Ben Lirio *I pledge my honor that I have abided by the Stevens Honor System*

# 1

After constructing a matrix with $x_1$, $x_2$, and $x_3$, I will preform the basic row and column operations.

$$\begin{bmatrix} -2 & 4 & -1 \\ 5 & 2 & 7 \\ 4 & -3 & 2 \end{bmatrix} \rightarrow \begin{bmatrix} 1 & 4 & -2 \\ -7 & 2 & 5 \\ -2 & -3 & 4 \end{bmatrix} \rightarrow \begin{bmatrix} 1 & 0 & 0 \\ -7 & 30 & -9 \\ -2 & 5 & 0 \end{bmatrix} \rightarrow \begin{bmatrix} 1 & 0 & 0 \\ 0 & 30 & -9 \\ 0 & 5 & 0 \end{bmatrix} \rightarrow \begin{bmatrix} 1 & 0 & 0 \\ 0 & 0 & -9 \\ 0 & 5 & 0 \end{bmatrix} \rightarrow \begin{bmatrix} 1 & 0 & 0 \\ 0 & 5 & 0 \\ 0 & 0 & 9 \end{bmatrix}$$

Thus $G \cong Z_1 \times Z_5 \times Z_9$

# 2

$F[x]$ is said to be a vector space when, for every $a, b \in F$ and $p(x), h(x) \in F[x]$

- $a(p(x) + h(x)) = ap(x) + ah(x)$
- $(a + b)p(x) = ap(x) + bp(x)$
- $a(bp(x)) = (ab)p(x)$
- $1p(x) = p(x)$

$$p(x) = c_0 + c_1x + c_2x^2 + ... + c_nx^n$$
$$h(x) = d_0 + d_1x + d_2x^2 + ... + d_nx^n$$

$$\begin{aligned}
a(p(x) + h(x)) & \\
&= a(c_0 + c_1x + c_2x^2 + ... + c_nx^n + d_0 + d_1x + d_2x^2 + ... + d_nx^n) \\
&= a((c_0 + d_0) + (c_1 + d_1)x + (c_2 + d_2)x^2 + ... + (c_n + d_n)x^n) \\
&= a(c_0 + d_0) + a(c_1 + d_1)x + a(c_2 + d_2)x^2 + ... + a(c_n + d_n)x^n \\
&= (ac_0 + ad_0) + (ac_1 + ad_1)x + (ac_2 + ad_2)x^2 + ... + (ac_n + ad_n)x^n \\
&= ac_0 + ac_1x + ac_2x^2 + ... + ac_nx^n + ad_0 + ad_1x + ad_2x^2 + ... + ad_nx^n \\
&= ap(x) + ah(x) \\
(a + b)p(x) & \\
&= (a + b)(c_0 + c_1x + c_2x^2 + ... + c_nx^n) \\
&= (a + b)c_0 + (a + b)c_1x + (a + b)c_2x^2 + ... + (a + b)c_nx^n) \\
&= ac_0 + ac_1x + ac_2x^2 + ... + ac_nx^n + bc_0 + bc_1x + bc_2x^2 + ... + bc_nx^n \\
&= ap(x) + bp(x) \\
a(bp(x)) & \\
&= a(b(c_0 + c_1x + c_2x^2 + ... + c_nx^n)) \\
&= a(bc_0 + bc_1x + bc_2x^2 + ... + bc_nx^n) \\
&= abc_0 + abc_1x + abc_2x^2 + ... + abc_nx^n \\
&= ab(c_0 + c_1x + c_2x^2 + ... + c_nx^n) \\
&= (ab)p(x) \\
1p(x) & \\
&= 1(c_0 + c_1x + c_2x^2 + ... + c_nx^n) \\
&= 1c_0 + 1c_1x + 1c_2x^2 + ... + 1c_nx^n \\
&= c_0 + c_1x + c_2x^2 + ... + c_nx^n \\
&= p(x)
\end{aligned}$$

## 3

### 3.1

$K$ is an ideal in $F$ when, for all $h'(x) \in K$, and for all $a(x) \in F[x]$,
then $a(x)h'(x) \in K$,

