$1_{\circ}\; x^2 + py + a = 0$

$x^2 + a = -py$ division algorithm

$x^2 \equiv -a \pmod{p}$ must be a quadratic residue mod p for there to exist solutions

$(-a/p) = 1$

6. $x^2 + 7y - 2 = 0$

$1 \overset{?}{=} (2/7)$ — 7 mod 8 = 7 therefore we can use theorem 9.6

$\boxed{1 \overset{\checkmark}{=} 1}$

because $(-a/p) = 1$ there exists an integer solution to the diophantine equation

2. 2 is not primitive root for any prime p of form $p = 3 \cdot 2^n + 1$ $n \in \mathbb{Z}^+$

~~For 2 to be primitive root $2^{p-1} \equiv 1 \pmod{p}$ is~~

consider when $2^{(p-1)/2} \equiv 1 \pmod{p} \Rightarrow (2/p) = 1$ in this case it would not be primitive root as $\frac{p-1}{2} < p-1$

case for $n \leq 2$ & p=7 can be proven as follows + p=13

7 mod 8 = 7 ∴ theorem 9.6 tells us that $(2/7) = 1$

$\checkmark$

therefore $2^{(7-1)/2} \equiv 1 \pmod{7}$ meaning 2 is not a primitive root for 7

case for $n > 2$: ~~p can be~~

p can be defined as $p = 3 \cdot 8 \cdot 2^{(n-2)} + 1 \in p = 8k + 1$

and thus p mod 8 will always be 1 allowing us to use theorem 9.6 to show that $(2/p) = 1$

and thus $2^{(p-1)/2} \equiv 1 \pmod{p}$ making 2 not a primitive root for all p

cases cover all $n \geq 0$ ∗ exhaustion

3. a. p is prime ; $\gcd(ab, p) = 1 \Rightarrow$ a, b, or ab is a quadratic residue mod p

$$\therefore (ab/p) = (a/p)(b/p)$$

case a+b are non-residues:

$(ab/b) = (-1)(-1) = 1$ ∴ ab would have to be a residue

case ab + ~~b are non~~ residues:

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

$1 = (a/p)$ ∴ a would have to be a residue

case ab + a ~~are~~ non-residues:

$\cancel{(-1)} = \cancel{(-1)}(b/p)$

$1 = (b/p)$ ∴ b would have to be a residue

Because of the basic legrande symbol properties demonstrated above, at least one of a, b, ab must be a quadratic residue

b. $p \mid (n^2-2)(n^2-3)(n^2-6)$ ~~or equivalently prove~~ $\forall n$

p must divide at least one of $p \mid (n^2-2)$, $p \mid (n^2-3)$, $p \mid (n^2-6)$

rewritten as congruency at least one must hold

$n^2 \equiv 2 \pmod{p}$ or $n^2 \equiv 3 \pmod{p}$ or $n^2 \equiv 6 \pmod{p}$

rewritten as legrande symbols

$(2/p) \overset{?}{=} 1$ or $(3/p) \overset{?}{=} 1$ or $(6/p) \overset{?}{=} 1$

and because $(6/p) = (2/p)(3/p)$ part a tells us that at least one holds true, thus proving the existence of a multiple of such specification #

5. a. $(71/73)$ primes

$= (73/71)$ — 71 mod 4 = 3, 73 mod 4 = 1 quadratic reciprocity

$= (2/71)$ — 71 mod 8 = 7 theorem 9.6

$= \boxed{1}$

b. $(461/773)$ primes — 461 mod 4 = 1 quadratic reciprocity

$= (773/461)$

$= (312/461)$

$= \cancel{(2^2/461)}(2/461)(3/461)(13/461)$

$= (461/2)(461/3)(461/13)$

$= \cancel{(1/2)}(-1/3)(6/13)$

$= \left((-1)^{3-1/2}\right)(2/13)(3/13)$

13 mod 8 = 5

13 mod 12 = 1

$= (-1)\cancel{(1)(1)}$

$= \boxed{-1}$

c. $(3658/12703) = (2/12703)(59/12703)(31/12703)$ primes

$= \cancel{(2/12703)}(-(12703/59))(-(12703/31))$

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

$= (2/59)(3/59)\cancel{(3^2/59)}(2/31)\cancel{(2^2/31)}(3/31)$

$= \cancel{(-1)(-1)}(59/3)\cancel{(31/3)}$

$= (-1/3) = \left((-1)^{\frac{3-1}{2}}\right) = \boxed{-1}$

12703 mod 4 = 3

12703 mod 8 = 7

59 mod 4 = 3

31 mod 4 = 3

59 mod 8 = 3

31 mod 8 = 7

6. a. $x^2 \equiv 219 \pmod{419}$ prime

$\hookrightarrow 1 \overset{?}{\equiv} (219/419)$

419 mod 12 = 11 = -1

$= (3/419)(73/419)$

419 mod 12 = 11 = -1
Theorem 9.10

$= (73/419)$

$= (419/73)$ via quadratic reciprocity law

73 mod 4 = 1

$= (54/73)$

$= \cancel{(2/73)}(3/73)\cancel{(3^2/73)}$

73 mod 4 = 1
∴ (2/73) = 1

$= (3/73)$

$\boxed{\equiv 1}$

73 mod 12 = 1
∴ (3/73) = 1

Because 219 is a quadratic residue [illegible] we can conclude that the congruence has a solution. #

b. $3x^2 + 6x + 5 \equiv 0 \pmod{89}$ prime

~~$3(x^2 + 2x) \equiv -5 \equiv 84 \pmod{89}$~~ gcd(3, 89) = 1

~~$x^2 + 2x \equiv 28 \pmod{89}$~~

$y^2 \equiv (b^2 - 4ac) \equiv -24 \equiv \underline{65} \pmod{\underline{89}}$ must have a solution

$1 \overset{?}{\equiv} (65/89)$

89 mod 4 = 1

$= (5/89)(13/89)$

89 mod 4 = 1

$= (89/5)(89/13)$ Quadratic reciprocity law

$= (-1/5)\ (-2/13)$

$= \left(\cancel{(-1)^{(5-1)/2}}\right)(-1/13)(2/13)$

$= \left(\cancel{(-1)^{(13-1)/2}}\right)(2/13)$

13 mod 8 = 5

$\boxed{= -1}$ as 13 mod 8 = 5

Because $(b^2 - 4ac)$ is not a quadratic residue, the quadratic congruence must NOT have a solution.