1$.

$\therefore$ [1] $\Leftrightarrow 12(3x^2 + 6x + 5) \equiv 0 \pmod{89}$
$\Leftrightarrow 36x^2 + 72x + 60 \equiv 0 \pmod{89}$

$\Leftrightarrow (6x+6)^2 + 24 \equiv 0 \pmod{89}$

$\Leftrightarrow (6x+6)^2 \equiv 65 \pmod{89}$

Let $y = 6x+6$. $\therefore$ [1] $\Leftrightarrow y^2 \equiv 65\ (89)$

$\therefore$ Consider $(65/89) = (13/89)(5/89)$

$13 \equiv 1 \pmod 4$, $5 \equiv 1 \pmod 4$, $89 \equiv 1 \pmod{89}$

$\therefore (13/89) = (89/13) = (11/13) = (13/11)$

$= (2/11) = -1$ as $11 \equiv 3 \pmod 8$

$(5/89) = (89/5) = (4/5) = (2^2/5) = 1$

$\therefore (65/89) = -1$

$\therefore$ [1] is <u>not solvable</u>.

(c) $2x^2 + 5x - 9 \equiv 0 \pmod{101}$ [1]

As in (a) Let $y = 2ax+b$, $d = b^2 - 4ac$,
so [1] $\Leftrightarrow y^2 \equiv d = 97 \pmod{101}$

$\therefore$ Consider $(97/101)$. 97 is prime

$97 \equiv 1 \pmod 4$, $101 \equiv 1 \pmod 4$

$\therefore (97/101) = (101/97) = (4/97) = (2^2/97) = 1$

$\therefore$ [1] is solvable.

4. Verify that if p is an odd prime, then

$$(-2/p) = \begin{cases} 1 & \text{if } p \equiv 1 \pmod 8 \text{ or } p \equiv 3 \pmod 8 \\ -1 & \text{if } p \equiv 5 \pmod 8 \text{ or } p \equiv 7 \pmod 8 \end{cases}$$

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

$$(-1/p) = \begin{cases} 1 & \text{if } p \equiv 1 \pmod 4 \\ -1 & \text{if } p \equiv 3 \pmod 4 \end{cases}$$ Corollary to Th. 9.2 p. 187

$$(2/p) = \begin{cases} 1 & \text{if } p \equiv 1 \pmod 8 \text{ or } p \equiv 7 \pmod 8 \\ -1 & \text{if } p \equiv 3 \pmod 8 \text{ or } p \equiv 5 \pmod 8 \end{cases}$$ Th. 9.6

$\therefore$ if $p \equiv 1 \pmod 8$, then $p \equiv 1 \pmod 4$, so
$(-2/p) = (-1/p)(2/p) = 1 \cdot 1 = 1$ [1]

if $p \equiv 3 \pmod 8$, then $p \equiv 3 \pmod 4$, so
$(-2/p) = (-1/p)(2/p) = -1 \cdot -1 = 1$ [2]

if $p \equiv 5 \pmod 8$, then $p \equiv 5 \pmod 4 \equiv 1 \pmod 4$.
$(-2/p) = (-1/p)(2/p) = 1 \cdot -1 = -1$ [3]

if $p \equiv 7 \pmod 8$, Then $p \equiv 7 \pmod 4 \equiv 3 \pmod 4$

$(-2/p) = (-1/p)(2/p) = -1 \cdot 1 = -1$ [4]

$$\therefore (-2/p) = \begin{cases} 1 & \text{if } p \equiv 1 \pmod 8 \text{ or } p \equiv 3 \pmod 8 \quad [1], [2] \\ -1 & \text{if } p \equiv 5 \pmod 8 \text{ or } p \equiv 7 \pmod 8 \quad [3], [4] \end{cases}$$

5. (a) Prove that if $p > 3$ is an odd prime, then

$$(-3/p) = \begin{cases} 1 & \text{if } p \equiv 1 \pmod 6 \\ -1 & \text{if } p \equiv 5 \pmod 6 \end{cases}$$

Pf: $(-3/p) = (-1/p) \cdot (3/p)$

(1) Suppose $p \equiv 1 \pmod 6$. Then $p - 1 = 6K$, some K.

(a) If K is even, Then $K = 2K'$, so $p - 1 = 12K'$, or $p \equiv 1 \pmod{12}$

$\therefore (-1/p) = (-1)^{\frac{p-1}{2}} = (-1)^{\frac{12K'}{2}} = (-1)^{6K'} = 1$

$(3/p) = 1$, by Th. 9.10

$\therefore (-3/p) = 1 \cdot 1 = 1$

(b) If K is odd, Then $K = 2K' + 1$, so $p - 1 = 6(2K' + 1) = 6 + 12K'$, or

$p \equiv 7 \pmod{12} \Leftrightarrow p \equiv -5 \pmod{12}$

$\therefore (-1/p) = (-1)^{\frac{p-1}{2}} = (-1)^{3+6k'} = -1$

$(3/p) = -1$, by Th. 9.10

$\therefore (-3/p) = -1 \cdot -1 = 1$

$\therefore p \equiv 1 \pmod 6 \Rightarrow (-3/p) = 1$

(2) Suppose $p \equiv 5 \pmod 6$. Then $p-5 = 6k$, some k

(a) If k is even, $k = 2k'$, some k', so
$p-5 = 12k'$, or $p \equiv 5 \pmod{12}$

$\therefore (-1/p) = (-1)^{\frac{p-1}{2}} = (-1)^{4+12k'} = 1$

$(3/p) = -1$, by Th. 9.10

$\therefore (-3/p) = 1 \cdot -1 = -1$

(b) If k is odd, $k = 2k'+1$, so
$p-5 = 12k'+6$, or $p \equiv 11 \pmod{12} \Leftrightarrow$
$p \equiv -1 \pmod{12}$

$\therefore (-1/p) = (-1)^{\frac{p-1}{2}} = (-1)^{5+6k'} = -1$

$(3/p) = 1$, by Th. 9.10

$\therefore (-3/p) = -1 \cdot 1 = -1$

$\therefore$ $p \equiv 5 \pmod 6 \Rightarrow (-3/p) = -1$

Note: $p \not\equiv 3 \pmod 6$, for if so, then
$p-3 = k \cdot 3 \cdot 2$, so $3 \mid p-3 \Rightarrow 3 \mid p$
Similarly for Th. 9.10

(b) Using part (a), show that there are infinitely many primes of the form $6k+1$.

Pf: Assume there are a finite number of primes of form $6k+1$, say, $p_1, \ldots, p_r$.

Consider $N = (2p_1p_2 \cdots p_r)^2 + 3$

$3 \nmid N$, for if $3 \mid N$, then $3 \mid (2p_1 \cdots p_r)^2$, so 3 must be one of p_i, but 3 is not of form $6k+1$.

$\therefore$ There must be some odd prime divisor, $p > 3$, of N.
And $p \neq p_i$, for if $p = p_i$, some i, then $p \mid N \Rightarrow p \mid 3$, a contradiction.

$\therefore N \equiv 0 \pmod{p}$, or equivalently,
$(2p_1p_2\cdots p_r)^2 \equiv -3 \pmod{p}$

$\therefore (-3/p) = 1$

$\therefore$ by (a), $p \equiv 1 \pmod{6}$, for if $p \equiv 5 \pmod{6}$, then $(-3/p) = -1$, and $p \not\equiv 3 \pmod{6}$ as shown above.

$\therefore p$ is of form $6k+1$, contradicting $p \neq p_i$.

$\therefore$ infinitely many primes of form $6k+1$.

6. Use Theorem 9.2 and problems 4 and 5 to determine which primes can divide integers of the forms n^2+1, n^2+2, or n^2+3 for some value of n.