From the definition that $K = I \cap J$, every $h'(x) \in K$ satisfies

$$\begin{aligned} h'(x) &\in I \\ h'(x) &\in J \end{aligned} \tag{1}$$

Therefore, since $I$, and $J$ are both ideals in $F[x]$. For all $a(x) \in F[x]$

$$\begin{aligned} f'(x) \in I &\implies a(x)f'(x) \in I \\ g'(x) \in J &\implies a(x)g'(x) \in J \end{aligned} \tag{2}$$

Then, using both (1) and (2), for all $h'(x) \in K$, and $a(x) \in F[x]$

$$a(x)h'(x) \in I$$
$$a(x)h'(x) \in J$$

Therefore, using $K = I \cap J$,

$$a(x)h'(x) \in K$$

### 3.2

Given

$$h(x) \in K$$

It is valid to claim,

$$h(x) \in I \cap J$$
$$h(x) \in I$$
$$h(x) \in J$$

Therefore, when $I = \langle f(x) \rangle$, every element $f'(x) \in I$ satisfies

$$f'(x) = a(x)f(x)$$

for some $a(x) \in F[x]$ (the same is true for $g(x)$

Then, for some $a(x), b(x) \in F[x]$

$$h(x) = a(x)f(x)$$
$$h(x) = b(x)g(x)$$

Which implies $f(x)$ and $h(x)$ both divide $h(x)$
Another way of saying this is, $h(x)$ is a common multiple of $f(x)$ and $g(x)$

### 3.3

Proof by contradiction. Assume there exists some common multiple of $f(x)$ and $g(x)$ named $a(x)$ such that

$$h(x) \nmid a(x)$$

Because $a(x)$ is a common multiple, for some $b(x), c(x) \in F[x]$

$$b(x)f(x) = a(x)$$
$$c(x)g(x) = a(x)$$

Then, since every ideal of $F[x]$ is principle and $\langle f(x) \rangle = I$, and $\langle g(x) \rangle = J$.

$$a(x) \in I$$
$$a(x) \in J$$

Using the definitition $K = I \cap J$ and $\langle h(x) \rangle = K$

$$a(x) \in K \implies h(x) | a(x)$$

This is again using the fact that every ideal in $F[x]$ is principle.

Comparing this the the assumption of $h(x) \not| a(x)$ we see there is a contradtion.

# 4

## 4.1

If $x^3 + x^2 + 2x + 1 \in \mathbb{Z}_3[x]$ irreducible, then $E = \mathbb{Z}_3[x]/\langle f(x) \rangle$ is a field.

We can see $f(x) = x^3 + x^2 + 2x + 1 \in \mathbb{Z}_3[x]$ is irreducible by testing

$$f(0) = 0 + 0 + 0 + 1 \equiv_3 1 \neq 0$$
$$f(1) = 1 + 1 + 2 + 1 \equiv_3 2 \neq 0$$
$$f(2) = 8 + 4 + 4 + 1 \equiv_3 2 \neq 0$$

Becuase $f(x)$ does not contain any zeros in $\mathbb{Z}_3$ it is a field.

## 4.2

$$\chi(E) = 3$$
$$|E| = 3^3 = 27$$

## 4.3

If $-x$ is primitive, then $(-x)^n \bmod x^3 + x^2 + 2x + 1 \neq 1$ for all natural numbers $n < 3^3 - 1$

In particular I only have to check the values 2 and 13 becuase PFF(26) $= 2 \cdot 13$ and $\frac{26}{13} = 2$, $\frac{26}{2} = 13$.

Using WolframAlpha PolynomialMod$[(-x)^{13}, x^3 + x^2 + 2x + 1]$

$$(-x)^2 \bmod x^3 + x^2 + 2x + 1 \equiv x^2$$
$$(-x)^{13} \bmod x^3 + x^2 + 2x + 1 \equiv 1$$

Therefore, the order of $(-x)$ is 13.
Hence, $(-x)$ is not primitive.

