9.1 Euler's Criterion

Note Title 5/10/2006

1. Solve the following quadratic congruences.

(a) $x^2 + 7x + 10 \equiv 0 \pmod{11}$

Let $y = 2ax + b = 2x + 7$, $d = b^2 - 4ac = 9$

$\therefore y^2 \equiv 9 \pmod{11}$, $\therefore y \equiv 3, 8 \; (= 11 - 3)$

$\therefore 2x + 7 \equiv 3 \pmod{11}$ $\qquad$ $2x + 7 \equiv 8 \pmod{11}$

$2x \equiv -4$ $\qquad$ $2x \equiv 1$, $10x \equiv 5$

$x \equiv -2 \equiv 9$ $\qquad$ $-x \equiv 5$, $x \equiv -5 \equiv 6$

$\therefore \underline{x \equiv 6, 9} \pmod{11}$

(b) $3x^2 + 9x + 7 \equiv 0 \pmod{13}$

$y = 2ax + b = 6x + 9$, $d = b^2 - 4ac = -3$

$\therefore y^2 \equiv -3 \equiv 10 \equiv 10 + 2 \cdot 13 = 36 \pmod{13}$

$\therefore y \equiv 6, 7 \; (= 13 - 6)$

$\therefore 6x + 9 \equiv 6 \pmod{13}$ $\qquad$ $6x + 9 \equiv 7 \pmod{13}$

$6x \equiv -3 \equiv 36$ $\qquad$ $6x \equiv -2$, $12x \equiv -4$

$x \equiv 6$ $\qquad$ $-x \equiv -4$, $x \equiv 4$

$\therefore \underline{x \equiv 4, 6} \pmod{13}$

(c) $5x^2+6x+1 \equiv 0 \pmod{23}$

$y = 2ax+b = 10x+6$, $d = b^2-4ac = 16$

$\therefore y^2 \equiv 16 \pmod{23}$, $y \equiv 4, 19\ (=23-4)$

$\therefore 10x+6 \equiv 4 \pmod{23}$ $\qquad$ $10x+6 \equiv 19 \pmod{23}$

$10x \equiv -2$, $20x \equiv -4$ $\qquad$ $10x \equiv 13$, $20x \equiv 26$

$-3x \equiv -4$, $-24x \equiv -32$ $\qquad$ $-3x \equiv 3$, $x \equiv -1$

$-x \equiv -32$, $x \equiv 9$ $\qquad$ $x \equiv 22$

$\therefore \underline{x \equiv 9, 22} \pmod{23}$

2. Prove that the quadratic congruence, $6x^2+5x+1 \equiv 0 \pmod{p}$ has a solution for every prime p, even though $6x^2+5x+1=0$ has no solution in integers.

Pf: $6x^2+5x+1=0$, $\dfrac{-5 \pm \sqrt{25-24}}{12} = \dfrac{-5 \pm 1}{12}$

$\therefore x = -\frac{1}{2}, -\frac{1}{3}$

$6x^2+5x+1 = (3x+1)(2x+1) \equiv 0 \pmod{p}$

$\therefore 3x+1 \equiv 0 \pmod{p}$ or $(2x+1) \equiv 0 \pmod{p}$

(1) If p is odd, then choose x s.t. $2x+1 = p$

$\therefore\ 2x+1 \equiv 0 \pmod p \Rightarrow 6x^2+5x+1 \equiv 0 \pmod p$

(2) If $p=2$, Then $3x+1 \equiv 0 \pmod 2$

$3x \equiv -1 \equiv 1,\ x \equiv 1$

$\therefore\ x \equiv 1 \pmod 2 \Rightarrow 3x \equiv 3,\ 3x+1 \equiv 4 \equiv 0 \pmod 2$

$\Rightarrow 6x^2+5x+1 \equiv 0 \pmod 2$

$\therefore$ There is a solution to $6x^2+5x+1 \equiv 0 \pmod p$ for all prime p.

3. (a) For an odd prime p, prove that the quadratic residues of p are congruent mod p to The integers

$$1^2, 2^2, \ldots, \left(\frac{p-1}{2}\right)^2$$

Pf: (1) For $a = 1^2, 2^2, \ldots, \left(\frac{p-1}{2}\right)^2$,

$$a^{\frac{p-1}{2}} = 1^{p-1}, 2^{p-1}, \ldots, \left(\frac{p-1}{2}\right)^{p-1}$$

But for $b = 1, 2, \ldots, \frac{p-1}{2}$, $\gcd(b,p)=1$ as $1 \le b < p-1$ and p is prime.