(a) $p \mid n^2+1 \iff n^2 \equiv -1 \pmod{p}$

For p odd, $(-1/p) = (-1)^{\frac{p-1}{2}}$, so $(-1/p) = 1 \iff \frac{p-1}{2}$ is even

$\therefore p > 3$, $p = 2k+1$, so $\frac{(2k+1)-1}{2}$ is even,

so $\frac{2k}{2} = k$ is even, so $k = 2k'$, $\therefore$
$p = 2(2k')+1 = 4k'+1$

$\therefore$ for p odd, $p \equiv 1 \pmod 4$

if $p=2$, n^2+1 must be even.

$\therefore p \mid n^2+1$ $\begin{cases} \text{if } n \text{ is odd, } p=2 \text{ or } p\equiv 1 \pmod 4 \\ \text{if } n \text{ is even, } p \equiv 1 \pmod 4 \end{cases}$

(b) $p \mid n^2+2 \iff n^2 \equiv -2 \pmod p$

If n is even, $2 \mid n^2+2$.
If n is odd, n^2+2 is odd, $2 \nmid n^2+2$

For p odd, $n^2 \equiv -2 \pmod p$ is solvable $\iff$
$(-2/p) = 1$.
By prob. (4) above, $(-2/p)=1$ if $p \equiv 1 \pmod 8$
or $p \equiv 3 \pmod 8$

$\therefore p \mid n^2+2$ $\begin{cases} \text{if } n \text{ is even, } p=2 \text{ or } p \equiv 1 \pmod 8 \text{ or} \\ \qquad p\equiv 3 \pmod 8 \\ \text{if } n \text{ is odd, } p \equiv 1 \pmod 8 \text{ or} \\ \qquad p \equiv 3 \pmod 8 \end{cases}$

(c) $p \mid (n^2+3) \iff n^2 \equiv -3 \pmod p$

Problem (5) above addresses $p > 3$, in

which case $(-3/p) = 1$ if $p \equiv 1 \pmod{6}$.

For $p = 2$,
If n is even, n^2+3 is odd, $2 \nmid n^2+3$
If n is odd, n^2+3 is even, so $2 \mid n^2+3$

For $p = 3$, $n^2+3 \equiv 0 \pmod{3} \Leftrightarrow n^2 \equiv 0 \pmod{3}$
$\Leftrightarrow 3 \mid n$

$$\therefore p \mid n^2+3 \begin{cases} \text{if } n \text{ is even, and } p \equiv 1 \pmod{6} \\ \quad \text{if also } 3 \mid n,\ p = 3 \\ \text{if } n \text{ is odd, } p = 2 \text{ or } p \equiv 1 \pmod{6} \\ \quad \text{if also } 3 \mid n,\ p = 3 \end{cases}$$

7. Prove there exist infinitely many primes of form $8k+3$.

Pf: Use prob. (4) above since it has conditions for $(-2/p)$ using $\pmod{8}$.

$\therefore$ Assume finitely many primes of form $8k+3$, which is odd, say $p_1, p_2, \dots, p_r$.

Consider $N = (p_1 p_2 \cdots p_r)^2 + 2$ (N is odd).
N must contain an odd prime divisor

p s.t. $p \neq p_i$, for if $p = p_i$, some i, then $p | N$ and $p | (p_1 \cdots p_r)^2 \Rightarrow p | 2$.

$\therefore N \equiv 0 \pmod{p}$ or $(p_1 \cdots p_r)^2 \equiv -2 \pmod{p}$

$\therefore$ By prob. (4) above, $p \equiv 1 \pmod{8}$ or $p \equiv 3 \pmod{8}$

Suppose $N = q_1^{k_1} \cdots q_s^{k_s}$ and all q_i are s.t. $q_i \equiv 1 \pmod{8}$.

$\therefore N = q_1^{k_1} q_2^{k_2} \cdots q_s^{k_s} \equiv 1 \pmod{8}$ [1]

But $p_i \equiv 3 \pmod{8}$, so $p_i^2 \equiv 9 \equiv 1 \pmod{8}$

$\therefore p_1^2 \cdots p_r^2 \equiv 1 \pmod{8}$

$\therefore (p_1 \cdots p_r)^2 + 2 \equiv 3 \pmod{8}$

$\therefore N \equiv 3 \pmod{8}$, a contradiction to [1].

$\therefore$ All q_i can't be s.t. $q_i \equiv 1 \pmod{8}$, So there must be some odd prime divisor $q_i = p$ of N s.t. $p \equiv 3 \pmod{8}$. And this contradicts p_i above being finite.

8. Find a prime number p that is simultaneously expressible in the forms x^2+y^2, u^2+2v^2, and r^2+3s^2.

If $x^2+y^2=p$, then $x^2 \equiv -y^2 \pmod{p}$, or

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

Similarly, $\frac{u^2}{v^2} \equiv -2 \pmod{p}$, $\frac{r^2}{s^2} \equiv -3 \pmod{p}$

where $\left(\frac{x}{y}\right)^2$, $\left(\frac{u}{v}\right)^2$, and $\left(\frac{r}{s}\right)^2$ are integers.

$\therefore$ Look at $(-1/p) = (-2/p) = (-3/p)$ as a minimum condition.

$(-1/p) = 1$, if $p \equiv 1 \pmod{4}$

$(-2/p) = 1$, if $p \equiv 1 \pmod{8}$ or $p \equiv 3 \pmod{8}$ [prob. 4]

$(-3/p) = 1$, if $p \equiv 1 \pmod{6}$ [prob. 5]

$\therefore$ if $p \equiv 1 \pmod{8}$, then $p \equiv 1 \pmod{4}$

if $p \equiv 1 \pmod{24}$, then $p \equiv 1 \pmod{4}$, $p \equiv 1 \pmod{8}$, and $p \equiv 1 \pmod{6}$.

$\therefore$ Consider $p = 1 + 24k$, for $k = 1, 2, 3, \ldots$

$\therefore$ Look at $25, 49, 73, \ldots$

73 is prime and $73 \equiv 1 \pmod 4$, $73 \equiv 1 \pmod 8$, and $73 \equiv 1 \pmod 6$.

To clean up, $8^2 + 3^2 = 73$

$1^2 + 2(6)^2 = 73$

$5^2 + 3(4)^2 = 73$

These were obtained by trial + error, but could have chosen different prime s.t. $p = 1 + 24k$ and then chosen x, y s.t. $\left(\frac{x}{y}\right)^2$ is an integer, etc.

9. If p and q are odd primes satisfying $p = q + 4a$ for some a, establish that $(a/p) = (a/q)$, and in particular, that $(6/37) = (6/13)$

Pf: Since $p = q + 4a$, $(p/q) = (q + 4a/q)$

But $q + 4a \equiv 4a \pmod q$, so $(q + 4a/q) = (4a/q)$
$= (2^2 a/q) = (a/q)$.

$\therefore (p/q) = (a/q)$ [1]

Similarly, $q = p - 4a$, so $(q/p) = (p-4a/p) = (-a/p)$

$\therefore (q/p) = (-a/p) = (-1/p)(a/p)$ [2]

If $p \equiv 1 \pmod 4$, Then $(-1/p) = 1$, [2] becomes

$(q/p) = (a/p)$ [2']

But by corollary 2 to Th. 9.9 (p. 198), $(p/q) = (q/p)$.

$\therefore$ By [1] and [2'], $(a/q) = (a/p)$

If $p \equiv 3 \pmod 4$, Then $(-1/p) = -1$, [2] becomes

$(q/p) = -(a/p)$ [2'']

Note That $p \equiv 4a + q \pmod 4 \Rightarrow p \equiv q \pmod 4$

$\therefore q \equiv 3 \pmod 4$

$\therefore$ By corollary 2 to Th. 9.9, $(p/q) = -(q/p)$

$\therefore$ By [1] and [2''], $(a/q) = (p/q) = -(q/p) =$
$= -(-(a/p))$

$\therefore (a/q) = (a/p)$.

