Name: Rajat Rajesh Shetty

CWID: 10477484

Assignment -5

Exercise 5.1 Compute All distinct powers of 2 modulo $n=29$ to find $\log_2(21)$

$2^1 \equiv_{29} 2$

$2^2 \equiv_{29} 4$

$2^3 \equiv_{29} 8$

$2^4 \equiv_{29} 16$

$2^5 \equiv_{29} 3$

$2^6 \equiv_{29} 6$

$2^7 \equiv_{29} 12$

$2^8 \equiv_{29} 24$

$2^9 \equiv_{29} 19$

$2^{10} \equiv_{29} 9$

$2^{11} \equiv_{29} 18$

$2^{12} \equiv_{29} 7$

$2^{13} \equiv_{29} 14$

$2^{14} \equiv_{29} 28$

$2^{15} \equiv_{29} 27$

$2^{16} \equiv_{29} 25$

$\boxed{2^{17} \equiv_{29} 21}$ — (1)

$2^1 = 2 \bmod 29$

$2^2 = 4 \bmod 29$

$2^3 = 8 \bmod 29$

$2^4 = 16 \bmod 29$

$2^5 = 32 = 3 \bmod 29$

$2^6 = 6 \bmod 29$

$2^7 = 2.2^6 = 12 \bmod 29$

$2^8 = 2.2^7 = 24 \bmod 29$

$2^9 = 2.2^8 = 19 \bmod 29$

$2^{10} = 2.2^9 = 9 \bmod 29$

$2^{11} = 18 \bmod 29$

$2^{17} = 21 \bmod 29$

$2^{18} = 13 \bmod 29$

$2^{19} = 26 \bmod 29$

$2^{20} = 23 \bmod 29$

$2^{21} = 17 \bmod 29$

$2^{22} = 5 \bmod 29$

$2^{23} = 10 \bmod 29$

$2^{24} = 20 \bmod 29$

$2^{25} = 11 \bmod 29$

$2^{26} = 22 \bmod 29$

$2^{27} = 15 \bmod 29$

$2^{28} = 1 \bmod 29$

find $\log_2(21)$ so Let $x = \log_2(21)$

$\Rightarrow 2^x = 21$

From (1), we get $2^{17} = 21 \bmod 29$

$\therefore x = 17.$

$\boxed{\log_2(21) = x = 17.}$

Exercise 5.2 use computations done in 5.1 to solve an instance $n=29$, $g=2$, $A=18$, $B=14$ of CDH. $p=29$ $g^{ab} \% p$ $a = \log_g(A)$ $b = \log_g(13)$

$a = \log_2(18)$

$2^a = 18 \bmod 29$

$\Rightarrow$ from computation

$2^{11} = 18 \bmod 29$

$\therefore a = 11$

$b = \log_g(B)$

$= \log_2(14)$

$2^b = 14 \bmod 29$

$2^{13} = 14 \bmod 29$

$b = 13$

$\therefore g^{ab} \% p.$

$2^{11 \cdot 13} \% 29$

$2^{143} \% 29$

$= 8$

Exercise 5.3 Suppose that Bob sends a message to Alice using Elgamal protocol. For public information collected by Eve $n=29$, $g=2$, $A=17$, $C_1=6$ & $C_2=10$ find m. use computations done in Exercise 5.1

⇒ $P=29$ $g=2$ $A=17$ $C_1=6$ $C_2=10$. find m.

$A = g^a \% p = 17 \Rightarrow 2^{21} \% 29 = 17.$

$a = 21$

another way to check $m = \frac{C_2}{C_1^a} \% 29.$

$= \frac{10}{6^{21}} \bmod 29$

$= (10 \cdot 12 \cdot 12) \bmod 29$

$\boxed{m = 19}$ //

$6^{-21} = 2^{-21} \cdot 3^{-21} \pmod{29}$

$2^{-21} \bmod 29 \Rightarrow 15^{21} \bmod 29$

$3^{-21} \bmod 29 \Rightarrow 10^{21} \bmod 29$

modulo inverse of 2 & 3 are (15 & 10 respectively) mod 29

$6^{-21} \bmod 29 = 6^7 \bmod 29$

$\Rightarrow 28$

$(28 \times 10) \bmod 29$

$= 19$

Exercise 5.4

For $n=37$ use the baby step-giant step algorithm to compute $\log_2(3)$ modulo n. I expect to see the list of babysteps, the list of giantstep, and a matching pair.

