9.4 Quadratic Congruence With Composite Moduli

Note Title 8/14/2006

1. (a) Show that 7 and 18 are the only incongruent solutions of $x^2 \equiv -1 \pmod{5^2}$

By Th. 8.12, $x^K \equiv -1 \pmod{25}$ has a solution $\iff (-1)^{\phi(25)/d} \equiv 1 \pmod{25}$, where $\phi(25) = 5^2 - 5 = 20$, $d = \gcd(K, \phi(25))$
Here $K=2$, $d = \gcd(2, \phi(25)) = 2$, and so $(-1)^{20/2} = (-1)^{10} = 1 \equiv 1 \pmod{25}$. $\therefore$ It has a solution, and Th. 8.12 says it has exactly $d = 2$ incongruent solutions.

$7 \not\equiv 18 \pmod{25}$, and $7^2 = 49 \equiv -1 \pmod{25}$, and $18^2 = 324 \equiv 24 \equiv -1 \pmod{25}$

To derive 7, 18, first solve for p^{k-1} to get x_0 and b

$\therefore x^2 \equiv -1 \pmod 5$, or $x^2 \equiv 4 \pmod 5$
$\therefore x_0 \equiv 2 \pmod 5$, $x_0^2 = 4 = -1 + (1)5$, so $x_0 = 2$, $b = 1$

Now solve $2x_0 y \equiv -b \pmod 5$, or $4y \equiv -1 \pmod 5$, $\therefore y_0 \equiv 1 \pmod 5$

$\therefore x_1 = x_0 + y_0 p^{k-1} = 2 + 1(5) = 7$ is a solution to $x^2 \equiv -1 \ (5^2)$, and $\therefore$ so is $-7 \equiv 18$.

$\therefore x \equiv 7, 18 \pmod{5^2}$

(b) Use part (a) to find the solutions of $x^2 \equiv -1 \pmod{5^3}$

(1) Solve $x^2 \equiv -1 \pmod{5^2}$. From (a), $x_0 = 7$.
$\therefore x_0^2 = a + b p^2$, or $7^2 = (-1) + b(5^2)$,
or $49 = (-1) + (2)(5^2)$, $b = 2$.

(2) Solve $2x_0 y \equiv -b \pmod{p}$, or

$14y \equiv -2 \pmod{5}$
$14y - 15y \equiv -2$
$-y \equiv -2$, or $y \equiv 2 \pmod{5}$

(3) $\therefore x_1 \equiv x_0 + y_0 p^2 = 7 + 2(5^2) = 57$

$\therefore \underline{x \equiv 57, -57} \pmod{5^3} \equiv 57, 68$

By Th. 8.12, $d = \gcd(k, \phi(5^3)) = \gcd(2, 100) = 2$, so exactly 2 solutions.

2. Solve each of the following quadratic congruences:

(a) $x^2 \equiv 7 \pmod{3^3}$

(1) First solve $x^2 \equiv 7 \pmod 3$, or $x^2 \equiv 1 \pmod 3$

Clearly, $x = \pm 1$. Choose $x = 1$.

$\therefore 1^2 = 7 + (-2)3$, so $x_0 = 1$, $b = -2$

(2) Solve $2x_0 y \equiv -b \pmod 3$, or

$2y \equiv 2 \pmod 3$, so $y = 1$.

(3) $\therefore$ A solution to $x^2 \equiv 7 \pmod{3^2}$ is

$x_0 + y_0 p = 1 + 1(3) = 4 = x_0'$

(4) $\therefore 4^2 = 7 + b' \cdot 3^2$, $b' = 1$.

(5) Now solve $2x_0' y' \equiv -b \pmod p$, or

$8y' \equiv -1 \pmod 3$, or $2y' \equiv 2 \pmod 3$,

so $y_0' = 1$

(6) $\therefore$ a solution to $x^2 \equiv 7 \pmod{3^3}$ is

$x_0' + y_0' \cdot 3^2 = 4 + (1) \cdot 9 = 13$. Also, -13.