10. Establish each of the following assertions:

(a) $(5/p) = 1 \iff p \equiv 1, 9, 11,$ or $19 \pmod{20}$

Pf: By def. of $(5/p)$, p is an odd prime.

(1) If $p \equiv 1, 9, 11,$ or $19 \pmod{20}$, Then

$p \equiv 1, 9, 11,$ or $19 \pmod 5 \Rightarrow$

$p \equiv 1$ or $4 \pmod 5$

Since $5 \equiv 1 \pmod 4$, Then $(5/p) = (p/5)$

$\therefore (5/p) = (p/5) = (1/5)$ or $(4/5) = (1/5)$

and $(1/5) = 1$.

$\therefore (5/p) = 1$.

(2) Suppose $(5/p) = 1$. Since $5 \equiv 1 \pmod 4$,

Then $(5/p) = (p/5) = 1$.

$\therefore 1 \equiv p^{\frac{5-1}{2}} \pmod 5$, or $1 \equiv p^2 \pmod 5$.

$\therefore p \equiv 1$ or $4 \pmod 5$.

Also, general for any odd number,

$p \equiv 1$ or $3 \pmod 4$.

$\therefore p \equiv 1 \pmod 5$ or $p \equiv 4 \pmod 5$

and $p \equiv 1 \pmod 4$ or $p \equiv 3 \pmod 4$

$\therefore\ 4p \equiv 4 \pmod{20}$ or $4p \equiv 16 \pmod{20}$
and $5p \equiv 5 \pmod{20}$ or $5p \equiv 15 \pmod{20}$

Substracting, $p \equiv 1$ or $-11 \pmod{20}$
or $p \equiv 11$, or -1 (mod 20

$\Rightarrow\ p \equiv 1, 9, 11,$ or $19 \pmod{20}$

(b) $(6/p) = 1 \iff p \equiv 1, 5, 19,$ or $23 \pmod{24}$

Pf: (1) Suppose $p \equiv 1, 5, 19,$ or $23 \pmod{24}$

Let $p \equiv 1 \pmod{24}$

$\therefore\ p \equiv 1 \pmod{12} \Rightarrow (3/p) = 1$ (Th. 9.10)
and $p \equiv 1 \pmod{8} \Rightarrow (2/p) = 1$ (Th. 9.6)

$\therefore\ (6/p) = (3/p)(2/p) = 1$

Let $p = 5 \pmod{24}$

$\therefore\ p \equiv 5 \pmod{12} \Rightarrow (3/p) = -1$ (Th. 9.10)
$p \equiv 5 \pmod{8} \Rightarrow (2/p) = -1$ (Th. 9.6)

$\therefore\ (6/p) = (3/p)(2/p) = (-1)(-1) = 1$

Let $p \equiv 19 \pmod{24}$

$\therefore p \equiv 19 \equiv 7 \equiv -5 \pmod{12} \Rightarrow (3/p) = -1$

$p \equiv 19 \equiv 3 \pmod{8} \Rightarrow (2/p) = -1$

$\therefore (6/p) = (3/p)(2/p) = (-1)(-1) = 1$

Let $p \equiv 23 \pmod{24}$

$\therefore p \equiv 23 \equiv 11 \equiv -1 \pmod{12} \Rightarrow (3/p) = 1$

$p \equiv 23 \equiv 7 \pmod{8} \Rightarrow (2/p) = 1$

$\therefore (6/p) = (3/p)(2/p) = 1$

(2) Suppose $(6/p) = 1$

$\therefore (3/p)(2/p) = 1 \Rightarrow$

$(3/p) = 1$ and $(2/p) = 1$

or $(3/p) = -1$ and $(2/p) = -1$

(a) If $(3/p) = 1$ then $p \equiv \pm 1 \pmod{12}$ by Th. 9.10, for $p \not\equiv 3$ or $9 \pmod{12}$, since then $3 \mid p$.

Also, $(2/p) = 1 \Rightarrow p \equiv \pm 1 \pmod{8}$ by Th. 9.6

(1) $p \equiv 1 \pmod{12}$ and $p \equiv 1 \pmod{8} \Rightarrow$

$$\left.\begin{array}{l} 2p \equiv 2 \pmod{24} \\ 3p \equiv 3 \pmod{24} \end{array}\right\} \Rightarrow \underline{p \equiv 1} \pmod{24} \text{ by subtracting}$$

(2) $p \equiv 1 \pmod{12}$ and $p \equiv -1 \pmod{8} \Rightarrow$

$$\left.\begin{array}{l} 2p \equiv 2 \pmod{24} \\ 3p \equiv -3 \pmod{24} \end{array}\right\} \Rightarrow p \equiv -5 \Rightarrow \underline{p \equiv 19} \pmod{24}$$

(3) $p \equiv -1 \pmod{12}$ and $p \equiv 1 \pmod{8} \Rightarrow$

$$\left.\begin{array}{l} 2p \equiv -2 \pmod{24} \\ 3p \equiv 3 \pmod{24} \end{array}\right\} \Rightarrow \underline{p \equiv 5} \pmod{24}$$

(4) $p \equiv -1 \pmod{12}$ and $p \equiv -1 \pmod{8} \Rightarrow$

$$\left.\begin{array}{l} 2p \equiv -2 \pmod{24} \\ 3p \equiv -3 \pmod{24} \end{array}\right\} \Rightarrow p \equiv -1 \Rightarrow \underline{p \equiv 23} \pmod{24}$$

$\therefore (6/p) = 1 \Rightarrow p = 1, 5, 19, \text{ or } 23 \pmod{24}$

(c) $(7/p) = 1 \Leftrightarrow p \equiv 1, 3, 9, 19, 25, \text{ or } 27 \pmod{28}$

Pf: (1) Suppose $(7/p) = 1$

(a) If $p \equiv 1 \pmod 4$, Then $(7/p) = (p/7)$

$\therefore 1 \equiv p^{\frac{7-1}{2}} = p^3 \pmod 7$

$\therefore$ running through $p \equiv 1, 2, 3, 4, 5, 6$ and looking at p^3, we get

$p \equiv 1, 2, \text{ or } 4 \pmod 7$

$\therefore\ p \equiv 1 \pmod 4$ and $p \equiv 1, 2, \text{ or } 4 \pmod 7$

(1) $\left.\begin{array}{l} p \equiv 1 \pmod 4 \\ p \equiv 1 \pmod 7 \end{array}\right\} \begin{array}{l} 7p \equiv 7 \pmod{28} \\ 4p \equiv 4 \pmod{28} \Rightarrow 8p \equiv 8 \end{array}$

$\therefore\ \underline{p \equiv 1} \pmod{28}$

(2) $\left.\begin{array}{l} p \equiv 1 \pmod 4 \\ p \equiv 2 \pmod 7 \end{array}\right\} \begin{array}{l} 7p \equiv 7 \pmod{28} \\ 4p \equiv 8 \pmod{28} \Rightarrow 8p \equiv 16 \end{array}$

$\therefore\ \underline{p \equiv 9} \pmod{28}$

(3) $\left.\begin{array}{l} p \equiv 1 \pmod 4 \\ p \equiv 4 \pmod 7 \end{array}\right\} \begin{array}{l} 7p \equiv 7 \pmod{28} \\ 4p \equiv 16 \pmod{28} \Rightarrow 8p \equiv 32 \end{array}$

