Name: Rajat Rajesh Shetty
IWID: 10477484.

Assignment-6

Exercise 6.1 solve quadratic congruence $x^2+7x+1 \equiv_{11} 0$

$\Rightarrow$ $x^2+7x+1 \equiv_{11} 0$

$x^2+7x \equiv_{11} -1$

$x^2+7x \equiv_{11} 10$

$x^2 \equiv_{11} 4x+10$

Applying $\pm a^{(p+1)/4}$ as $\Rightarrow$ $x = (4x+10)^3$

$\Rightarrow \boxed{11 \equiv_4 3}$

$x = (4x+10)(4x+10)(4x+10)$

$\Rightarrow 2.(2x+5)2.(2x+5).2(2x+5)$

$\Rightarrow 2^3.(2x+5)(2x+5)^2$

$x = -3$ or 8 or $(2x+5)$ or $(2x+5)^2$

$x = -5/2$

Let consider $(2x+5)^2$

$4x^2+20x+25$

$4x^2+9x+3 \equiv_{11} 0$.

$4x^2 \equiv_{11} -9x-3$

$= 2x+8$

$\therefore x = -8/2 = -4$

$-4 \bmod 11$

$\Rightarrow 7$

$=$

Verifying with answers $-3, 8, 7$.

$x^2+7x+1 = 3^2-21+1$ ×

$x=8$: $64+56+1 = -2+1+1 = 0$ ✓

$x=7$ $49+49+1 = 99 \bmod 11 = 0$ ✓

$\therefore$ 7, 8 are soln to the given eqn.

Exercise 6.2

Find all square roots of 11 modulo 35.

$x^2 \equiv_{35} 11$

$x^2 \equiv_5 11$, $x^2 \equiv_7 11$

$\Rightarrow \begin{cases} x^2 \equiv_5 1 \\ x^2 \equiv_7 4 \end{cases} \Rightarrow \begin{cases} x \equiv_5 \pm 1 \\ x \equiv_7 \pm 2 \end{cases}$

all combinat^n

$x \equiv_5 1 \quad x \equiv_7 2$

$x \equiv_5 -1 \quad x \equiv_7 2$

$x \equiv_5 1 \cdot x \equiv_7 -2$

$x \equiv_5 -1 \quad x \equiv_7 -2$

$x \equiv_5 1$, $x \equiv_7 4$

$\begin{cases} x \equiv_5 4 \\ x \equiv_7 2 \end{cases}$ $\begin{cases} x \equiv_5 1 \\ x \equiv_7 5 \end{cases}$ $\begin{cases} x \equiv_5 4 \\ x \equiv_7 5 \end{cases}$

using chinese remainder theorem, we get

$x \equiv_{35} 16, 9, 26, 19$

Exercise 6.3

Find the values of the following legendre symbols.

(a) $19/23$ (b) $18/23$

(a) $a = 19 \quad p = 23$

$a/p = a^{(p-1)/2}$

$= 19^{(23-1)/2} \Rightarrow 19^{11} \quad \therefore (19/23) = -1$ //

$19^{11} \equiv_{23} -1$

or

$\left(\frac{19}{23}\right) = \left(\frac{-23}{19}\right) = \left(\frac{-4}{19}\right) = -\left(\frac{2}{19}\right)\left(\frac{2}{19}\right)$

$\Rightarrow -(-1)(-1) \Rightarrow -1$ //

(b) $18/43$

$a = 18$. $p = 43$. $\quad 18^{21} \equiv_{43} -1$

$18^{(43-1)/2} \Rightarrow 18^{21}$ $\quad \therefore (18/43) = -1$ //

$$(18/43) = (2/43)(9/43) \Rightarrow -1 \cdot (34/43) = -1 \cdot (2/43)\left(\frac{-17}{43}\right)$$

$$\Rightarrow (-17/43) = (26/43) = -1 \cdot (4/13) = -1 \cdot (2/13) \cdot (2/13)$$

$\Rightarrow -1$

Exercise 6.4

Assume that a is a quadratic residue of an odd prime p & $ab \equiv_p a$. P.T either both a & b are quadratic residues of p, or both quadratic non residues of p.

$\Rightarrow$ a is a quadratic residue of p & $ab \equiv_p a$

$x^2 \equiv_p r$ $\quad ab \equiv_p a$.

So since a is a residue

$(ab)^{p-1/2} \equiv_p a^{(p-1)/2}$ $\quad$ since $r^{(p-1)/2} = 1$

so, $(ab)^{p-1/2} \equiv_p 1$

For $(ab)^{p-1/2} \equiv_p 1$ to be true

$a^{p-1/2} \equiv_p b^{p-1/2} = 1$

or

$a^{p-1/2} = b^{p-1/2} \equiv -1 \bmod p$.

Thus both a, b are quadratic residues of p or non-residues of p by Euler's Criteria.

Exercise 6.5

For a remote coin toss, Alice selects $p=47, q=79$. Bob chooses $x=123$. of 4 no Alice then calculates which 2 represents loosing calls? which 2 are present willing calls?

⇒ $n = p \cdot q$ $\quad x=123$.

$= 47 \cdot 79 = 3713$. $\quad \gcd(123, 3713) = 1$

$a = x^2 \% n$.

$= 123^2 \% 3713 \equiv 277$.

$x^2 \equiv_{47} 277 \equiv_{47} 42$

$42^{\frac{47+1}{4}} = 42^{12}$

$x^2 \equiv_{47} 277$

$x^2 \equiv_{79} 277$ $\Rightarrow$ $\begin{cases} x^2 \equiv_{47} 42 \\ x^2 \equiv_{79} 40 \end{cases}$ $\Rightarrow$ $\begin{cases} 42^{12} \equiv_{47} 18 \text{ & we get } \pm 18 \\ 40^{20} \equiv_{79} 44 \text{ & } \pm 44 \end{cases}$ $\quad 40^{\frac{79+1}{4}} = 40^{20}$

so, we will have 4 systems of linear congruences

$\begin{cases} x \equiv_{47} 18 \\ x \equiv_{79} 44 \end{cases}$ $\begin{cases} x \equiv_{47} -18 \\ x \equiv_{79} 44 \end{cases}$ $\begin{cases} x \equiv_{47} 18 \\ x \equiv_{79} -44 \end{cases}$ $\begin{cases} x \equiv_{47} -18 \\ x \equiv_{79} -44 \end{cases}$

using CRT,

$x \equiv_{3713} 676, 123, 3590, 3037.$

$-123 \equiv_{3713} 3590$ $\quad -676 \equiv_{3713} 3037.$

if Alice sends 3590 or 123 Alice wins. } winning calls

if Alice sends 676 & 3037 she loses } loosing calls