(7) $\therefore x \equiv 13, -13$ or $\underline{x \equiv 13, 14} \pmod{3^3}$

(b) $x^2 \equiv 14 \pmod{5^3}$

(1) $x^2 \equiv 14 \pmod 5$, or $x^2 \equiv 4 \pmod 5$. $\therefore x_0 = 2$
$\therefore 2^2 = 14 + b \cdot 5$, $b = -2$

(2) $\therefore$ Solve $2x_0 y \equiv -b \pmod 5$, or $4y \equiv 2 \pmod 5$,
$2y \equiv 1 \pmod{5}$, $y = 3$

(3) $\therefore$ a solution to $x^2 \equiv 14 \pmod{5^2}$ is
$x_0 + y_0 p = 2 + 3(5) = 17$

(4) $\therefore 17^2 = 14 + b(5^2)$, $b = 11$

(5) $\therefore$ Solve $2x_0 y \equiv -b \pmod p$, or
$34y \equiv -11 \pmod 5$, or $4y \equiv 4 \pmod 5$,
$\therefore y = 1$.

(6) $\therefore$ a solution to $x^2 \equiv 14 \pmod{5^3}$ is
$17 + 1(5^2) = 42$, or -42. $125 - 42 = 83$

$\therefore x \equiv \underline{42, 83} \pmod{5^3}$

(c) $x^2 \equiv 2 \pmod{7^3}$

(1) $x^2 \equiv 2 \pmod 7$, $x_0 = 3$
$3^2 = 2 + (1)7$, so $b = 1$

(2) $2(3)y \equiv -1 \pmod 7$, or $6y \equiv 6 \pmod 7$,
$y = 1$.

(3) $\therefore$ solution to $x^2 \equiv 2 \pmod{7^2}$ is
$x_0 + yp = 3 + (1)\cdot 7 = 10$

$10^2 = 2 + b(7^2)$, $b = 2$

(4) $\therefore$ solve $2(10)y \equiv -2 \pmod 7$, or
$20y \equiv -2 \pmod 7$ or $-y \equiv -2 \pmod 7$,
$y = 2$

(5) $\therefore$ solution to $x^2 \equiv 2 \pmod{7^3}$ is
$10 + (2)(7^2) = 108$, -108. $7^3 - 108 = 343 - 108 =$
235

$\therefore x \equiv 108, 235 \pmod{7^3}$

3. Solve the congruence $x^2 \equiv 31 \pmod{11^4}$

(1) Solve $x^2 \equiv 31 \pmod{11}$, or $x^2 \equiv 9 \pmod{11}$. $\therefore x = 3$
$3^2 = 31 + b(11)$, $b = -2$.

(2) $\therefore 2(3)y \equiv 2 \pmod{11}$, $6y \equiv 2 \pmod{11}$, $y=4$

(3) $\therefore x+yp = 3+(4)(11) = 47$ is a solution to $x^2 \equiv 31 \pmod{11^2}$

$\therefore 47^2 = 31 + 6(11^2)$, $6 = 18$

(4) $\therefore 2x_0 y \equiv -6 \pmod{11} \Leftrightarrow 2(47)y \equiv -18 \pmod{11}$

$94y \equiv 4 \pmod{11}$, or $6y \equiv 4 \pmod{11}$

$12y \equiv 8 \pmod{11}$

$y \equiv 8 \pmod{11}$

(5) $\therefore 47 + 8(11^2) = 1015$ is a solution to $x^2 \equiv 31 \pmod{11^3}$.

$\therefore 1015^2 = 31 + 6(11^3)$, $6 = 774$

(6) $\therefore$ Solve $2x_0 y \equiv -6 \pmod{11}$, or

$2030y \equiv -774 \pmod{11}$, or

$6y \equiv 7 \pmod{11}$

$12y \equiv 14 \pmod{11}$

$y \equiv 3 \pmod{11}$

(7) $\therefore 1015 + 3(11^3) = 5008$ is a solution to $x^2 \equiv 31 \pmod{11^4}$. $11^4 - 5008 = 9633$

$\therefore x \equiv \underline{5008, 9633} \pmod{11^4}$

4. Find the solutions of $x^2+5x+6 \equiv 0 \pmod{5^3}$ and $x^2+x+3 \equiv 0 \pmod{3^3}$

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

$(x+3)(x+2) \equiv 0 \pmod{5^3}$, $\therefore$ $x \equiv -3, -2$, or
$x \equiv \underline{122, 123} \pmod{5^3}$