$\therefore\ \underline{p \equiv 25} \pmod{28}$

(b) If $p \equiv 3 \pmod 4$, Then $(7/p) = -(p/7)$
since $7 \equiv 3 \pmod 4$

$\therefore\ -1 \equiv p^{\frac{7-1}{2}} = p^3 \pmod 7$

$\therefore\ p \equiv 3, 5, \text{ or } 6 \pmod 7, \Rightarrow$

$4p \equiv 12, 20, \text{ or } 24 \pmod{28} \Rightarrow$

$8p \equiv 24, 40, \text{ or } 48 \pmod{28}$

$p \equiv 3 \pmod 4 \Rightarrow 7p \equiv 21 \pmod{28}$

(1) $7p \equiv 21 \pmod{28}$
$8p \equiv 24 \pmod{28}$ $\Big\}$ $\underline{p \equiv 3} \pmod{28}$

(2) $7p \equiv 21 \pmod{28}$
$8p \equiv 40 \pmod{28}$ $\Big\}$ $\underline{p \equiv 19} \pmod{28}$

(3) $7p \equiv 21 \pmod{28}$
$8p \equiv 48 \pmod{28}$ $\Big\}$ $\underline{p \equiv 27} \pmod{28}$

$\therefore (7/p) = 1 \Rightarrow p \equiv 1, 3, 9, 19, 25,$ or $27 \pmod{28}$

(2) Suppose $p \equiv 1, 3, 9, 19, 25,$ or $27 \pmod{28}$

By def. of $(7/p)$, p is an odd prime.
Also, note $7 \equiv 3 \pmod 4$

(a) If $p \equiv 3, 19,$ or $27 \pmod{28}$, Then
$p \equiv 3, 19,$ or $27 \pmod 4$, so $p \equiv 3 \pmod 4$

$\therefore (7/p) = -(p/7)$ (corollary 1, p. 198)

Also, $p \equiv 3, 19,$ or $27 \pmod 7 \Rightarrow$
$p \equiv 3, 5, 6 \pmod 7$

$\therefore (p/7) = (3/7), (5/7),$ or $(6/7)$

$(3/7) = -(7/3) = -(1/3) = -1$

$(5/7) = (7/5) = (2/5) = -1$

$(6/7) = (3/7)(2/7) = (-1)(1) = -1$

$\therefore (p/7) = -1$

$\therefore (7/p) = -(p/7) = 1$

(b) If $p \equiv 1, 9,$ or $25 \pmod{28}$, Then
$p \equiv 1, 9,$ or $25 \pmod 4$, so $p \equiv 1 \pmod 4$

$\therefore (7/p) = (p/7)$ (corollary 1, p. 198)

Also, $p \equiv 1, 9, 25 \pmod 7$

$\therefore (p/7) = (1/7), (9/7), (25/7)$

$= 1, (2/7), (4, 7)$

$= 1, 1, 1$

$\therefore (7/p) = (p/7) = 1.$

$\therefore p \equiv 1, 3, 9, 19, 25, 27 \pmod{28} \Rightarrow (7/p) = 1$

11. Prove that there are infinitely many primes of the form $5K-1$.

Pf: Assume finitely many primes of form $5K-1$. Call them $p_1, p_2, \dots, p_r$, where $p_r > p_i$, $1 \le i < r$.

Consider the integer $M = 5(n!)^2 - 1$. For $n \ge 1$, M is odd, since $n!$ is even as it contains 2. $\therefore$ M has an odd prime divisor.
Note that any odd prime divisor p of M must be s.t. $p > n$; for if $p \le n$, then $p \mid n!$, so $p \mid M$ and $p \mid 5(n!)^2 \Rightarrow p \mid 1$, a contradiction.

$\therefore$ For $N = 5(p_r!)^2 - 1$, let p be any odd prime divisor. $\therefore$ $p > p_r$ and p cannot be of form $5K-1$.

$\therefore$ $5(p_r!)^2 \equiv 1 \pmod{p} \Leftrightarrow 25(p_r!)^2 \equiv 5 \pmod{p}$ [1]

since $p > p_r \ge 19 = 5K-1$ for $K=4$.
$\therefore$ $\gcd(5, p) = 1$.

$\therefore$ [1] $\Rightarrow (5/p) = 1$

But from prob. 10(a) above, $p \equiv 1, 9, 11,$ or $19 \pmod{20}$
$\Rightarrow p \equiv 1, 9, 11, 19 \pmod 5 \Rightarrow$
$p \equiv 1$ or $4 \pmod 5$

if $p \equiv 4 \pmod 5$, Then $p \equiv -1 \pmod 5 \Rightarrow$
$p = 5K-1$, some K. This can't be
since $p > p_r$ and p_r is The largest
prime of form $5K-1$.

$\therefore p \equiv 1 \pmod 5$, or $p = 5K+1$

Since p is any odd prime divisor of N,
Then
$$N = (5K_1+1)^{n_1}(5K_2+1)^{n_2}\cdots(5K_s+1)^{n_s}$$

But $(5K_i+1)^{n_i}$ is of form $5K'+1$,
so N is of form $5K''+1$.

But This contradicts $N = 5(p_r!)^2 - 1$
of form $5K-1$.
(if $5K-1 = 5K''+1$, Then $5(K-K'') = 2 \Rightarrow 5 | 2$).

$\therefore$ Assumption of finite number of primes of form $5K-1$ is false.

12. Verify the following:

(a) The prime divisors $p \neq 3$ of the integer n^2-n+1 are of form $6k+1$.

Pf: First note n^2-n+1 is odd for all $n \geq 1$.
For if n is odd, n^2 is odd, so n^2-n is even, so n^2-n+1 is odd.
If n is even, n^2 is even, n^2-n is even, so n^2-n+1 is odd.

$\therefore$ prime divisors p of $n^2-n+1 \neq 2$.
With assumption $p \neq 3$, then $p > 3$.

If $p \mid n^2-n+1$, then $p \mid 4n^2-4n+4$.
$(2n-1)^2 = 4n^2-4n+1$
$\therefore p \mid [(2n-1)^2+3]$

$\therefore (2n-1)^2 \equiv -3 \pmod{p} \Rightarrow (-3/p) = 1$

$\therefore p \equiv 0,1,2,3,4,5 \pmod{6}$.
if $p \equiv 0,2,4 \pmod{6}$, then $p \equiv 0,2,4 \pmod{2}$
$\Rightarrow 2 \mid p$, which can't be since $p > 3$.
if $p \equiv 3 \pmod{6}$, then $p \equiv 3 \pmod{3} \Rightarrow$
$3 \mid p$, which can't be since $p > 3$.

$\therefore p \equiv 1$ or $5 \pmod 6$. By prob. 5(a) above, $p \equiv 1 \pmod 6$; for $p \equiv 5 \Rightarrow (-3/p) = -1$.

$\therefore p \equiv 1 \pmod 6 \Rightarrow p = 1 + 6k$, some k.

(b) The prime divisors $p \neq 5$ of the integer n^2+n-1 are of the form $10k+1$ or $10k+9$

Pf: If $p \mid n^2+n-1$, then $p \mid 4n^2+4n-4$.

$$(2n+1)^2 - 5 = 4n^2+4n-4.$$

$$\therefore p \mid n^2+n-1 \Rightarrow p \mid (2n+1)^2-5 \Rightarrow (2n+1)^2 \equiv 5 \pmod p.$$

If $p \neq 5$, then $\gcd(p,5)=1$, so $(5/p)$ is defined.

$\therefore$ If $p \neq 5$, $p \mid n^2+n-1 \Rightarrow (5/p) = 1$

By Prob. 10(a), $p \equiv 1, 9, 11, 19 \pmod{20}$

$\Rightarrow p \equiv 1, 9, 11, 19 \pmod{10}$

$\Rightarrow p \equiv 1$ or $9 \pmod{10}$

$\Rightarrow p = 1 + 10k$ or $p = 9 + 10k$, some k.

(c) The prime divisors p of the integer $2n(n+1)+1$ are of the form $p \equiv 1 \pmod 4$.