By Fermat's Th., $b^{p-1} \equiv 1 \pmod p$

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

$\therefore$ By Euler's Criterion, $1^2, 2^2, \ldots, \left(\frac{p-1}{2}\right)^2$ are quadratic residues of p.

(2) $1^2, 2^2, \ldots, \left(\frac{p-1}{2}\right)^2$ are incongruent mod p

For if $a^2 \equiv b^2 \pmod{p}$, $1 \le a, b \le \frac{p-1}{2}$, $a \ne b$,
Then $a^2 - b^2 \equiv 0 \iff (a-b)(a+b) \equiv 0 \pmod{p}$
But $a+b \le \frac{p-1}{2} + \frac{p-1}{2} = p-1$

$\therefore \gcd(a+b, p) = 1$, so can divide by $a+b$.
$\therefore a-b \equiv 0 \pmod{p} \Rightarrow a \equiv b \Rightarrow a = b$,
a contradiction.

(3) Let a be any quadratic residue of p.
$\therefore x^2 \equiv a \pmod{p}$ has a solution.
Let it be x_0 s.t. $1 \le x_0 \le p-1$.
$\therefore p - x_0$ is also a solution.
One of x_0, $p - x_0$ must be $\le \frac{p-1}{2}$.

For if $x_0 > \frac{p-1}{2}$, Then $-x_0 < -\frac{p-1}{2}$,

$$\text{so } p - x_0 < p - \frac{p-1}{2} = \frac{p-1}{2}$$

$\therefore$ One of x_0^2 or $(p-x_0)^2$ is equal to $1^2, 2^2, \ldots, \left(\frac{p-1}{2}\right)^2$

Since $x_0^2 \equiv (p-x_0)^2 \equiv a$, Then a must be congruent to one of $1^2, 2^2, \ldots, \left(\frac{p-1}{2}\right)^2$

(b) Verify that the quadratic residues of 17 are 1, 2, 4, 8, 9, 13, 15, 16.

By (a),

$$\begin{array}{ll} 1^2 \equiv 1 & 5^2 \equiv 25 \equiv 8 \\ 2^2 \equiv 4 & 6^2 \equiv 36 \equiv 2 \\ 3^2 \equiv 9 & 7^2 \equiv 49 \equiv 15 \\ 4^2 \equiv 16 & 8^2 \equiv 64 \equiv 13 \end{array}$$

4. Show that 3 is a quadradic residue of 23, but a nonresidue of 31.

$$3^{\frac{23-1}{2}} = 3^{11} = 3^2(3^3)^3 = 9\,(27)^3 \equiv 9 \cdot (4)^3 \pmod{23}$$
$$\equiv 9 \cdot 64 \equiv 9\,(-5) \equiv -45+46 \equiv 1.$$

$\therefore\ \underline{3^{\frac{23-1}{2}} \equiv 1 \pmod{23}} \Rightarrow 3$ a quadradic reside of 23

$$3^{\frac{31-1}{2}} = 3^{15} = (3^3)^5 = 27^5 \equiv (-4)^5 \pmod{31}$$
$$\equiv -4^3 \cdot 4^2 \equiv (-64)(16) \equiv (-64+62)(16) \equiv -32 \equiv -1$$

$\therefore\ \underline{3^{\frac{31-1}{2}} \equiv -1 \pmod{31}} \Rightarrow 3$ a quadratic nonresidue of 31.

5. Given that a is a quadratic residue of odd prime p, prove the following

(a) a is not a primitive root of p

Pf: If a were a primitive root of p, then $a^n \not\equiv 1 \pmod{p}$ for $1 \le n < p-1$, by def.

But by Euler's criterion, $a^{\frac{p-1}{2}} \equiv 1 \pmod{p}$. p is odd so $\frac{p-1}{2}$ is an integer, and $1 \le \frac{p-1}{2} < p-1$, which contradicts the above.