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

$\gcd(4, 3^3) = 1$, $\therefore$ $x^2+x+3 \equiv 0 \Leftrightarrow 4x^2+4x+12 \equiv 0$
$\Leftrightarrow (2x+1)^2 + 11 \equiv 0$
$\Leftrightarrow (2x+1)^2 \equiv 16 \pmod{3^3}$

$\therefore$ $2x+1 \equiv 4$, $2x+1 \equiv -4$
$2x \equiv 3$ $\quad$ $2x \equiv -5$
$28x \equiv 42$ $\quad$ $28x \equiv -70$ $\quad$ $(\gcd(14, 3^3) = 1)$
$x \equiv 42$ $\quad$ $x \equiv -70$
$x \equiv 15$ $\quad$ $x \equiv 11$

$\therefore$ $x \equiv \underline{11, 15} \pmod{3^3}$

5. Prove that if the congruence $x^2 \equiv a \pmod{2^n}$, where a is odd and $n \geq 3$, has a solution, then

it has exactly four incongruent solutions.

Pf: Note: can't invoke Th. 8.12 since 2^n has no primitive roots for $n \geq 3$.

Since a is odd, if x is a solution, Then x must be odd. Also, $-x$ is a solution.

Suppose y is any other solution.
$\therefore y^2 \equiv a \pmod{2^n}$, so $x^2 \equiv y^2 \pmod{2^n}$, $n \geq 3$.

$$\therefore (x-y)(x+y) \equiv 0 \pmod{2^n}$$

$$\Leftrightarrow \frac{x-y}{2} \cdot \frac{x+y}{2} \equiv 0 \pmod{2^{n-2}}, \quad n \geq 3$$
by Th. 4.3

But note That $\frac{x-y}{2} + \frac{x+y}{2} = x$, which is odd.

$\therefore$ Ony one of $\frac{x-y}{2}, \frac{x+y}{2}$ is even.

(1) Suppose $\frac{x-y}{2}$ is The even factor, so $\frac{x+y}{2}$ is The odd factor

$$\therefore (x-y)\left(\frac{x+y}{2}\right) \equiv 0 \pmod{2^{n-1}} \Rightarrow$$

$$x - y \equiv 0 \pmod{2^{n-1}} \Rightarrow$$
$$x \equiv y \pmod{2^{n-1}}$$

(2) Suppose $\frac{x+y}{2}$ is the even factor, so $\frac{x-y}{2}$ is the odd factor

$$\therefore (x+y)\left(\frac{x-y}{2}\right) \equiv 0 \pmod{2^{n-1}} \Rightarrow$$

$$x+y \equiv 0 \pmod{2^{n-1}} \Rightarrow$$
$$x \equiv -y \pmod{2^{n-1}}$$

(1), (2) $\Rightarrow$ if y is any other solution,

$$y = \pm x + k\,2^{n-1}$$

for k odd, $k = 2r+1$, some r.

$$\therefore y = \pm x + 2^{n-1} + r2^n$$

$$\therefore y \equiv \pm x + 2^{n-1} \pmod{2^n} \qquad [1]$$

for k even, $k = 2r$, some r.

$$\therefore y = \pm x + r\,2^n$$

$$\therefore y \equiv \pm x \pmod{2^n} \qquad [2]$$

$\therefore$ [1], [2] $\Rightarrow$ only incongruent solutions, mod 2^n, are $x, -x, x + 2^{n-1}, -x + 2^{n-1}$.

6. From $23^2 \equiv 17 \pmod{2^7}$, find three other solutions of the quadratic congruence $x^2 \equiv 17 \pmod{2^7}$

From #5 above, solutions are $23, -23, 23 + 2^6$, and $-23 + 2^6$ mod 2^7.

$2^6 = 64$, $2^7 = 128$. $\therefore -23 + 2^7 = 105$

$\therefore$ $\underline{\underline{23, 105, 87, 41 \pmod{2^7}}}$

7. First determine the values of a for which the congruences below are solvable, and then find the solutions of these congruences.