⇒ $n=37.$ $\log_2(3) \bmod 37.$

$g=2$

$\varphi(37) = 36 \Rightarrow ppf(36) = 2^2 \cdot 3^2.$

$121 = 36 = N.$ $n = 1 + \sqrt{N}$ $n = 7$

$2^{36} \equiv_{37} 1$ $2^9 \equiv_{37} 31.$ $2^4 \equiv_{37} 16$

$2^{18} \equiv_{37} 36$

$2^{12} \equiv_{37} 26.$

List of babysteps:

$2^0 \equiv_{37} 1$ $2^1 \equiv_{37} 2$ $2^2 \equiv_{37} 4$ $2^3 \equiv_{37} 8$

$2^4 \equiv_{37} 16$ $2^5 \equiv_{37} 32$ $2^6 \equiv_{37} 27$ ~~$2^9 \equiv_{37} 27$~~

$2^7 \equiv_{37} 17.$

Then compute $g^{-n} = 2^{-7} \equiv_{37} 2^{29} \equiv_{37} 24$.

list of giantsteps,

$h \cdot g^0 \equiv_{37} 3 \cdot g^0 \equiv_{37} 3$ $\quad 3 \cdot g^{-7} \equiv_{37} 35$

$3 \cdot 2^{-7} = 24$

$3 \cdot 2^{-7 \cdot 2} \equiv_{37} 26$

$3 \cdot 2^{-7 \cdot 3} \equiv_{37} 32$

$3 \cdot 2^{-7 \cdot 4} \equiv_{37} 28$

$3 \cdot 2^{-7 \cdot 5} \equiv_{37} 2$

$3 \cdot 2^{-7 \cdot 6} \equiv_{37} 33$

$3 \cdot 2^{-7 \cdot 7} \equiv_{37} 15$

$2^{-7 \cdot 4} = 2^{-28}$
$\Rightarrow 2^8 \bmod 37$
$\Rightarrow 34$

$2^{-7 \cdot 5} = 2^{-35}$
$\Rightarrow 2^1 \bmod 37$
$\Rightarrow 2$

$2^{-7 \cdot 2}$
$2^{-14} \equiv 2^{22} \bmod 37$
$\Rightarrow 21$
$21 \cdot 63 \bmod 37$
$2^{-21} \Rightarrow 2^{15} \bmod 37$
$\Rightarrow 69$

$2^{-7 \cdot 6} = 2^{-42}$
$2^{-49} = 2^{23} \bmod 37$
$= 5$
$\Rightarrow 2^{30} \bmod 37$
$= 11$

Matching pair

$2^s \equiv_{37} h \cdot 2^{-7 \cdot 3} = h \cdot 2^{-21}$

$h = 2^{26}$ $\quad \Leftarrow$ $\log_2(3) \bmod 37 = 26$

Exercise 5.5 for $N = 37$ and $g = 2$ use pohlig-hellman algo. to compute $\log_2(19)$ modulo 37. compute x_i's directly by computing sufficiently many powers of g_i.

$\Rightarrow n = 37, \quad g = 2 \quad \varphi(37) = 36 \quad 2^2 \cdot 3^2$

$2^{18} \equiv_{37} 36$
$2^{12} \equiv_{37} 26$
$12 \mid 36$

$N_1 = \frac{36}{2^2} = 9 \quad g_1 = 2^9 \equiv_{37} 31 \quad h_1 = 19^9 \equiv_{37} 6 \quad \log_{31}(6) = x_1$

$N_2 = 4 \quad g_2 = 2^4 \equiv_{37} 16 \quad h_2 = 19^4 \equiv_{37} 7 \quad \log_{16}(7) = x_2$