(b) The integer $p-a$ is a quadratic residue or nonresidue of p according as $p \equiv 1 \pmod{4}$ or $p \equiv 3 \pmod{4}$

Pf: Consider $x^2 \equiv p-a \pmod{p}$. This is equivalent to $x^2 \equiv -a \pmod{p}$.

$\therefore$ $-a$ (or $p-a$) is a quadratic residue or nonresidue according to whether $(-a)^{\frac{p-1}{2}} \equiv 1 \pmod{p}$ or $(-a)^{\frac{p-1}{2}} \equiv -1 \pmod{p}$, since a is a quadratic residue, then $a^{\frac{p-1}{2}} \equiv 1 \pmod{p}$.

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

$\therefore$ $p-a$ is a quadratic residue or nonresidue according to whether $(-1)^{\frac{p-1}{2}}$ is 1 or -1, and this according to whether $\frac{p-1}{2}$ is even or odd.

$$\frac{p-1}{2} \text{ is even} \iff \frac{p-1}{2} = 2k, \text{ some } k,$$
$$\iff p-1 = 4k$$
$$\iff p \equiv 1 \pmod 4)$$

$$\frac{p-1}{2} \text{ is odd} \iff \frac{p-1}{2} = 2k+1, \text{ some } k$$
$$\iff p-1 = 4k+2$$
$$\iff p = 3+4k$$
$$\iff p \equiv 3 \pmod 4)$$

$\therefore$ $p-a$ is a quadratic residue or nonresidue according to whether $p \equiv 1 \pmod 4$ or $p \equiv 3 \pmod 4$

(c) If $p \equiv 3 \pmod 4$, then $x \equiv \pm a^{\frac{p+1}{4}} \pmod p$ are the solutions of the congruence $x^2 \equiv a \pmod p$.

Pf: $x \equiv \pm a^{\frac{p+1}{4}} \implies x^2 \equiv a^{\frac{p+1}{2}} = a^{\frac{p-1+2}{2}} = a^{\frac{p-1}{2}} \cdot a$

Since a is a quadratic residue, $a^{\frac{p-1}{2}} \equiv 1$

$\therefore$ $a^{\frac{p-1}{2}} \cdot a \equiv a$.

$\therefore$ $x^2 \equiv a \pmod{p}$ when $x \equiv \pm a^{\frac{p+1}{4}}$

$\frac{p+1}{4}$ is an integer when $\frac{p+1}{4} = k$, some k,

$\therefore$ $p+1 = 4k$, $p = -1+4k$, $p \equiv -1 \pmod{4}$, or $p \equiv 3 \pmod{4}$.

Also, by Lagrange's Th. (Th. 8.5), There are at most 2 solution, so

$x \equiv \pm a^{\frac{p+1}{4}}$ are the exact solutions.

6. Let p be an odd prime and $\gcd(a,p)=1$. Establish that the quadratic congruence $ax^2+bx+c \equiv 0 \pmod{p}$ is solvable $\Longleftrightarrow$ b^2-4ac is zero or a quadratic residue of p.

Pf: Since $\gcd(a,p)=1$ and p is an odd prime, $\gcd(4a,p)=1$.

$\therefore$ Solutions to

$$4a(ax^2+bx+c) \equiv 0 \pmod{p} \qquad [1]$$

are equivalent to

$$ax^2 + bx + c \equiv 0 \pmod{p} \qquad [2]$$

since you can divide [1] by $4a$ to get [2]

But $4a(ax^2 + bx + c) = 4a^2x^2 + 4abx + 4ac$

$$= (2ax+b)^2 - b^2 + 4ac$$

$$= (2ax+b)^2 - (b^2 - 4ac)$$

$\therefore$ Solutions to

$$ax^2 + bx + c \equiv 0 \pmod{p} \qquad [2]$$

are equivalent to

$$(2ax+b)^2 \equiv b^2 - 4ac \pmod{p} \qquad [3]$$

(a) Suppose $b^2 - 4ac \equiv 0 \pmod{p}$

$\therefore$ Solutions to [2] are equivalent to

$(2ax+b)^2 \equiv 0 \pmod{p}$

which is equivalent to

$$2ax \equiv -b \pmod{p}$$

Since $\gcd(2a,p)=1$, this has a unique solution mod p (Th. 4.7).

