Exercise 4.1

→ let $d' \leftarrow \dfrac{d}{\gcd(d,p-1)}$, $\quad p'-1 \leftarrow \dfrac{p-1}{\gcd(d,p-1)}$

⇒ $x^{d'} - a$ in $\mathbb{Z}_{p'}$ has a unique root $= a^{k'}$

where $d'k' \equiv 1 \mod (p'-1)$

if $a^{k'} \not\equiv 1$ ⇒ No sol^n

else $k', 2k', 3k' \dots \gcd(d,p-1)k'$ are all powers (p) s.t. a^p is a root.

∴ 0 sol^n or $\gcd(d,p-1)$ sol^n

Exercise 4.2

→ Every 2 steps, degree reduces by 1

cost of division = $d \log d$

⇒ $O(2\cdot d\cdot \underbrace{d^2 \cdot \log^2(p)}_{\text{each step}})$

each step d terms requiring $d\cdot \log p$ time computation

Date :
Page No.:

Exercise 4.3

$\mathbb{Z}_{67}$

(i) $x^5 = 3$ $(x^d = a)$

$d = 5$ $p-1 = 66$ $\Rightarrow$ $\gcd(d, p-1) = 1$

$\therefore 5k = 1 \mod 66$

$\Rightarrow 5k - 66y = 1$

$(-13, -1)$

$\therefore -13 \equiv 54 \mod 67$

$\therefore x = 3^{54}$ is a solution

(ii) $x^3 = 2$ $x^d = a$

$d = 3$ $p-1 = 66$ $\gcd(d, p-1) = 3$

$d' = 1$ $p'-1 = 22$

$\therefore x = 2$ in $\mathbb{Z}_{23}$ solution is 2^{22}

$\Rightarrow$ ~~other solutions~~

2^{22} in $\mathbb{Z}_{67} = 37 \neq 1$

$2^0 = 1$, $2^1 = 2$, $2^2 = 4$, $2^4 = 16$, $2^8 = -10$, $2^{16} = 8$

$\therefore 2^{20} = 18 = (-5$

$2^{22} = -20 = 3$

No solution

(iii) $x^2 = 3$ $x^d = a$

$d = 2$ $p-1 = 66$ $\Rightarrow \gcd = 2$

$x = 3$ in $\mathbb{Z}_{34}$

3^{33} in $\mathbb{Z}_{67} = -1$ $\therefore$ No solution

Date :

Page No.:

(iv) $x^2 = 17$

$\to 17^{33} \bmod 67 = 1$

$\therefore$ has 2 solutions

$x = 33$ and 34

~~17^{33} is a solution~~

~~17^{66} is a solution~~

Exercise 4.4

$\to$ $h(x) - f(x) = \alpha(x)\, q(x)$

$h(x) - g(x) = \beta(x)\, r(x)$

$\therefore h(x) = f(x) + \alpha(x) q(x) = g(x) + \beta(x) r(x)$

$\Rightarrow$ We can solve $\alpha(x)q(x) - \beta(x)r(x) = g(x) - f(x)$ using euclids Algorithm to find $\alpha(x)$, $\beta(x)$

This is possible because $q(x)$, $r(x)$ are irreducible, $\therefore$ no common factors, hence $\gcd = 1$ $\therefore$ By Bezout's Lemma $\alpha(x)$, $\beta(x)$ exist

Exercise 4.5

(a) $x^2 + 1$ in $\mathbb{Z}_{11}$, check if $x^2 = 10$ has solutions

$10^{\frac{10}{2}} = 10^5$

$10^1 = 10$, $10^2 = 1$ $10^4 = 1$ $\Rightarrow 10^5 = 10 \neq 1$

$\therefore$ No solⁿ hence irreducible

Date :
Page No.:

Illy $x^2 = 2$

$\Rightarrow$ check $2^5 = 32$ mod 11 $= -1$

hence no soln

(b) $f(x) - (x+2) = \alpha(x)(x^2+1)$

$f(x) - (2x-3) = \beta(x)(x^2-2)$

$\Rightarrow \cancel{(x+2)}\ (2x-3) - (x+2) = \alpha(x)(x^2+1) - \beta(x)(x^2-2)$

$\Rightarrow x - 5 = \alpha(x)(x^2+1) - \beta(x)(x^2-2)$

first solve for $p = 1$

a	b	q	x	y	u	v
x^2+1	x^2-2	1	1	0	0	1
x^2-2	3	$4x^2+7$	0	1	1	-1
3	0	–	1	-1		

$(1, 1)$

$$x^2-2 \overline{\left) \begin{array}{l} x^2+1 \\ x^2-2 \\ \hline 3 \end{array} \right.}^{\,1}$$

$$3 \overline{\left) \begin{array}{l} x^2-2 \\ x^2 \\ \hline 10 \\ 10 \end{array} \right.}^{\,4x^2+7}$$

Date :
Page No.:

$\therefore \alpha(x) = 1 \quad \beta(x) = 1 \Rightarrow 1(x^2+1) - 1(x^2-2) = 3$

$\therefore 3^{-1} = 4$

$\therefore 4(x^2+1) - 4(x^2-2) = 1$

$\therefore$ to solve $(x-5)$ just multiply

$4(x-5)(x^2+1) - 4(x-5)(x^2-2) = x-5$

$\therefore f(x) = x+2 + 4(x-5)(x^2+1)$

$= x+2 + 4(x^3-5x^2+x-5)$

$= 4x^3 - 20x^2 + 5x - 18$

$= \underline{4x^3 + 2x^2 + 5x + 4}$