Pf: $2n(n+1)+1 = 2n^2 + 2n + 1$

If $p \mid 2n(n+1)+1$, then $p \mid 4n^2+4n+2 \Rightarrow$

$p \mid (2n+1)^2 + 1 \Rightarrow (2n+1)^2 \equiv -1 \pmod p$

$\therefore p \mid 2n(n+1)+1 \Rightarrow (-1/p) = 1$

$\Rightarrow p \equiv 1 \pmod 4$

by corollary on p. 187.

(d) The prime divisors p of the integer $3n(n+1)+1$ are of the form $p \equiv 1 \pmod 6$

Pf: $3n(n+1)+1 = 3n^2 + 3n + 1$

$\therefore p \mid 3n(n+1)+1 \Rightarrow p \mid 36n^2 + 36n + 12$

$\Rightarrow p \mid (6n+3)^2 + 3$

$\Rightarrow (6n+3)^2 \equiv -3 \pmod p$ [1]

Note that if n is even or odd, $n(n+1)$ is even. $\therefore$ $3n(n+1)+1$ is odd, so $p \neq 2$.
If $p=3$, then $p \mid 3n(n+1)+1 \Rightarrow p \mid 1$.
$\therefore$ $p \neq 3$.

$\therefore$ $p > 3$, so $\gcd(-3, p) = 1$, so

$$[1] \Rightarrow (-3/p) = 1.$$

By prob. 5(a), $p \equiv 1 \pmod 6$.

13. (a) Show that if p is a prime divisor of $839 = 38^2 - 5 \cdot 11^2$, then $(5/p) = 1$. Use this fact to conclude that 839 is a prime number.

Pf: (1) If $p \mid 38^2 - 5 \cdot 11^2$, then

$$38^2 - 5 \cdot 11^2 \equiv 0 \pmod p \Leftrightarrow 38^2 \equiv 5 \cdot 11^2 \pmod p$$

$\therefore$ 38 is a solution to $x^2 \equiv 5 \cdot 11^2 \pmod p$, and so $(5 \cdot 11^2/p) = 1 \Rightarrow (5/p)(11^2/p) = 1$
$\Rightarrow (5/p) = 1$.

(2) Since $29^2 = 841 > 839$ only need to consider primes < 29 (discussion p. 45).

By prob. 10 (a), $(5/p)=1 \Rightarrow$

$p \equiv 1, 9, 11, 19 \pmod{20} \Rightarrow$

$p \equiv 1, 9, 11, 19 \pmod{10} \Rightarrow$

$p \equiv 1, 9 \pmod{10} \Rightarrow p = 11$ or 19

If $19 \mid 38^2 - 5\cdot 11^2$, then $19 \mid 5\cdot 11^2$.
If $11 \mid 38^2 - 5\cdot 11^2$, then $11 \mid 38^2$.
Both of these are false, so there is no prime p s.t. $(5/p)=1$.

$\therefore (5/p) \neq 1$, assumption that 839 is divisible by a prime is false
$\Rightarrow$ 839 is prime.

(b) Prove that both $397 = 20^2 - 3$ and $283 = 29^2 - 3\cdot 6^2$ are primes.

(1) $397 = 20^2 - 3$

Assume there is a prime divisor p s.t. $p \mid 397$
Since $20^2 = 400$, only consider $p < 20$.
$\therefore 20^2 \equiv 3 \pmod{p} \Rightarrow (3/p) = 1$.
By Th. 9.10, $p \equiv \pm 1 \pmod{12}$
$\therefore p = 11$ or 13.
But $11 \nmid 397$ and $13 \nmid 397$, so there is

no p s.t. $p \mid 397 \Rightarrow 397$ is prime.

(2) $733 = 29^2 - 3 \cdot 6^2$

Assume there is a prime p s.t. $p \mid 733$.
$28^2 = 784$, so just consider $p < 28$.

$29^2 \equiv 3 \cdot 6^2 \pmod{p} \Rightarrow (3 \cdot 6^2 / p) = 1 \Rightarrow (3/p) = 1$
$\therefore$ By Th. 9.10, $p \equiv \pm 1 \pmod{12}$.
$\therefore$ $p = 11, 13$, or 23.
But $11 \nmid 737$, $13 \nmid 733$, and $23 \nmid 733$.
$\therefore$ no prime p s.t. $p \mid 733 \Rightarrow 733$ is prime.

14. Solve the quadratic congruence $x^2 \equiv 11 \pmod{35}$

Since $35 = 7 \cdot 5$, x is a solution $\Leftrightarrow$ x is a solution to: $x^2 \equiv 11 \pmod{5}$ and
$x^2 \equiv 11 \pmod{7}$

$\therefore$ $x^2 \equiv 11 \pmod{5} \Leftrightarrow x^2 \equiv 1 \pmod{5}$
$\Leftrightarrow x \equiv \pm 1 \pmod{5}$
$x^2 \equiv 11 \pmod{7} \Leftrightarrow x^2 \equiv 4 \pmod{7}$
$\Leftrightarrow x \equiv \pm 2 \pmod{7}$

$\therefore$ (a) $x \equiv 1 \pmod{5}$ and $x \equiv 2 \pmod{7}$

(b) $x \equiv 1 \pmod 5$ and $x \equiv -2 \pmod 7$

(c) $x \equiv -1 \pmod 5$ and $x \equiv 2 \pmod 7$

(d) $x \equiv -1 \pmod 5$ and $x \equiv -2 \pmod 7$

For all of These, $n = 5 \cdot 7$, $N_1 = 7$, $N_2 = 5$

$\therefore\ 7x_1 \equiv 1 \pmod 5$ $\qquad$ $5x_2 \equiv 1 \pmod 7$

$2x_1 \equiv 1,\ 6x_1 \equiv 3$ $\qquad$ $15x_2 \equiv 3$

$x_1 \equiv 3$ $\qquad$ $x_2 \equiv 3$

(a) $x \equiv 1 \pmod 5$ and $x \equiv 2 \pmod 7$

$$\therefore\ x = 1 \cdot 7 \cdot 3 + 2 \cdot 5 \cdot 3 = 51 \pmod{35}$$
$$\equiv \underline{16} \pmod{35}$$

(b) $x \equiv 1 \pmod 5$ and $x \equiv -2 \pmod 7$

$$\therefore\ x = 1 \cdot 7 \cdot 3 + (-2) \cdot 5 \cdot 3 = -9 \equiv \underline{26} \pmod{35}$$

(c) $x \equiv -1 \pmod 5$ and $x \equiv 2 \pmod 7$

$$\therefore\ x = (-1) \cdot 7 \cdot 3 + 2 \cdot 5 \cdot 3 = 9 \equiv \underline{9} \pmod{35}$$

(d) $x \equiv -1 \pmod 5$ and $x \equiv -2 \pmod 7$

$\therefore x = (-1)\cdot 7\cdot 3 + (-2)\cdot 5\cdot 3 = -51 \equiv \underline{19} \pmod{35}$

$\therefore$ $\underline{x \equiv 9, 16, 19, \text{ or } 26 \pmod{35}}$

15. Establish that 7 is a primitive root of any prime of the form $2^{4n}+1$.

Pf: For $n=0$, $2^{4n}+1 = 2$, $\phi(2) = 1$, $7^1 = 7$, and $7 \equiv 1 \pmod 2$, so you could say 7 (and every odd integer) is a primitive root of 2.

So assume $n > 0$. $\therefore$ $2^{4n}+1$ is odd

By prob. 7 of section 9.1 (p.184), every quadratic non-residue of prime $p = 2^k+1$ is a primitive root of p.

$2^{4n}+1$ is of form 2^k+1, so just need to show 7 is a quadratic nonresidue of prime $p = 2^{4n}+1$. i.e., $(7/p) = -1$.

