Ben Lirio
I plege my honor that I have abided by the Stevens Honor System.

5 Homework

5.1 Excercise

x	$(2^x)\%29$
0	1
1	2
2	4
3	8
4	16
5	3
6	6
7	12
8	24
9	19
10	9
11	18
12	7
13	14
14	28
15	27
16	25
17	21
18	13
19	26
20	23
21	17
22	5
23	10
24	20
25	11
26	22
27	15

$log_2(21) = 17$

5.2 Excercise

In CDH the following equations are true
$g^a \equiv A \pmod{n}$
$g^b \equiv B \pmod{n}$
$A^b \equiv B^a \equiv g^{ab} \pmod{n}$
Therefore when $n = 29$, $A = 18$, $B = 14$, the following must be true. $K \equiv 18^b \equiv$

$14^a \equiv 2^{log_2(18)log_2(14)} \pmod{n}$. According to the previous table $log_2(18) = 11$ and $log_2(14) = 13 \bmod 29$. Consequently $2^{(11)(13)} \equiv 2^{143} \bmod 29$. Using Fermat's little theorem, I notice $2^{28} \equiv 1 \bmod 29$. Which simplifies the equation to $2^3 \equiv 8 \bmod 29$. Leading to $K = \mathbf{8}$.

5.3 Excercise

Given $n = 29$, $g = 2$, $A = 17$, $c_1 = 6$, $c_2 = 10$, one way for Eve to compute the message is for her find the ephemeral key, I'll call k. This key was used to generate both c_1, and c_2 as follows, $c_1 \equiv g^k \bmod 29$ and $c_2 \equiv mA^k \bmod 29$. Therefore $k = log_2(c_1) \equiv log_2(6) \equiv 6 \bmod 29$. Using $k = 6$. Next I would like to find $(A^k)^{-1}$ in order to calculate $(A^k)^{-1}c_2 \equiv mA^k(A^k)^{-1} \equiv m \bmod 29$

5.4 Excercise

I will first create two generating functions using the given values, one I will call babystep, and the other I will call giant step. Babystep is $(e)g^i$ where e is the multiplicative identity, g is the generator and i is the current generation step. The giant step function will be h^{-in} where h is the value I am taking the log of and $n = floor(\sqrt{N}) + 1$ where N is the order.

$N = 36$
$g = 2$
$h = 3$
$e = 1$
$n = 7$
Note: one helpful precomputation is $u = g^{-n} = 24$

i,j	baby-step $(e)g^i$	giant-step $(h)g^{-jn}$
0	1	3
1	2	35
2	4	26
3	8	32
4	16	28
5	32	6

Match found on $i = 5$ and $j = 3$. $(1)2^5 \equiv (3)2^{(-3)(7)} \equiv \bmod 37$

Now if I multiply both sides by the g^{-jn} the right side will simplify to just $h = 3$ and the left side will be a power of g. $2^{26} \equiv 3 \pmod{37}$. So $m = \mathbf{3}$

5.5 Excercise

First I notice that $\phi(37) = 36 = 2^2 3^2$. So I will solve two concruencies, one mod 2^2 and the other mod 3^2. Using the the formula. For simplicity, let $c_i = p_i^{e_i}$ where p_i is a prime factor and e_i is the exponent of that factor.

$19^{\frac{\phi(37)}{c_i}} \equiv 2^{\frac{\phi(37)r}{c_i}} \pmod{37}$

Where r is bound by $0 \leq r < c_i$

$19^9 \equiv 2^{9(r)} \pmod{37}$ is valid for $r = 3$ therefore $x \equiv 3 \pmod 4$
$19^4 \equiv 2^{4(r)} \pmod{37}$ is valid for $r = 8$ therefore $x \equiv 8 \pmod 9$

Using the Chinese Remainder Theorem I can calculate x as follows: Using the first congrunce I get $x = 3 + 4y$. Now I can plug this into the second formula to obtain $3 + 4y \equiv 8 (\mathrm{mod}\ 9)$. Which can be simplified down to, $4y \equiv 5(\mathrm{mod}\ 9)$. Using Extended Euclidean algorithm, I find the multiplicative inverse of $4(\mathrm{mod}\ 9)$ is 7. So $y \equiv 35 \equiv 8(\mathrm{mod}\ 9)$. Now using the equivalance $y = 8$, I can plug it back into the relation and get $x = 3 + 4(8) = 35$. Therefore $log_2 19 = 35 \pmod{37}$

5.6 Excercise

I wasted too much time making tables in LaTeX and ran out of time.

5.7 Excercise

- $(\mathbb{Z}, +, \cdot)$
  - (R1) Associativity $(a + b) + c = a + (b + c)$, Identity $a + 0 = a$, Invertability $a - a = 0$, Commutativity, $a + b = b + a$. Since all of these are valid for $(\mathbb{Z}, +)$, (R1) passes.
  - (R2) Multiplication is associative, meaning $(a*b)*c = a*(b*c)$ which is trivialy true, and the identify $1 \in \mathbb{Z}$ is also true. (R2) passes.
  - (R3) Although not a complete proof, I will give an example of $(a + b)c = ac + bc$ given $a, b, c \in \mathbb{Z} a = 2, b = 4, c = 3$. I can compute $(2 + 4)3 = (2)(3) + (4)(3)$. Both simplify to 18. From here it is trivialy true to see that $c(a + b) = ca + cb$. (R3) passes.

  Therefore $(\mathbb{Z}, +, \cdot)$ is a ring.

- $(\mathbb{Z}_{\ltimes}, +, \cdot)$ Comparing this example with the previos one I can show $[a]_n + [b]_n = [a + b]_n$, and that $[a]_n \cdot [b]_n = [a \cdot b]_n$. Because I have this one to one map, it is valid to say that $(\mathbb{Z}_{\ltimes}, +, \cdot)$ is a ring as long as $(\mathbb{Z}, +, \cdot)$ is a ring, which has already been proved.

- $(\mathbb{U}_{\ltimes}, +, \cdot)$ Proof by counter example, in attempting to satisfy (R1) I found $2, 3 \in U_{10}$, but $2 + 3 = 5 \notin U_{10}$ since $gcd(5, 10) \neq 1$.

- $(\mathbb{N}, +, \cdot)$ Proof by counter example, in attempting to satisfy (R1) I found that $(\mathbb{N}, +)$ does not contain any addative inverses. Specifically, $42 \in \mathbb{N}$, but $-42 \notin \mathbb{N}$.

- $\{a + b\sqrt{5} | a, b \in \mathbb{Z}\}$ This case is also proved in a similar fassion to the (1), but there are a couple special cases. $\sqrt{5} + \sqrt{5} = 2\sqrt{5}$ which stays in the group. Also $\sqrt{5} \cdot \sqrt{5} = 5$ stays in the ring as well. Therefore, (5) is a ring.

- Intuitively this relation may seem like a ring, but the definition says nothing about it satisfying distributivity. So I have to go with No, it is not a ring.