$h_i = g_1^{(x_i)}$

Let's compute power of 31 & 16 until we get 6,

$31^0 \equiv_N 1 \quad 31^1 \equiv_{37} 31 \quad 31^2 \equiv_{37} 36 \quad 31^3 \equiv_{37} 6$ ←

compute powers of 16 until we get 7;

$h_2 = g_2^{(x_2)}$

$16^0 \equiv_{37} 1$ $16^1 \equiv_{37} 16$ $16^2 \equiv_{37} 34$ $16^3 \equiv_{37} 26$

$16^4 \equiv_{37} 9$ $16^5 \equiv_{37} 33$ $16^6 \equiv_{37} 10$ $16^7 \equiv_{37} 12$

$(16)^8 \equiv_{37} 7$ ✓

Hence, $x_1 = 3$ and $x_2 = 8$

$\Rightarrow 3$ $\Rightarrow 8$

using CRT,

$X \equiv_4 3$

$X \equiv_9 8$

$\Rightarrow x = 35$

$x \equiv 6 \bmod n_1$ $x_1 \equiv 3 \bmod 4$

$x \equiv 6_2 \bmod n_2$ $x_2 \equiv 8 \bmod 9$

$N_i = \frac{N}{n_i}$ $N = 4 \cdot 9$

$= 36$

$n_1 = 4$

$n_2 = 9$

$9x_1 \equiv 1 \bmod 4$

$x_1 \equiv 1 \bmod 4$

$4x_2 \equiv 1 \bmod 9$

$x_2 \equiv 7 \bmod 9$

b_i	N_i	x_i	$b_i N_i x_i$
3	9	1	27
8	4	7	224

$\therefore x = (27 + 224) \bmod 36$

$= 251$

$251 \bmod 36$

$\Rightarrow 35$ //

Exercise 5.6

For $N = 43$ & $g = 5$ compute $\lg$, choose $B = 3$, compute B-smooth powers $g^i \bmod 43$ for $i = 1 \ldots 15$ & use them to compute $\log_5(2)$ & $\log_5(3)$.

$\Rightarrow n = 43$ $g = 5$ $\lg$ choose $B = 3$.

$\phi(43) = 42$.

$= 6 \times 7$

$\Rightarrow 2^1 \times 7 \times 3$

$g^i \bmod 43$:

$\Rightarrow g^{5^{20}} \bmod 6$

$5^1 \bmod 43 = 5$

$5^2 \bmod 43 = 5^2$

$5^3 \bmod 43 = 3 \cdot 13$

$5^4 \bmod 43 = 23$

$5^5 \bmod 43 = 29$

$5^6 \bmod 43 = 2^2 \cdot 2^2$ ✓

$5^7 \bmod 43 = 37$

$5^8 \bmod 43 = 13$

$5^9 \bmod 43 = 22 = 2 \times 11$

$5^{10} \bmod 43 = 2^3 \times 3^1$ ✓

$5^{11} \bmod 43 = 2 \times 17^1$

$5^{12} \bmod 43 = 41$

$5^{13} \bmod 43 = 33 \Rightarrow 11 \times 3$

$5^{14} \bmod 43 = 36 = 2^2 \times 3^2$ ✓

$5^{15} \bmod 43 = 8 = 2^3$ ✓

$|3| = 42$

$5^{21} \equiv_{43} 42$

$5^7 \equiv_{43} 16$

$5^{14} \equiv_{43} 36$

$5^6 \bmod 43 = 2^2 \cdot 2^2 \Rightarrow 6 \equiv_{42} 4 \log_g(2) \Rightarrow 6 \equiv 4 \log_5(2)$ - (1)

$5^{10} \bmod 43 = 2^3 \times 3^1 \Rightarrow 10 \equiv_{42} 3\log_g(2) + \log_g(3) \Rightarrow 10 \equiv 3\log_5(2) + \log_5(3)$ - (2)

$5^{14} \bmod 43 = 2^2 \times 3^2 \Rightarrow 14 \equiv_{42} 2\log_g(2) + 2\log_g(3) \Rightarrow 14 \equiv 2\log_5(2) + 2\log_5(3)$ - (3)