Note that for $n = 3k$, $2^{4n}+1$ is not prime, for $2^{4n}+1 = 2^{12k}+1 = (2^{4k})^3+1$ which can be factored to $(2^{4k}+1)\left[(2^{4k})^2 - 2^{4k}+1\right]$

$\therefore 2^{4n}+1$ can only be prime if $n=3k+1$ or $n=3k+2$, for $k=0,1,2,\ldots$

Note: $2^{4n}+1 = 2^{2\cdot 2n}+1 = 4^{2n}+1 \equiv 1 \pmod 4$.

$\therefore (7/p) = (p/7)$, by corollary 2, p. 198.

$\therefore$ need to show $(p/7) = -1$ for $n = 3k+1$ or $n=3k+2$, $k=0,1,2\ldots$, assuming p prime

$n=3k+1$: Look at $(2^{4(3k+1)}+1) \pmod 7$, and note $8 \equiv 1 \pmod 7$

$$\begin{aligned} 2^{4(3k+1)}+1 &= 2^{3(3k+1)}\cdot 2^{(3k+1)}+1 \\ &= (8^{3k+1})(8^k\cdot 2)+1 \\ &\equiv (1)(1\cdot 2)+1 \equiv 3 \pmod 7 \end{aligned}$$

$$\therefore (2^{4(3k+1)}+1/7) = (3/7) = -(7/3) = -(1/3) = -1$$

$n=3k+2$: $$\begin{aligned} 2^{4(3k+2)}+1 &= 2^{3(3k+2)}\cdot 2^{3k+2}+1 \\ &= (8^{3k+2})(8^k\cdot 4)+1 \\ &\equiv (1)(1\cdot 4)+1 \equiv 5 \pmod 7 \end{aligned}$$

$$\therefore (2^{4(3k+2)}+1/7) = (5/7) = (7/5) = (2/5) = -1$$

$\therefore$ When $2^{4n}+1$ is prime, $(p/7)=-1$, so $(7/p)=-1$, so 7 is a quadratic nonresidue, and $\therefore$ by prob. 7, section 9.1, 7 is a primitive root of $2^{4n}+1$.

16. Let a and $b>1$ be relatively prime integers, with b odd. If $b = p_1 p_2 \cdots p_r$ is the decomposition of b into odd primes (not necessarily distinct), then the Jacobi symbol (a/b) is defined by

$$(a/b) = (a/p_1)(a/p_2)\cdots(a/p_r)$$

where (a/p_i) is the Legendre symbol.

Evaluate $(21/221)$, $(215/253)$, $(631/1099)$

(a) $(21/221)$ $\quad 221 = 13\cdot 17$

$$\begin{aligned} \therefore (21/221) &= (21/13)(21/17) \\ &= (3/13)(7/13)(3/17)(7/17) \\ &= (13/3)(13/7)(17/3)(17/7) \\ &= (1/3)(6/7)(2/3)(3/7) \end{aligned}$$

$= (1)(3/7)(2/7)(-1)(3/7)$

$= (-1)(3^2/7)(2/7) = (-1)(1)(1) = -1$

$\therefore (21/221) = -1$

(b) $(215/253)$ $253 = 11 \cdot 23$, $215 = 5 \cdot 43$

$\therefore (215/253) = (215/11)(215/23)$

$= (5/11)(43/11)(5/23)(43/23)$

$= (11/5)(10/11)(23/5)(20/23)$

$= (1/5)(2/11)(5/11)(3/5)(4/23)(5/23)$

$= (1)(-1)(1)(5/3)(1)(23/5)$

$= (-1)(2/3)(3/5)$

$= (-1)(-1)(5/3) = (2/3) = -1$

$\therefore (215/253) = -1$

(c) $(631/1099)$ $1099 = 7 \cdot 157$, 631 is prime

$\therefore (631/1099) = (631/7)(631/157)$

$= (1/7)(3/157)$

$= (1)(157/3) = (1/3) = 1$

$\therefore (631/1099) = 1$

17. Under the hypothesis of the previous problem, show that if a is a quadratic residue of b, then $(a/b) = 1$;

but the converse is false.

Pf: (a) Assume $x^2 \equiv a \pmod{b}$ has a solution.
Let $b = p_1 p_2 \cdots p_r$, and note $\gcd(a, b) = 1$

$\therefore x^2 \equiv a \pmod{p_1}$, $x^2 \equiv a \pmod{p_2}, \ldots, x^2 \equiv a \pmod{p_r}$

and note $\gcd(a, p_i) = 1$.

$\therefore (a/p_i) = 1$, $\therefore (a/b) = (a/p_1)(a/p_2) \cdots (a/p_r)$

$= (1)(1) \cdots (1) = 1$.

(b) Now assume $(a/b) = 1$ and let $b = p_1 p_2$
$\therefore (a/b) = (a/p_1)(a/p_2)$.

$\therefore$ it may be that $(a/p_1) = (a/p_2) = -1$

$\therefore$ There would not be a solution to
$x^2 \equiv a \pmod{b}$.

As a concrete example, $(2/3) = -1$ and
$(2/5) = -1$. $\therefore (2/15) = 1$, but
$x^2 \equiv 2 \pmod{15}$ can't have a solution.
If it did, then so would $x^2 \equiv 2 \pmod{3}$

18. Prove that the following properties of the Jacobi hold: If b and b' are positive odd integers and $\gcd(aa', bb') = 1$, then

(a) $a \equiv a' \pmod{b}$ implies that $(a/b) = (a'/b)$

Pf: Let $b = p_1 p_2 \cdots p_r$ be the decomposition of b into odd primes (not necessarily distinct). Then by def. of (a/b), where (a/p_i) is the Legendre symbol,

$$(a/b) = (a/p_1)(a/p_2) \cdots (a/p_r)$$

From $\gcd(aa', bb') = 1$, we get $\gcd(a, p_i) = 1$ and $\gcd(a', p_i) = 1$.

From $a \equiv a' \pmod{b}$, we get $a \equiv a' \pmod{p_i}$

$\therefore$ from Th. 9.2, $(a/p_i) = (a'/p_i)$.

$\therefore (a/p_1) \cdots (a/p_r) = (a'/p_1) \cdots (a'/p_r)$

$\therefore (a/b) = (a'/b)$

(b) $(aa'/b) = (a/b)(a'/b)$

As in (a) above, let $b = p_1 p_2 \cdots p_r$.

Note that $\gcd(aa', bb') = 1 \Rightarrow \gcd(a/b) = 1$ and $\gcd(a'/b) = 1$.

Using Th. 9.2,

$$(aa'/b) = (aa'/p_1)(aa'/p_2) \cdots (aa'/p_r)$$

$$= (a/p_1)(a'/p_1)(a/p_2)(a'/p_2) \cdots (a/p_r)(a'/p_r)$$

$$= (a/p_1)(a/p_2) \cdots (a/p_r) \cdot (a'/p_1)(a'/p_2) \cdots (a'/p_r)$$

$$= (a/b)(a'/b)$$

(c) $(a/bb') = (a/b)(a/b')$

First note $\gcd(aa', bb') = 1 \Rightarrow \gcd(a/b) = 1$ and $\gcd(a/b') = 1$.