(a) $x^2 \equiv a \pmod{2^4}$

By Th. 9.12, solvable $\Leftrightarrow a \equiv 1 \pmod 8$.

$2^4 = 16$. $\therefore$ $\underline{\underline{a = 1 \text{ or } 9}}$

Now use #5 above.

$a = 1$: $x = 1, -1, 1 + 2^3, -1 + 2^3$

$x \equiv 1, -1+16, 9, 7$

$\therefore\ x \equiv \underline{1, 7, 9, 15} \pmod{2^4}$

$a = 9$: $x = 3, -3, 3+2^3, -3+2^3$

$\therefore\ x = \underline{3, 13, 11, 5}$

(b) $x^2 \equiv a \pmod{2^5}$

$2^5 = 32$. solvable $\iff a \equiv 1 \pmod 8$,

$\therefore\ a = 1, 9, 17,$ or 25

$a = 1$: $x \equiv \pm 1, \pm 1 + 2^4$

$\therefore\ x \equiv \underline{1, 31, 17, 15}$

$a = 9$: $x \equiv \pm 3, \pm 3 + 2^4$

$\therefore\ x \equiv \underline{3, 29, 19, 13}$

$a = 17$: $\therefore\ x^2 \equiv 17 + 32 = 49$

$\therefore\ x \equiv \pm 7, \pm 7 + 2^4$

$\therefore\ x \equiv \underline{7, 25, 23, 9}$

$a = 25$: $x \equiv \pm 5, \pm 5 + 2^4$

$\therefore x = 5, 27, 21, 11$

(c) $x^2 \equiv a \pmod{2^6}$

$2^6 = 64$. $\therefore$ solvable $\Leftrightarrow a \equiv 1 \pmod 8$

$\therefore a = 1, 9, 17, 25, 33, 41, 49, 57$

$a = 1$: $\pm 1, \pm 1 + 2^5$

$\therefore x \equiv 1, 63, 33, 31$

$a = 9$: $\pm 3, \pm 3 + 2^5$

$\therefore x \equiv 3, 61, 35, 29$

$a = 17$: $17 + 64 = 81$. $\therefore \pm 9, \pm 9 + 2^5$

$\therefore x \equiv 9, 55, 41, 23$

$a = 25$: $\pm 5, \pm 5 + 2^5$

$\therefore x \equiv 5, 59, 37, 27$

$a = 33$: $33 + 64 = 97, 33 + 128 = 161, 33 + 192 = 225$

$\therefore \pm 15, \pm 15 + 2^5$

$\therefore x \equiv 15, 49, 47, 17$

$a = 41$: $41 + 64 = 105, 41 + 128 = 169$

$\therefore \pm 13, \pm 13 + 2^5$

$\therefore x \equiv 13, 51, 45, 19$

$a = 49 : \pm 7, \pm 7 + 2^5$

$\therefore x \equiv 7, 57, 39, 25$

$a = 57 : 57 + 64 = 121$

$\therefore \pm 11, \pm 11 + 2^5$

$\therefore x \equiv 11, 53, 43, 21$

8. For fixed $n > 1$, show that all the solvable congruences $x^2 \equiv a \pmod{n}$ with $\gcd(a, n) = 1$ have the same number of solutions.

Pf: Let $n = 2^{k_0} p_1^{k_1} \cdots p_r^{k_r}$, $k_i \geq 0$

For $p_i^{k_i}$, $k_i \geq 1$, we can use Th. 8.12 to state that $x^2 \equiv a \pmod{p_i^{k_i}}$ has exactly 2 solutions.

The actual value of a doesn't matter, as long as $\gcd(a, p_i^{k_i}) = 1$.

For $x^2 \equiv a \pmod{2^{k_0}}$, $k_0 \geq 1$, Th. 9.12 states there are just 2 solutions for $x^2 \equiv a \pmod{2}$ (i.e., $1, -1$), 2 solutions for $x^2 \equiv a \pmod{4}$ when $a \equiv 1 \pmod{4}$

(i.e. $x = 1, 3$), and for $x^2 \equiv a \pmod{2^n}$, $n \geq 3$, when $a \equiv 1 \pmod 8$, problem #5 shows there are exactly 4 solutions.