$\therefore ax^2+bx+c \equiv 0 \pmod{p}$ is solvable $\Leftrightarrow$
$b^2-4ac \equiv 0 \pmod{p}$

(b) $b^2-4ac \not\equiv 0 \pmod{p}$ and is a quadratic residue of p.

$\therefore y^2 \equiv b^2-4ac \pmod{p}$ has a solution by definition.
Let y_1 be s.t. $y_1^2 \equiv b^2-4ac \pmod{p}$, $1 \le y_1 \le p-1$.
$\therefore p-y_1$ is also a solution.
By Lagrange Th., these are the only solutions. They are also incongruent.
For if $y_1 \equiv p-y_1 \pmod{p}$, then
$2y_1 \equiv p \equiv 0 \pmod{p} \Leftrightarrow y_1 \equiv 0 \pmod{p}$ as $\gcd(p,2)=1$. $\therefore b^2-4ac \equiv 0$, a contradiction

Letting $y_1 = 2ax+b$, then

$y^2 \equiv b^2-4ac \pmod{p}$ is equivalent to

$2ax+b \equiv b^2-4ac \pmod{p}$ and
$p-(2ax+b) \equiv b^2-4ac \pmod{p}$, or

$$2ax \equiv b^2 - 4ac - b \pmod{p} \quad [4]$$

and $$2ax \equiv 4ac - b^2 - b \pmod{p} \quad [5]$$

Since $\gcd(2a, p) = 1$, by Th. 4.7,
[4] and [5] have unique solutions.

$\therefore$ Assuming $b^2 - 4ac \not\equiv 0 \pmod{p}$,

$b^2 - 4ac$ a quadratic residue of p

$\Leftrightarrow (2ax + b)^2 \equiv b^2 - 4ac \pmod{p}$ is solvable,

$\Leftrightarrow ax^2 + bx + c \equiv 0 \pmod{p}$ is solvable.

7. If $p = 2^k + 1$ is prime, verify that every quadratic nonresidue of p is a primitive root of p.

Pf: Let a be a quadratic nonresidue of p.

$\therefore$ By Euler's criterion, $a^{\frac{p-1}{2}} \equiv -1 \pmod{p}$

Since $2^k + 1$ is prime, $k \geq 1$. $p - 1 = 2^k$,
$\therefore \frac{p-1}{2} = 2^{k-1}$

$$\therefore a^{2^{k-1}} \equiv -1 \pmod{p}. \quad [1]$$

$\therefore \left(a^{2^{k-1}}\right)^2 = a^{2^k} \equiv 1 \pmod{p}$, and

$\phi(p) = p-1 = 2^k$.

Let n be order of a mod p. $\therefore n \mid 2^k$ by Th. 8.1.

$\therefore$ if $n \neq 2^k$, then $n = 2^r$, $r < k$

$\therefore a^{2^r} \equiv 1 \pmod{p}$ [2]

If $r = k-1$, then a contradiction is reached by [1].

If $r < k-1$, then square [2] $k-1-r$ times.

$$\therefore \left(a^{2^r}\right)^2 = a^{2\cdot 2^r} = a^{2^{r+1}} \equiv 1 \pmod{p}$$

$$\left(a^{2^{r+1}}\right)^2 = a^{2\cdot 2^{r+1}} = a^{2^{r+2}} \equiv 1 \pmod{p}$$

$$\vdots$$

$$\left(a^{2^{k-2}}\right)^2 = a^{2\cdot 2^{k-2}} = a^{2^{k-1}} \equiv 1 \pmod{p}$$

$\therefore$ again, a contradiction is reached by [1]

$\therefore n = 2^k$, so order of a is $p-1 = \phi(p)$

8. Assume r is a primitive root of prime p, where $p \equiv 1 \pmod 8$.

(a) Show that the solutions of the quadratic congruence $x^2 \equiv 2 \pmod p$ are given by

$$x \equiv \pm\left(r^{7(p-1)/8} + r^{(p-1)/8}\right) \pmod p$$

Pf: Since r is a prim. root of p, $r^{p-1} \equiv 1 \pmod p$

But $p-1 = 8k$, some k, or $\frac{p-1}{8} = k$, an integer.