As in (a), let $b = p_1 p_2 \cdots p_r$ and let $b' = p_1' p_2' \cdots p_r'$. $\therefore bb' = p_1 p_2 \cdots p_r p_1' p_2' \cdots p_r'$

$$\therefore (a/bb') = (a/p_1)(a/p_2) \cdots (a/p_r)(a/p_1')(a/p_2') \cdots (a/p_r')$$

$$= (a/b)(a/b')$$

(d) $(a^2/b) = (a/b^2) = 1$

From (b), letting $a' = a$,

$$(a^2/b) = (a \cdot a/b) = (a/b)(a/b)$$
$$= (a/p_1) \cdots (a/p_r)(a/p_1) \cdots (a/p_r)$$
$$= (a/p_1)^2 \cdots (a/p_r)^2 = 1 \cdots 1 = 1$$

Similarly, letting $b = b'$ in (c),

$$(a/b^2) = (a/b)(a/b) = 1 \text{ as above.}$$

(e) $(1/b) = 1$

This follows from (d) letting $a = 1$ so that $1 = (a^2/b) = (1^2/b) = (1/b)$

(f) $(-1/b) = (-1)^{(b-1)/2}$

If $b = p_1 p_2 \cdots p_r$, Then by def., and using Th. 9.2,

$$(-1/b) = (-1/p_1)(-1/p_2) \cdots (-1/p_r)$$

$$= (-1)^{(p_1-1)/2}(-1)^{(p_2-1)/2} \cdots (-1)^{(p_r-1)/2} \qquad [1]$$

Now use the hint: if u and v are odd integers, Then $u = 2r+1$, $v = 2s+1$, some r, s.

$\therefore \frac{u-1}{2} = r, \quad \frac{v-1}{2} = s.$

$$\frac{uv-1}{2} = \frac{(2r+1)(2s+1)-1}{2} = \frac{4rs+2r+2s}{2}$$

$$= 2rs + r + s$$

$\therefore r+s \equiv r+s \pmod 2 \Rightarrow$

$r+s \equiv 2rs + r + s \pmod 2 \Rightarrow$

$$\frac{u-1}{2} + \frac{v-1}{2} \equiv \frac{uv-1}{2} \pmod 2$$

$\therefore \left[\frac{u-1}{2} + \frac{v-1}{2}\right]$ and $\left[\frac{uv-1}{2}\right]$ must both be odd, or both must be even.

$$\therefore (-1)^{\left[\frac{u-1}{2} + \frac{v-1}{2}\right]} = (-1)^{\left[\frac{uv-1}{2}\right]}$$

$\therefore [1]$ becomes $(-1)^{\left[\frac{p_1-1}{2}\right]}(-1)^{\left[\frac{p_2-1}{2}\right]} \cdots (-1)^{\left[\frac{p_r-1}{2}\right]}$

$$= (-1)^{\left[\frac{p_1p_2-1}{2}\right]} \cdots (-1)^{\left[\frac{p_r-1}{2}\right]}$$

$$= (-1)^{\left[\frac{p_1p_2\cdots p_r-1}{2}\right]} = (-1)^{\frac{b-1}{2}}$$

$\therefore (-1/b) = (-1)^{(b-1)/2}$

(g) $(2/b) = (-1)^{(b^2-1)/8}$

Let $b = p_1 \cdots p_r$

By def., $(2/b) = (2/p_1) \cdots (2/p_r)$

Using corollary to Th. 9.6, p. 191, $(2/p_i) = (-1)^{(p_i^2-1)8}$

$\therefore (2/b) = (-1)^{(p_1^2-1)/8} (-1)^{(p_2^2-1)/8} \cdots (-1)^{(p_r^2-1)/8}$

Now use the hint: if u, v are odd integers,
Then $u = 4r+1$ or $u = 4r+3$, some r
$v = 4s+1$ or $v = 4s+3$, some s

(1) $u = 4r+1$, $v = 4s+1$

$\therefore u^2-1 = 16r^2+8r$, $v^2-1 = 16s^2-8r$

$\therefore \frac{u^2-1}{8} + \frac{v^2-1}{8} = 2r^2+r+2s^2+s$

$\therefore \frac{u^2-1}{8} + \frac{v^2-1}{8} \equiv r+s \pmod 2$ [1]

$uv = 16rs + 4r + 4s + 1$

$$(uv)^2 = 16^2 r^2 s^2 + 64 r^2 s + 64 rs^2 + 16 rs$$
$$+ 64 r^2 s + 16 r^2 + 16 rs + 4r$$
$$+ 64 rs^2 + 16 rs + 16 s^2 + 4s$$
$$+ 16 rs + 4r + 4s + 1$$

$$\therefore (uv)^2 - 1 = 16^2 r^2 s^2 + 128 r^2 s + 128 rs^2 + 64 rs$$
$$+ 16 r^2 + 16 s^2 + 8r + 8s$$

$$\therefore \frac{(uv)^2-1}{8} \equiv r + s \pmod 2 \quad [2]$$

$$\therefore [1], [2] \Rightarrow \frac{u^2-1}{8} + \frac{v^2-1}{8} \equiv \frac{(uv)^2-1}{8} \pmod 2$$

(2) $u = 4r+1, \ v = 4s+3$

$$u^2 - 1 = 16r^2 + 8r, \ v^2 - 1 = 16s^2 + 24s + 8$$

$$\therefore \frac{u^2-1}{8} + \frac{v^2-1}{8} = 2r^2 + r + 2s^2 + 3s + 1$$

$$\therefore \frac{u^2-1}{8} + \frac{v^2-1}{8} \equiv r + s + 1 \pmod 2 \quad [1]$$

$$uv = 16rs + 12r + 4s + 3$$
$$(uv)^2 = 16^2 r^2 s^2 + (16)(12) r^2 s + 64 rs^2 + 48 rs$$
$$+ (12)(16) r^2 s + 144 r^2 + 48 rs + 36 r$$
$$+ 64 rs^2 + 48 rs + 16 s^2 + 12 s$$
$$+ 48 rs + 36 r + 12 s + 9$$

$$\therefore (uv)^2 - 1 = 16r^2s^2 + (24)(16)r^2s + 128rs^2 + (4)(48)rs + 144r^2 + 16s^2 + 72r + 24s + 8$$

$$\therefore \frac{(uv)^2-1}{8} \equiv 9r + 3s + 1 \equiv r + s + 1 \pmod 2 \; [2]$$

$$\therefore [1], [2] \Rightarrow \frac{u^2-1}{8} + \frac{v^2-1}{8} \equiv \frac{(uv)^2-1}{8} \pmod 2$$

(3) $u = 4r + 3$, $v = 4s + 1$

same as #(2) above, by symmetry.

(4) $u = 4r + 3$, $v = 4s + 3$

$$u^2 - 1 = 16r^2 + 24r + 8, \quad v^2 - 1 = 16s^2 + 24s + 8$$

$$\therefore \frac{u^2-1}{8} + \frac{v^2-1}{8} = 2r^2 + 3r + 1 + 2s^2 + 3s + 1$$

$$\therefore \frac{u^2-1}{8} + \frac{v^2-1}{8} \equiv 3r + 3s \equiv r + s \pmod 2 \quad [1]$$

$$uv = 16rs + 12r + 12s + 9$$

$$(uv)^2 - 1 = 16^2r^2s^2 + (16)(12)r^2s + (16)(12)rs^2 + 144rs + (12)(16)r^2s + 144r^2 + 144rs + (9)(12)r + (12)(16)rs^2 + 144rs + 144s^2 + (9)(12)s + 144rs + (9)(12)r + (9)(12)s + 80$$

$$= 16^2 r^2 s^2 + (24)(16) r^2 s + (24)(16) r s^2 +$$
$$(4)(144) rs + 144 r^2 + 144 s^2 +$$
$$(9)(24) r + (9)(24) s + 80$$

$$\therefore \frac{(uv)^2 - 1}{8} \equiv 27r + 27s \equiv r + s \pmod{2} \quad [2]$$

$$\therefore [1], [2] \Rightarrow \frac{u^2-1}{8} + \frac{v^2-1}{8} \equiv \frac{(uv)^2-1}{8} \pmod{2}$$

$$=$$

$$\therefore (1), (2), (3), (4) \Rightarrow \frac{u^2-1}{8} + \frac{v^2-1}{8} \equiv \frac{(uv)^2-1}{8} \pmod{2}$$

$$\therefore (2/b) = (-1)^{(p_1^2-1)/8} (-1)^{(p_2^2-1)/8} \cdots (-1)^{(p_r^2-1)/8}$$
$$= (-1)^{[(p_1 p_2)^2 - 1]/8} \cdots (-1)^{(p_r^2-1)/8}$$
$$= (-1)^{[(p_1 p_2 \cdots p_r)^2 - 1]/8}$$
$$= (-1)^{[b^2-1]/8}$$

19. Derive the Generalized Quadratic Reciprocity Law: If a and b are relatively prime positive odd integers, each greater than 1, then

$$(a/b)(b/a) = (-1)^{\frac{a-1}{2} \cdot \frac{b-1}{2}}$$

Pf: Let $a = p_1 p_2 \cdots p_r$, $b = q_1 q_2 \cdots q_s$ be the prime decompositions of a and b, where, since a and b are odd, p_i and q_j are odd primes, not necessarily distinct.