$\therefore$ if $\gcd(a, n) = 1$, then there are $2 \cdot 2^r$ possible solutions if $a \equiv 1 \pmod 4$ and $a \not\equiv 1 \pmod 8$, and $4 \cdot 2^r$ possible solutions if $a \equiv 1 \pmod 8$.
Label these solutions x_{iK_i}, so that, for example, x_{1K_1} and x_{2K_1} are the solutions to $x^2 \equiv a \pmod{p_1^{K_1}}$

$\therefore$ Consider the $4 \cdot 2^r$ ($a \equiv 1 \pmod 8$) or $2 \cdot 2^r$ ($a \equiv 1 \pmod 4$, $a \not\equiv 1 \pmod 8$) linear equation systems:

$$\begin{array}{ll} x \equiv x_{1K_0} \pmod{2^{K_0}} & x \equiv x_{2K_0} \pmod{2^{K_0}} \\ \vdots & \vdots \\ x \equiv x_{1K_r} \pmod{p_r^{K_r}} & x \equiv x_{1K_r} \pmod{p_r^{K_r}} \\ & \\ \vdots \qquad \cdots & x \equiv x_{2K_0} \pmod{2^{K_0}} \\ & \vdots \\ & x \equiv x_{2K_r} \pmod{p_r^{K_r}} \end{array}$$

By the Chinese Remainder Th., there is a simultaneous solution unique to $n = 2^{k_0} p_1^{k_1} \cdots p_r^{k_r}$ for each system.

Thus, the number of solutions is, for any a with $\gcd(a, n) = 1$:

2^r, if $n = p_1^{k_1} \cdots p_r^{k_r}$

$2 \cdot 2^r$, if $n = 2 p_1^{k_1} \cdots p_r^{k_r}$

$2 \cdot 2^r$, if $n = 2^2 p_1^{k_1} \cdots p_r^{k_r}$ and $a \equiv 1 \pmod 4$,

$4 \cdot 2^r$, if $n = 2^{k_0} p_1^{k_1} \cdots p_r^{k_r}$, $k_0 \geq 3$ and $a \equiv 1 \pmod 8$

9. (a) Without actually finding them, determine the number of solutions of the congruences $x^2 \equiv 3 \pmod{11^2 \cdot 23^2}$ and $x^2 \equiv 9 \pmod{2^3 \cdot 3 \cdot 5^2}$

(1) $x^2 \equiv 3 \pmod{11^2 \cdot 23^2}$

$x^2 \equiv 3 \pmod{11^2}$ and $x^2 \equiv 3 \pmod{23^2}$

each will have 2 solutions (by Th. 8.12)

so $2 \cdot 2 = \underline{4}$ solutions

(2) $x^2 \equiv 9 \pmod{2^3 \cdot 3 \cdot 5^2}$

$x^2 \equiv 9 \pmod{2^3}$ has 4 (by prob. #5)

$x^2 \equiv 9 \pmod{3} \Leftrightarrow x^2 \equiv 0 \pmod{3}$, so just 1 solution ($x \equiv 0$).

$x^2 \equiv 9 \pmod{5^2}$ has 2 solutions.