### 4.4

The inverse of $(x+1) \in E$ is an element $a(x)$ such that

$$(x+1) \cdot a(x) \equiv 1 \text{ mod } x^3 + x^2 + 2x + 1$$

And, since I know that $(x+1)^{26} \equiv 1 \text{ mod } x^3 + x^2 + 2x + 1$ then,

$$(x+1) \cdot (x+1)^{25} \equiv 1 \text{ mod } x^3 + x^2 + 2x + 1$$

Using WolframAlpha PolynomialMod$[(x+1)^{25}, x^3 + x^2 + 2x + 1]$

$$(x+1)^{-1} \equiv (x^2 + 2) \text{ mod } x^3 + x^2 + 2x + 1$$

Technically $|(x+1)| = 13$ so I only have to calculate $(x+1)^{12}$, but to be more general I kept $(x+1)^{25}$ (And becuase I have WolframAlpha).

## 5

Given the field $E = \mathbb{Z}_3[x]/\langle x^3 + x^2 + 2x + 1\rangle$, $g = x \in \mathbb{Z}_3[x]$, and $h = x^2 + 2x + 2 \in \mathbb{Z}_3[x]$ I will compute $log_g(h) \in E$ using the **Pohlig-Hellman algorithm**.

Because the order of $|x| = 26$ in $E$, and the factors of 26 are 2 and 13, I will need two $N_i$'s.

$$N_1 = 26/2 = 13$$
$$N_2 = 26/13 = 2$$

Next, I will use WolframAlpha to calculate $g_i$'s.

$$g_1 = x^{13} \equiv 2 \text{ mod } x^3 + x^2 + 2x + 1$$
$$g_2 = x^2 \equiv x^2 \text{ mod } x^3 + x^2 + 2x + 1$$

Similarly, I will compute $h_i$'s.

$$h_1 = (x^2 + 2x + 2)^{13} \equiv 2 \text{ mod } x^3 + x^2 + 2x + 1$$
$$h_2 = (x^2 + 2x + 2)^2 \equiv (x+1) \text{ mod } x^3 + x^2 + 2x + 1$$

Then through simple iteration with WolframAlpha, I get.

$$log_2(2) = 1 = x_1$$
$$log_{x^2}(x+1) = 4 = x_2$$

Making sure to keep my primes in the same order 2 then 13, I create the following congruence

$$\begin{cases} x \equiv_2 1 \\ x \equiv_{13} 4 \end{cases}$$

Then a simple Chinese Remainder Algorithm

$$\begin{aligned} x &\equiv_2 1 \\ x &= 2y + 1 \\ 2y + 1 &\equiv_{13} 4 \\ 2y &\equiv_{13} 3 \\ y &\equiv_{13} 8 \\ x &= 2 \cdot 8 + 1 \\ x &= 17 \end{aligned}$$

Therefore, $x^{17} \equiv x^2 + 2x + 2 \text{ mod } x^3 + x^2 + 2x + 1$

In $\mathbb{Z}_3[x]/\langle x^3 + x^2 + 2x + 1\rangle$, $log_x(x^2 + 2x + 2) = 17$

# 6

## 6.1

Given polynomials $f(x) = 2x^3 + 6x^2 + 5x + 1$ and $g(x) = 3x^4 + x^3 + 3x^2 + x + 3$ both in $\mathbb{Z}_7[x]$, I will use the Extended Euclidean Algorithm to find $\gcd\big(g(x), f(x)\big)$

$$g(x) = f(x) \cdot (5x + 3) + (2x^2 + 2x) \implies \gcd\big(g(x), f(x)\big) = \gcd\big(f(x), (2x^2 + 2x)\big)$$

$$f(x) = (2x^2 + 2x) \cdot (x + 2) + (x + 1) \implies \gcd\big(f(x), (2x^2 + 2x)\big) = \gcd\big((2x^2 + 2x), (x + 1)\big)$$

$$(2x^2 + 2x) = (x + 1) \cdot (2x) + 0 \implies \gcd\big((2x^2 + 2x), (x + 1)\big) = \gcd\big((x + 1), 0\big) = (x + 1)$$

Therefore $\gcd\big(f(x), g(x)\big) = (x + 1)$

## 6.2

Here, I will compute $\alpha(x), \beta(x) \in \mathbb{Z}_7[x]$, such that $\gcd\big(f(x), g(x)\big) = \alpha(x)f(x) + \beta(x)g(x)$.