Let $x \equiv \pm\left(r^{7(p-1)/8} + r^{(p-1)/8}\right) \pmod p$

$$\therefore x^2 \equiv \left(r^{7(p-1)/8} + r^{(p-1)/8}\right)^2 \pmod p$$

$$= r^{14(p-1)/8} + r^{2(p-1)/8} + 2r^{p-1}$$

$$\equiv r^{14(p-1)/8} + r^{2(p-1)/8} + 2 \pmod p$$

$\therefore$ Need to show $r^{14(p-1)/8} + r^{2(p-1)/8} \equiv 0 \pmod p$ to show $x^2 \equiv 2 \pmod p$.

$$r^{14(p-1)/8} + r^{2(p-1)/8} = r^{2(p-1)/8}\left(r^{12(p-1)/8} + 1\right)$$

But $\gcd(r, p) = 1$, so $\gcd(r^{2(p-1)/8}, p) = 1$

$\therefore$ If can show $r^{12(p-1)/8} \equiv -1 \pmod{p}$,

Then $x^2 \equiv 2 \pmod{p}$.

$$r^{12(p-1)/8} = r^{8(p-1)/8} \cdot r^{4(p-1)/8}$$

$$= r^{p-1} \cdot r^{4(p-1)/8}$$

$$\equiv r^{4(p-1)/8} = r^{\frac{p-1}{2}}$$

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

Then $r^{\frac{p-1}{2}} \equiv -1$ or $r^{\frac{p-1}{2}} \equiv 1 \pmod{p}$, but not both, since otherwise $-1 \equiv 1 \pmod{p}$, so $p \equiv 2$, a contradiction to $p \equiv 1 \pmod{8}$.

But $r^{\frac{p-1}{2}} \not\equiv 1$ since r is a primitive root (order of $r = p-1$).

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

$\therefore$ $r^{12(p-1)/8} \equiv -1 \pmod{p}$

$\therefore$ if $x \equiv \pm(r^{7(p-1)/8} + r^{(p-1)/8}) \pmod{p}$, Then $x^2 \equiv 2 \pmod{p}$, and Lagrange's Th. shows there are no more solutions.

(b) Use part (a) to find all solutions to the two congruences $x^2 \equiv 2 \pmod{17}$ and $x^2 \equiv 2 \pmod{41}$

(1) $x^2 \equiv 2 \pmod{17}$

3 is a primitive root of 17

$$\therefore x \equiv \pm\left(3^{7(17-1)/8} + 3^{(17-1)/8}\right) \pmod{17}$$

$$= \pm(3^{14} + 3^2) \pmod{17}$$

$$= \pm 3^2(3^{12}+1) = \pm 9(3^{12}+1)$$

$3^2 = 9$, $3^4 \equiv -4$, $3^8 \equiv 16 \equiv -1$, $3^{12} \equiv 4$

$$\therefore x \equiv \pm 9(4+1) = \pm 45 \equiv \underline{6, 11} \pmod{17}$$

(2) $x^2 \equiv 2 \pmod{41}$

6 is a prim. root of 41 (table p. 166)

$\therefore x \equiv \pm \left(6^{7(41-1)/8} + 6^{(41-1)/8}\right) \pmod{41}$

$= \pm\left(6^{35} + 6^{5}\right) = \pm 6^5\left(6^{30}+1\right)$

$6^2 = 36 \equiv -5,\ 6^3 = -30 \equiv 11,\ 6^4 \equiv 66 \equiv 25 \equiv -16$

$6^5 \equiv -96 \equiv -14,\ 6^6 \equiv -84 \equiv -2$

$\therefore 6^{30} \equiv (-2)^5 \equiv -32 \equiv 9$

$\therefore x \equiv \pm 14(9+1) = \pm 140 \equiv \pm 17 = 17, 24$

$\therefore x \equiv 17, 24 \pmod{41}$

9. (a) If $ab \equiv r \pmod{p}$, where r is a quadratic residue of the odd prime p, prove that a and b are both quadratic residues of p or both nonresidues of p.

Pf: Since $\gcd(r,p)=1$, then $\gcd(ab,p)=1$,
$\therefore \gcd(a,p)=1$ and $\gcd(b,p)=1$.

Suppose a is a quadratic residue and b a nonresidue.