$\therefore 4 \cdot 1 \cdot 2 = \underline{8}$ solutions

(6) Solve $x^2 \equiv 9 \pmod{2^3 \cdot 3 \cdot 5^2}$

$x^2 \equiv 9 \pmod{2^3}$

$x = \pm 3,\ \pm 3 + 2^2$ by prob. #5,

$\therefore x \equiv 3, 5, 7, 1 \pmod{2^3}$

$x^2 \equiv 9 \pmod{3} \Leftrightarrow x \equiv 0 \pmod{3}$

$x^2 \equiv 9 \pmod{5^2}$

$x = \pm 3$, or $x \equiv 3, 22 \pmod{5^2}$

(1) $x \equiv 1 \pmod{8}$

$x \equiv 0 \pmod{3}$

$x \equiv 3 \pmod{25}$

$n = 600 = 2^3 \cdot 3 \cdot 5^2$

$N_1 = 75 = 3 \cdot 5^2$

$N_2 = 200 = 2^3 \cdot 5^2$

$N_3 = 24 = 2^3 \cdot 3$

$\therefore 75 x_1 \equiv 1 \pmod{8}$

$3x_1 \equiv 1,\ 9x_1 \equiv 3$

$x_1 \equiv 3$

$200 x_2 \equiv 1 \pmod{3}$

$2x_2 \equiv 1,\ 4x_2 \equiv 2$

$x_2 \equiv 2$

$24x_3 \equiv 1 \pmod{25}$

$-x_3 \equiv 1, \; x_3 \equiv -1 \equiv 24$

$\therefore (1)(75)(3) + 0\cdot(200)(2) + (3)(24)(-1) = 153$

$\therefore x \equiv \underline{153} \pmod{2^3\cdot 3\cdot 5^2}$

(2) $x \equiv 3 \pmod 8$ as above, $N = 2^3\cdot 3\cdot 5^2$

$x \equiv 0 \pmod 3$ $N_1 = 75, N_2 = 200, N_3 = 24$

$x \equiv 3 \pmod{25}$ $x_1 = 3, \; x_2 = 2, \; x_3 = -1$

$\therefore x = (3)(75)(3) + 0 + (3)(24)(-1) = 603$

$\therefore \underline{x \equiv 3} \pmod{2^3\cdot 3\cdot 5^2}$

(3) $x \equiv 5 \pmod 8$ as in (1), $N = 2^3\cdot 3\cdot 5^2$

$x \equiv 0 \pmod 3$ $N_1 = 75, N_2 = 200, N_3 = 24$

$x \equiv 3 \pmod{25}$ $x_1 = 3, \; x_2 = 2, \; x_3 = -1$

$\therefore x = (5)(75)(3) + 0 + (3)(24)(-1) = 1053$

$\therefore \underline{x \equiv 453} \pmod{2^3\cdot 3\cdot 5^2}$

(4) $x \equiv 7 \pmod 8$ as in (1), $N = 2^3\cdot 3\cdot 5^2$

$x \equiv 0 \pmod 3$ $N_1 = 75, N_2 = 200, N_3 = 24$

$x \equiv 3 \pmod{25}$ $x_1 = 3, \; x_2 = 2, \; x_3 = -1$

$\therefore\ x = (7)(75)(3) + 0 + (3)(24)(-1) = 1503$

$\therefore\ x \equiv \underline{303} \pmod{2^3 \cdot 3 \cdot 5^2}$

(5) $x \equiv 1 \pmod 8$ as in (1), $N = 2^3 \cdot 3 \cdot 5^2 = 600$
$x \equiv 0 \pmod 3$ $N_1 = 75, N_2 = 200, N_3 = 24$
$x \equiv 22 \pmod{25}$ $x_1 = 3,\ x_2 = 2,\ x_3 = -1$

$x = (1)(75)(3) + 0 + (22)(24)(-1) = -303$

$\therefore\ x \equiv \underline{297} \pmod{2^3 \cdot 3 \cdot 5^2}$

(6) $x \equiv 3 \pmod 8$ as in (1), $N = 2^3 \cdot 3 \cdot 5^2 = 600$
$x \equiv 0 \pmod 3$ $N_1 = 75, N_2 = 200, N_3 = 24$
$x \equiv 22 \pmod{25}$ $x_1 = 3,\ x_2 = 2,\ x_3 = -1$

$x = (3)(75)(3) + 0 + (22)(24)(-1) = 147$

$\therefore\ x \equiv \underline{147} \pmod{2^3 \cdot 3 \cdot 5^2}$

(7) $x \equiv 5 \pmod 8$ as in (1), $N = 2^3 \cdot 3 \cdot 5^2 = 600$
$x \equiv 0 \pmod 3$ $N_1 = 75, N_2 = 200, N_3 = 24$
$x \equiv 22 \pmod{25}$ $x_1 = 3,\ x_2 = 2,\ x_3 = -1$