$$\begin{aligned}
(x + 1) &= f(x) - (2x^2 + 2x) \cdot (x + 2) \\
(2x^2 + 2x) &= g(x) - f(x) \cdot (5x + 3) \\
(x + 1) &= f(x) - \big(g(x) - f(x) \cdot (5x + 3)\big) \cdot (x + 2) \\
(x + 1) &= f(x) \cdot (1 + (5x + 3) \cdot (x + 2)) - g(x) \cdot (x + 2) \\
(x + 1) &= f(x) \cdot (5x^2 + 6x) + g(x) \cdot -(x + 2) \\
(x + 1) &= f(x) \cdot (5x^2 + 6x) + g(x) \cdot (6x + 5)
\end{aligned}$$

Hence, $\alpha(x) = (5x^2 + 6x)$ and $\beta(x) = (6x + 5)$

# 7

## 7.1

Given $f(x) = x^3 + 1 \in \mathbb{Z}_2[x]$, the multiplication table of the quotient ring $E = \mathbb{Z}_2[x]/\langle f(x)\rangle$ is

| | $0$ | $1$ | $x$ | $x+1$ | $x^2$ | $x^2+1$ | $x^2+x$ | $x^2+x+1$ |
|---|---|---|---|---|---|---|---|---|
| $0$ | $0$ | $0$ | $0$ | $0$ | $0$ | $0$ | $0$ | $0$ |
| $1$ | $0$ | $1$ | $x$ | $x+1$ | $x^2$ | $x^2+1$ | $x^2+x$ | $x^2+x+1$ |
| $x$ | $0$ | $x$ | $x^2$ | $x^2+x$ | $1$ | $x+1$ | $x^2+1$ | $x^2+x+1$ |
| $x+1$ | $0$ | $x+1$ | $x^2+x$ | $x^2+1$ | $x^2+1$ | $x^2+x$ | $x^2+1$ | $0$ |
| $x^2$ | $0$ | $x^2$ | $1$ | $x^2+1$ | $x$ | $x^2+x$ | $x+1$ | $x^2+x+1$ |
| $x^2+1$ | $0$ | $x^2+1$ | $x+1$ | $x^2+x$ | $x^2+x$ | $x+1$ | $x^2+1$ | $0$ |
| $x^2+x$ | $0$ | $x^2+x$ | $x^2+1$ | $x+1$ | $x+1$ | $x^2+1$ | $x^2+x$ | $0$ |
| $x^2+x+1$ | $0$ | $x^2+x+1$ | $x^2+x+1$ | $0$ | $x^2+x+1$ | $0$ | $0$ | $x^2+x+1$ |

## 7.2

The zero divisors of $E$ are

$$\begin{aligned}
(x + 1) \cdot (x^2 + x + 1) \equiv 0 &\implies (x + 1) \text{ is a zero divisor} \\
(x^2 + 1) \cdot (x^2 + x + 1) \equiv 0 &\implies (x^2 + 1) \text{ is a zero divisor} \\
(x^2 + x) \cdot (x^2 + x + 1) \equiv 0 &\implies (x^2 + x) \text{ is a zero divisor} \\
(x^2 + x + 1) \cdot (x + 1) \equiv 0 &\implies (x^2 + x + 1) \text{ is a zero divisor}
\end{aligned}$$

### 7.3

The set of units $U$ in $E$ are

$$\begin{aligned}(1)\cdot(1) \equiv 1 &\implies (1) \in U\\ (x)\cdot(x^2) \equiv 1 &\implies (x) \in U\\ (x^2)\cdot(x) \equiv 1 &\implies (x^2) \in U\end{aligned}$$

### 7.4

The unit $U$ in $E$ are closed under multiplication

| | $1$ | $x$ | $x^2$ |
|---|---|---|---|
| $1$ | $1$ | $x$ | $x^2$ |
| $x$ | $x$ | $x^2$ | $1$ |
| $x^2$ | $x^2$ | $1$ | $x$ |