$\therefore a^{\frac{p-1}{2}} \equiv 1,\ b^{\frac{p-1}{2}} \equiv -1 \pmod{p}$

$\therefore r^{\frac{p-1}{2}} \equiv a^{\frac{p-1}{2}} \cdot b^{\frac{p-1}{2}} \equiv -1 \pmod{p}$,

which makes r a nonresidue by corollary to Euler's criterion.

$\therefore a^{\frac{p-1}{2}} \equiv b^{\frac{p-1}{2}} \equiv 1$ or $a^{\frac{p-1}{2}} \equiv b^{\frac{p-1}{2}} \equiv -1 \pmod{p}$

(b) If a and b are both quadratic residues of the odd prime p or both nonresidues of p, show that the congruence $ax^2 \equiv b \pmod{p}$ has a solution.

Pf: Assume $\gcd(a,p) = \gcd(b,p) = 1$.

$\therefore ax^2 \equiv b \pmod{p}$

is equivalent to,

$a^2x^2 \equiv ab \pmod{p}$, or

$(ax)^2 \equiv ab \pmod{p}$.

$\therefore ax^2 \equiv b \pmod{p}$ has a solution $\Leftrightarrow$ ab is a quadratic residue.

By (a) ab is a quadratic residue $\Leftrightarrow$ a, b are both quadratic residues or both nonresidues.

$\therefore ax^2 \equiv b \pmod{p}$ has a solution $\Leftrightarrow$ a, b are both quadratic residues or both nonresidues.

10. Let p be an odd prime and $\gcd(a,p) = \gcd(b,p) = 1$. Prove that either all three of the quadratic congruences $x^2 \equiv a \pmod{p}$, $x^2 \equiv b \pmod{p}$, $x^2 \equiv ab \pmod{p}$ are solvable or exactly one of them admits a solution.

Pf: Suppose more than one congruence admits a solution.

(1) Assume $x^2 \equiv a \pmod{p}$, $x^2 \equiv b \pmod{p}$ are solvable.
By Euler's criterion, $a^{\frac{p-1}{2}} \equiv b^{\frac{p-1}{2}} \equiv 1 \pmod{p}$

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

and so $x^2 \equiv ab \pmod{p}$ is solvable.

(2) Assume $x^2 \equiv a \pmod{p}$, $x^2 \equiv ab \pmod{p}$ are solvable (case of $x^2 \equiv b$ and $x^2 \equiv ab$ is analagous).

$\therefore$ By Euler's criterion, $a^{\frac{p-1}{2}} \equiv 1 \pmod{p}$

and $(ab)^{\frac{p-1}{2}} = a^{\frac{p-1}{2}} \cdot b^{\frac{p-1}{2}} \equiv 1 \pmod{p}$ [1]

Since $\gcd(a,p)=1$, Then $\gcd(a^{\frac{p-1}{2}}, p) = 1$

$\therefore$ Dividing by [1] by $a^{\frac{p-1}{2}}$, we get

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

$\therefore$ By Euler's criterion, $x^2 \equiv b \pmod{p}$ is sollvable.

11. (a) Knowing 2 is a primitive root of 19, find all The quadratic residues of 19.

Proof to Th. 9.1 shows That if a is a quadratic residue, Then if r is a prim. root of 19, Then $r^k \equiv a \pmod{p}$, $1 \le k \le p-1$, and k is even.

$\therefore$ Look at all 2^k for k even and $1 \le k \le 18$

$\therefore 2^2 \equiv 4$ $2^8 \equiv 4 \cdot 7 \equiv 9$ $2^{14} \equiv -32 \equiv 6$

$2^4 \equiv 16$ $2^{10} \equiv 4 \cdot 9 \equiv -2 \equiv 17$ $2^{16} \equiv 24 \equiv 5$