$5^{15} \bmod 43 = 2^3 \cdot \Rightarrow 15 \equiv_{42} 3\log_5(2)$ - (4)

now (1) - (4)

we get

$(6 - 15) \equiv_{42} \log_5(2)$

$-9 \equiv_{42} \log_5(2) \Rightarrow 33 \equiv_{42} \log_5(2)$

sub $\log_5(2)$ value in (2) we get

$10 \equiv_{42} 3 \cdot 33 + \log_5(3)$

$10 - 99 \equiv_{42} \log_5(3) \Rightarrow -89 \equiv_{42} \log_5(3)$

$37 \equiv_{42} \log_5(3)$

$\therefore \boxed{\log_5(2) = 33}$ & $\boxed{\log_5(3) = 37}$

Exercise 5.1. which of the following are rings? Explain.

(1) $(\mathbb{Z}, +, \cdot)$

(2) $(\mathbb{Z}_n, +, \cdot)$

(3) $(U_n, +, \cdot)$

(4) $(N, +, \cdot)$

(5) $\{a + b\sqrt{5} \mid a, b \in \mathbb{Z}\}$ with standard addition & multiplication.

(6) The set of all real-valued functions $\mathbb{R}^{\mathbb{R}} = \{f : \mathbb{R} \to \mathbb{R}\}$ with $+, \cdot$ defined as follows:

$(f+g)(x) = f(x) + g(x)$

$(f \cdot g)(x) = f(x) \cdot g(x)$

(2) $(\mathbb{Z}_n, +, \cdot)$

since $\mathbb{Z}_n$ consists of natural nos & $x \neq 0$

$|13| = 4/7$

(1) $(Z, +, .)$ to be true.

(R1) $a+e=e+a=a$ $e=0$ exists.

(R2) $(Z, .)$ is associative as 1 exists.

(R3) since $(a+b)c = ac+bc$ & $c(a+b) = ca+cb$

so $(Z, +, .)$ is ring.

---

(2) $(Z_n, +, .)$

(R1) $a+b=c=m \in Z_n$ is a abelian group

(R2) multiplicative is associative $(a.b).c = a.(b.c)$.

(R3) $(a+b)c = ac+bc$ & $c(a+b) = ca+cb$ for all $a, b, c \in Z_n$

since it satisfies all 3 condition,

$\therefore$ it is a ring.

---

(3) $(U_n, +, .)$

since U_n consists of all elements mod n, $e=0$ doesnot exist.

So, $(U_n, +, .)$ is not ring.

---

(4) $(N, +, .)$

N consists of all natural no.s but, no $e=0$ exists

so $(N, +, .)$ is not ring.

(5) $(a+b\sqrt{5} \mid a,b \in Z, +, \cdot)$

$(a+b\sqrt{5}) \cdot (c+d\sqrt{5}) = ac + 5bd + \sqrt{5}(ad+bc)$

since $e=0$ exists, multiplicative is associative with $1a$ exists

$((a+b\sqrt{5}) \cdot c + d) \cdot c + b\sqrt{5} = (a+b\sqrt{5})c = ac + b\sqrt{5}c$

$\therefore \{a+b\sqrt{5} + a,b \in Z\}$ is ring.

---

(6) $(f+g)(x) = f(x) + g(x) - (i)$

$(f \cdot g)(x) = f(x) \cdot g(x)$

since, its set of R valued function bounded by (i) & (ii); it also extends the properties of real no ie, for any functn $(p+q)(x)$.

$$(f+g)(x) \cdot (p+q) = (f \cdot p)x + (f \cdot q)x + (g \cdot p)(x) + (g \cdot q)(x) =$$
$$f(x) \cdot p(x) + f(x) \cdot g(x) + g(x) \cdot p(x) + g(x) \cdot g(x)$$

Hence, this satisfies R_1 as abelian-group with $e=0$

R_2 is associative as multiplicath is associative with 1 as unity.

$p(x) \cdot (f+g)x = p(x) \cdot f(x) + f(x) \cdot g(x) = f(x) \cdot p(x) + g(x) \cdot p(x) = (f+g)(x) \cdot p(x)$

R_3 is satisfied.

Hence the set is a ring.