Since $\gcd(a,b)=1$, then $p_i \neq q_j$ for any i,j.

By def. of (a/b), and using Th. 9.2(d),

$$(a/b) = (a/q_1)(a/q_2)\cdots(a/q_s)$$

$$= (p_1\cdots p_r/q_1)(p_1\cdots p_r/q_2)\cdots(p_1\cdots p_r/q_s)$$

$$= (p_1/q_1)\cdots(p_r/q_1)\cdot$$
$$(p_1/q_2)\cdots(p_r/q_2)\cdot$$
$$\vdots$$
$$(p_1/q_s)\cdots(p_r/q_s)$$

$$= (p_1/q_1)(p_1/q_2)\cdots(p_1/q_s)\cdot$$
$$(p_2/q_1)(p_2/q_2)\cdots(p_2/q_s)\cdot$$
$$\vdots$$
$$(p_r/q_1)(p_r/q_2)\cdots(p_r/q_s)$$

[rearranging rows & cols to get r rows, s cols]

Similarly,

$$(b/a) = (q_1/p_1)\cdots(q_s/p_1)\cdot$$ [r rows, s cols]

$$(q_1/p_2)\cdots(q_s/p_2)\cdot$$
$$\vdots$$
$$(q_1/p_r)\cdots(q_s/p_r)$$

$\therefore (a/b)(b/a) =$ [aligning (a/b) rows with (b/a) rows]

$$(p_1/q_1)(p_1/q_2)\cdots(p_1/q_s)\cdot(q_1/p_1)\cdots(q_s/p_1)\cdot$$
$$(p_2/q_1)(p_2/q_2)\cdots(p_2/q_s)\cdot(q_1/p_2)\cdots(q_s/p_2)\cdot$$
$$\vdots$$
$$(p_r/q_1)(p_r/q_2)\cdots(p_r/q_s)\cdot(q_1/p_r)\cdots(q_s/p_r)$$

$$= (p_1/q_1)(q_1/p_1)\cdots(p_1/q_s)(q_s/p_1)\cdot$$
$$(p_2/q_1)(q_1/p_2)\cdots(p_2/q_s)(q_s/p_2)\cdot$$
$$\vdots$$
$$(p_r/q_1)(q_1/p_r)\cdots(p_r/q_s)(q_s/p_r)$$

Now using quadratic reciprocity on (p_i/q_j)

$$= (-1)^{\frac{p_1-1}{2}\cdot\frac{q_1-1}{2}} \cdots (-1)^{\frac{p_1-1}{2}\cdot\frac{q_s-1}{2}} \cdot$$

$$(-1)^{\frac{p_2-1}{2}\cdot\frac{q_1-1}{2}} \cdots (-1)^{\frac{p_2-1}{2}\cdot\frac{q_s-1}{2}}$$

$$\vdots$$

$$(-1)^{\frac{p_r-1}{2}\cdot\frac{q_1-1}{2}} \cdots (-1)^{\frac{p_r-1}{2}\cdot\frac{q_s-1}{2}}$$

$$= (-1)^{\left(\frac{p_1-1}{2}\right)\left[\frac{q_1-1}{2}+\cdots+\frac{q_s-1}{2}\right]} \cdot$$

$$(-1)^{\left(\frac{p_2-1}{2}\right)\left[\frac{q_1-1}{2}+\cdots+\frac{q_s-1}{2}\right]} \cdot$$

$$\vdots$$

$$(-1)^{\left(\frac{p_r-1}{2}\right)\left[\frac{q_1-1}{2}+\cdots+\frac{q_s-1}{2}\right]} \qquad [1]$$

By prob. 18(f) above, when u, v are odd integers,

$$(-1)^{\frac{u-1}{2}+\frac{v-1}{2}} = (-1)^{\frac{uv-1}{2}}$$

$\therefore$ [1] becomes,

$$(a/b)(b/a) = (-1)^{\left(\frac{p_1-1}{2}\right)\left(\frac{q_1\cdots q_s-1}{2}\right)} \cdot$$

$$(-1)^{\left(\frac{p_2-1}{2}\right)\left(\frac{q_1\cdots q_s-1}{2}\right)} \cdot$$

$$\vdots$$

$$(-1)^{\left(\frac{p_r-1}{2}\right)\left(\frac{q_1\cdots q_s-1}{2}\right)}$$

$$= (-1)^{\left(\frac{p_1-1}{2}\right)\left(\frac{b-1}{2}\right)} \cdot$$

$$(-1)^{\left(\frac{p_2-1}{2}\right)\left(\frac{b-1}{2}\right)} \cdot$$

$$\vdots$$

$$(-1)^{\left(\frac{p_r-1}{2}\right)\left(\frac{b-1}{2}\right)}$$

$$= (-1)^{\left[\frac{p_1-1}{2} + \frac{p_2-1}{2} + \cdots + \frac{p_r-1}{2}\right]\left(\frac{b-1}{2}\right)}$$

$$= (-1)^{\left[\frac{p_1 p_2 \cdots p_r - 1}{2}\right]\left(\frac{b-1}{2}\right)}$$

$$= (-1)^{\left[\frac{a-1}{2}\right]\left(\frac{b-1}{2}\right)}$$

$$\therefore (a/b)(b/a) = (-1)^{\left(\frac{a-1}{2}\right)\left(\frac{b-1}{2}\right)}$$

20. Using the Generalized Quadratic Reciprocity Law, determine whether the congruence, $x^2 \equiv 231 \pmod{1105}$ is solvable.

First, note $231 = 3 \cdot 7 \cdot 11$, $1105 = 5 \cdot 13 \cdot 17$.
$\therefore \gcd(231, 1105) = 1$.

By prob. 17 above, if 231 is a quadratic residue of 1105 (i.e., $x^2 \equiv 231 \pmod{1105}$ has a solution), then $(231/1105) = 1$. Can't use converse, but if can show $(231/1105) = -1$, Then can state $x^2 \equiv 231 \pmod{1105}$ is <u>not</u> solvable.

$$\therefore (231/1105)(1105/231) = (-1)^{\frac{231-1}{2} \cdot \frac{1105-1}{2}}$$

$$= (-1)^{(115)(552)} = 1$$

$$\therefore (231/1105)(1105/231)(1105/231) = (1105/231)$$

Using prob. 18(d),

$$(231/1105) = (1105/231)$$

$$= (181 + 4 \cdot 231/231) \quad [181 \text{ is prime}]$$

$$= (181/231) \quad [\text{prob. } 18(a)]$$

$$= (181/3)(181/7)(181/11)$$

$$= (1/3)(6/7)(5/11)$$

$$= (2/7)(3/7)(11/5)$$

$$= (1)(-1)(1) = -1$$

$\therefore (231/1105) = -1$, so

$x^2 \equiv 231 \pmod{1105}$ is <u>not</u> solvable.