$2^6 = 64 \equiv 7$ $2^{12} \equiv -8 \equiv 11$ $2^{18} \equiv 20 \equiv 1$

$\therefore$ 1, 4, 5, 6, 7, 9, 11, 16, 17

(b) Find the quadratic residues of 29 and 31

Can use method in (a), or easier, method in Example 9.1

29: $1^2 \equiv 28^2 \equiv 1$
$2^2 \equiv 27^2 \equiv 4$
$3^2 \equiv 26^2 \equiv 9$
$4^2 \equiv 25^2 \equiv 16$
$5^2 \equiv 24^2 \equiv 25$
$6^2 \equiv 23^2 \equiv 7$
$7^2 \equiv 22^2 \equiv 20$
$8^2 \equiv 21^2 \equiv 64 \equiv 6$
$9^2 \equiv 20^2 \equiv 81 \equiv 23$
$10^2 \equiv 19^2 \equiv 13$
$11^2 \equiv 18^2 \equiv 121 \equiv 5$
$12^2 \equiv 17^2 \equiv 144 \equiv -1 \equiv 28$
$13^2 \equiv 16^2 \equiv 169 \equiv 24$
$14^2 \equiv 15^2 \equiv 196 \equiv 51 \equiv -7 \equiv 22$

$\therefore$ 1, 4, 5, 6, 7, 9, 13, 16, 20, 22, 23, 24, 25, 28

31: $1^2 \equiv 30^2 \equiv 1$
$2^2 \equiv 29^2 \equiv 4$
$3^2 \equiv 28^2 \equiv 9$
$4^2 \equiv 27^2 \equiv 16$
$5^2 \equiv 26^2 \equiv 25$
$6^2 \equiv 25^2 \equiv 5$
$7^2 \equiv 24^2 \equiv 18$
$8^2 \equiv 23^2 \equiv 2$
$9^2 \equiv 22^2 \equiv 81 \equiv 19$
$10^2 \equiv 21^2 \equiv 7$
$11^2 \equiv 20^2 \equiv -3 \equiv 28$
$12^2 \equiv 19^2 \equiv 20$
$13^2 \equiv 18^2 \equiv 169 \equiv 45 \equiv 14$
$14^2 \equiv 17^2 \equiv 196 \equiv 10$
$15^2 \equiv 16^2 \equiv 225 \equiv 8$

$\therefore 1, 2, 4, 5, 7, 8, 9, 10, 14, 16, 18, 19, 20, 25, 28$

12. If $n > 2$ and $\gcd(a, n) = 1$, then a is called a quadratic residue of n whenever there exists an integer x s.t. $x^2 \equiv a \pmod{n}$. Prove that if a is a quadratic residue of $n > 2$, then $a^{\phi(n)/2} \equiv 1 \pmod{n}$.

Pf: Since $\gcd(a, n) = 1$ and $x^2 \equiv a \pmod{n}$, then $\gcd(x^2, n) = 1$, and so $\gcd(x, n) = 1$ (if x and n had a common divisor, $d > 1$, then $d \mid x \Rightarrow d \mid x^2$).

By Euler's Th., $x^{\phi(n)} \equiv 1 \pmod{n}$

$$\therefore a^{\phi(n)/2} \equiv (x^2)^{\phi(n)/2} = x^{\phi(n)} \equiv 1 \pmod{n}$$

13. Show that the result of the previous problem does not provide a sufficient condition for the existence of a quadratic residue of n; i.e., find relatively prime integers a and n, with $a^{\phi(n)/2} \equiv 1 \pmod{n}$, for which the congruence $x^2 \equiv a \pmod{n}$ is not solvable.

Intuition suggests, from section 8.3, that

if n is composite and doesn't have a prim. root,
Then finding such an a will be easier.

$\therefore$ Let $n=6$ $\mod 6$, $1^2 \equiv 1$ $\quad 4^2 \equiv 4$

$2^2 \equiv 4$ $\quad 5^2 \equiv 1$

$3^2 \equiv 3$

$\therefore x^2 \equiv 5 \pmod 6$ is not solvable

$\phi(6) = 2$, however $5^1 \not\equiv 1 \pmod 6$

Try $n=8$ $\mod 8$, $1^2 \equiv 1$ $\quad 4^2 \equiv 0$ $\quad 7^2 \equiv 1$

$2^2 \equiv 4$ $\quad 5^2 \equiv 1$

$3^2 \equiv 1$ $\quad 6^2 \equiv 4$

$\therefore x^2 \equiv a \pmod 8$ not solvable if $a = 3, 5, 7$

$\phi(8) = 4$ $\therefore \phi(8)/2 = 2$

And, $3^2 \equiv 5^2 \equiv 7^2 \equiv 1 \pmod 8$.

$\therefore$ Let $\underline{n = 8}$, $\underline{a = 3, 5, \text{ or } 7}$.