$x = (5)(75)(3) + 0 + (22)(24)(-1) = 597$

$\therefore x \equiv \underline{597} \pmod{2^3 \cdot 3 \cdot 5^2}$

(8) $x \equiv 7 \pmod 8$ as in (1), $N = 2^3 \cdot 3 \cdot 5^2 = 600$
$x \equiv 0 \pmod 3$ $N_1 = 75,\ N_2 = 200,\ N_3 = 24$
$x \equiv 22 \pmod{25}$ $x_1 = 3,\ x_2 = 2,\ x_3 = -1$

$$x = (7)(75)(3) + 0 + (22)(24)(-1) = 1047$$

$\therefore x \equiv \underline{447} \pmod{2^3 \cdot 3 \cdot 5^2}$

$\therefore \underline{x \equiv 3, 147, 153, 297, 303, 447, 453, 597 \pmod{2^3 \cdot 3 \cdot 5^2}}$

10. (a) For an odd prime p, prove that the congruence $2x^2 + 1 \equiv 0 \pmod p$ has a solution if and only if $p \equiv 1$ or $3 \pmod 8$.

Pf: As $\gcd(8, p) = 1$, $2x^2 + 1 \equiv 0 \pmod p$ has a solution $\Leftrightarrow$ $8(2x^2+1) \equiv 0 \pmod p$ has a solution.
$\therefore$ Look at $16x^2 = (4x)^2 \equiv -8 \pmod p$.
Let $y = 4x$, Then can solve $4x \equiv y \pmod p$ since $y^2 \equiv -8$, $\gcd(y^2, p) = \gcd(y, p) = 1$, so $4x \equiv y \pmod p$ has a unique

solution.

$\therefore\ y^2 \equiv -8 \pmod{p}$ has a solution

$\iff (-8/p) = 1$

$(-8/p) = (-1/p)(2^3/p) = (-1/p)(2/p)$

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

(a) $(2/p) = -1 \iff p \equiv 3 \pmod 8$ or
$p \equiv 5 \pmod 8$

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

$\iff \frac{p-1}{2} = 2k+1$, some k

$\iff p-1 = 4k+2$

$\iff p = 3+4k$

$\therefore\ (2/p) = (-1/p) = -1 \iff p \equiv 3 \pmod 8$

(b) $(2/p) = 1 \iff p \equiv 1 \pmod 8$ or
$p \equiv 7 \pmod 8$

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

$\Leftrightarrow \frac{p-1}{2} = 2k$, some k

$\Leftrightarrow p-1 = 4k$

$\Leftrightarrow p = 1+4k$

$\therefore (2/p) = (-1/p) = 1 \Leftrightarrow p \equiv 1 \pmod 8$

$\therefore$ (a) + (b) show $2x^2+1 \equiv 0 \pmod p \Leftrightarrow$
$p \equiv 1$ or $3 \pmod 8$

(b) Solve the congruence $2x^2+1 \equiv 0 \pmod{11^2}$

Let $z = 4x$, $\therefore z^2 \equiv -8 \pmod{11^2}$

Use method discribed in proof to Th. 9.11

First solve $z^2 \equiv -8 \pmod{11}$

$\therefore z^2 \equiv 3 \pmod{11}$
$z \equiv 5 \pmod{11}$ $\quad \therefore x_0 = 5$

$\therefore x_0^2 = -8 + b(11)$, $b = 3$

Now solve $2x_0 y \equiv -b \pmod p$

$\therefore\ 2(5)y \equiv -3 \pmod{11}$

$-y \equiv -3 \pmod{11}$

$y \equiv 3 \pmod{11}$ $\quad y_0 = 3$

$\therefore\ x_0 + y_0 p = 5 + 3(11) = 38$

$\therefore\ z = 38$ solves $z^2 \equiv -8 \pmod{11^2}$

Now convert back using $z \equiv 4x \pmod{11^2}$

$\therefore\ 4x \equiv 38 \pmod{11^2}$

$2x \equiv 19 \pmod{121}$

$122x \equiv 19(61) = 1159 \pmod{121}$

$x \equiv 1159 \equiv 70 \pmod{11^2}$

$\therefore\ x \equiv \pm 70 \pmod{11^2}$

$\therefore\ x \equiv \underline{51, 70} \pmod{11^2}$