

Handout for Sections 9.1, 9.2, & 9.3

① Remember the relation between the solutions of $ax^2 + bx + c \equiv 0 \pmod{p}$ and $y^2 \equiv d \pmod{p}$, where $y = 2ax + b$ & $d = b^2 - 4ac$

② Does $x^2 \equiv 7 \pmod{31}$ have a soln.?

i.e., is 7 a quad. residue of 31? i.e., check $7^{15} \equiv 1 \pmod{31}$?

$$7^2 \equiv 49 \equiv 18 \pmod{31}, 7^4 \equiv 18^2 \equiv 324 \equiv 14 \pmod{31},$$

$$7^8 \equiv 14^2 \equiv 196 \equiv 10 \pmod{31}, 7^{16} \equiv 10^2 \equiv 100 \equiv 7 \pmod{31}$$

Since, 7 & 31 are coprime, we get $7^{15} \equiv 1 \pmod{31}$.

So, a soln. exists & since $(7^8)^2 \equiv 7 \pmod{31}$, $x \equiv 7^8$ is a soln., $\& 7^8 \equiv 10 \pmod{31}$, so $x \equiv 10 \pmod{31}$ is a soln.

The second soln. is $x \equiv 21 \pmod{31}$ ($\because 21 = 31 - 10$).

③ Does $x^2 \equiv 85 \pmod{97}$ have soln.? i.e., find $(85/97)$.

$$(85/97) = (-12/97) = (-1/97)(4/97)(3/97)$$

Since $85 \equiv -12 \pmod{97}$ by multiplicity

$$= (-1/97)(3/97) = 1$$

since $4 = 2^2$

$$(-1/97) = (-1)^{\frac{97-1}{2}} = (-1)^{48} = 1$$

$$(3/97) = (97/3) = (1/3) = 1$$

By QRL

since $97 \equiv 1 \pmod{4}$

So,
soln.
exists.

$$(85/97) = (-1/97)(3/97) = 1$$

④ Solve $3x^2 + 9x + 7 \equiv 0 \pmod{13}$

This is the same as $y^2 \equiv 10 \pmod{13}$ where $y \equiv 6x + 9 \pmod{13}$

Clearly, $y \equiv \pm 6 \pmod{13}$ is also the solutions,

so, $6x + 9 \equiv 6 \pmod{13}$ & $6x + 9 \equiv -6 \pmod{13}$ give the solns. for x .

$6x \equiv -3 \pmod{13}$ gives $x \equiv 6 \pmod{13}$, by EA or Blabkshup

$6x \equiv -15 \pmod{13}$ gives $x \equiv 4 \pmod{13}$, by — n —

$$⑤ (19/23) = (-4/23) = (4/23)(-1/23) = 1 \cdot (-1) = -1$$

$$(-23/59) = (36/59) = (6^2/59) = 1$$

(2)

$$(-53/2d) = (3d/2d) = (d/d) = 1$$

$$\textcircled{2} \quad (1/d^3) = (-1/\sqrt{3}) = (\sqrt{3})(-\sqrt{3}) = 1 \cdot (-1) = -1$$

$$p \equiv -12 \pmod{13} \Rightarrow d \equiv 1 \pmod{13} \Rightarrow p \equiv -1 \pmod{13}$$

⑦ Find $(7/13)$ using Gauss Lemma.

$$\frac{13-1}{2} = 6 \text{ so, } S = \{7, 14, 21, 28, 35, 42\}$$

modulo 13, $7 \equiv 7, 14 \equiv 1, 21 \equiv 8, 28 \equiv 2, 35 \equiv 9, 42 \equiv 3$.

Out of which: 7, 8, and 9 are larger than 6.5

$$\therefore (7/13) = (-1)^3 = -1$$

⑧ Using QRL, $(-219/383) = (-1/383)(3/383)(7^3/383)$

$$(-1/383) = (-1)^{(383-1)/2} = (-1)^{191} = -1$$

$$(3/383) = (383-3)/2 = -(18/73) = -(9/73)(2/73) = -(1)(+1) = -1$$

$$(7^3/383) = (-13\sqrt{7}) = (-1\sqrt{7})(\sqrt{13})(\sqrt{13}) = 1$$

$$\textcircled{3} \quad \text{Now } x_5 \equiv 82 \pmod{31} \text{ from step 3 to find } (82/31)$$

$$\text{Using CRT, } x_5 \equiv 12 \pmod{31} \quad x_5 \equiv 25 \pmod{31} \quad (x_5-12)/31 = 1$$

$$\text{Now } x_6 \equiv 12 \pmod{31} \quad \text{and } (x_6)_5 = 12 \pmod{31} \quad x_6 \equiv 12 \pmod{31}$$

$$\text{Now } x_6 \equiv 12 \pmod{31} \quad \text{and } x_6 \equiv 12 \pmod{31} \quad \text{from step 3}$$

$$x_6 \equiv 12 \pmod{31} \quad \text{and } x_6 \equiv 12 \pmod{31} \quad x_6 \equiv 12 \pmod{31}$$

$$x_6 \equiv 12 \pmod{31} \quad \text{and } x_6 \equiv 12 \pmod{31} \quad x_6 \equiv 12 \pmod{31}$$

$$\text{Now } 12 \pmod{31} \text{ is a primitive root of 31. } \{12^k \pmod{31}\}_{k=0}^{30}$$

$$\text{Now } x_6 \equiv 12 \pmod{31} \quad \text{and } x_6 \equiv 12 \pmod{31}$$

$$x_6 \equiv 12 \pmod{31} \quad \text{and } x_6 \equiv 12 \pmod{31} \quad x_6 \equiv 12 \pmod{31}$$

$$\text{Now } x_6 \equiv 12 \pmod{31} \quad \text{and } x_6 \equiv 12 \pmod{31}$$

$$\text{Hence } x_6 \equiv 12 \pmod{31}$$

(1)