### 7.5

The set $U$ is a group under $\cdot$ because it satisfies

**Associativity**. $a(bc) = (ab)c$ for all $a, b, c \in E$.

**Identity**. The identity $e = 1$ in $U$.

**Inverses**. The set $U$ is defined as the elements in $E$ with an inverse.

### 7.6

The primitive elements in the group $U$ are elements that generate $U$

$$\begin{aligned}(x) &= (x)\\ (x)^2 &= (x^2)\\ (x)^3 &= (1)\end{aligned}$$

$$\begin{aligned}(x^2) &= (x^2)\\ (x^2)^2 &= (x)\\ (x^2)^3 &= (1)\end{aligned}$$

$U$ contains 2 primitive elements.

## 8

To find the dishonest participant, I will compute the secret with two keys at a time until I have enough information

First, with $(12, 2)$ and $(3, 14)$

$$\begin{aligned}l_1(x) &= \frac{x-14}{2-14} = 7(x-14) = 7x+4\\ l_2(x) &= \frac{x-2}{14-2} = 10(x-2) = 10x+14\end{aligned}$$

$$12\cdot(7x+4) + 3\cdot(10x+14) = 12x+5$$

Using share #1, #2, the secret is 5.

Then, with $(12, 2)$ and $(9, 11)$

$$l_1(x) = \frac{x - 11}{2 - 11} = 15(x - 11) = 15x + 5$$
$$l_2(x) = \frac{x - 2}{11 - 2} = 2(x - 2) = 2x + 13$$

$$12 \cdot (15x + 5) + 9 \cdot (2x + 13) = 11x + 7$$

Using share #1, #3, the secret is 7.

Now I know that either #1, #2, or #3 is a bad share.
Therefore, I know #4 is correct

Using $(3, 14)$ and $(7, 12)$

$$l_1(x) = \frac{x - 12}{14 - 12} = 9(x - 12) = 9x + 11$$
$$l_2(x) = \frac{x - 14}{12 - 14} = 8(x - 14) = 8x + 7$$

$$3 \cdot (9x + 11) + 7 \cdot (8x + 7) = 15x + 14$$

Using #4 and #2 I get 14 as my secret

If #4 is correct and none of my answers match, that must mean #1 is dishonest which makes 14 my secret.

To verify I will also check #2 and #3
With $(3, 14)$ and $(9, 11)$ I get

$$l_1(x) = \frac{x - 11}{14 - 11} = 6(x - 11) = 6x + 2$$
$$l_2(x) = \frac{x - 14}{11 - 14} = 11(x - 14) = 11x + 16$$

$$3 \cdot (6x + 2) + 9 \cdot (11x + 16) = 15x + 14$$

The secret of 14 is verified.

# 9

## 9.1

The elliptic curve $y^2 = x^3 + 2x + 6$ is not singular because

$$4 \cdot 2^3 + 27 \cdot 6^2 \neq 0$$

### 9.2

To find the order of $(1,3) \in \mathcal{E}$ can be calculated by taking the multiples of $(1,3)$

$$
\begin{aligned}
1 \cdot (1,3) &= (1,3) \\
2 \cdot (1,3) &= (7,5) \\
3 \cdot (1,3) &= (8,12) \\
4 \cdot (1,3) &= (3,0) \\
5 \cdot (1,3) &= (8,1) \\
6 \cdot (1,3) &= (7,8) \\
7 \cdot (1,3) &= (1,10) \\
8 \cdot (1,3) &= \mathcal{O}
\end{aligned}
$$

Hence, $|(1,3)| = 8$

### 9.3

$\mathcal{E}$ is cyclic over $\mathbb{Z}_{13}$ if and only if $\gcd\big(|\mathcal{E}|, 13-1\big) = 1$

$$\gcd\big(16, 12\big) \neq 1$$

Hence, $\mathcal{E}$ is not cyclic.

To demonstrate this, here is the order of each element

$$
\begin{aligned}
|(1,10)| &= 8 \\
|(3,0)| &= 2 \\
|(4,0)| &= 2 \\
|(6,0)| &= 2 \\
|(7,5)| &= 4 \\
|(7,8)| &= 4 \\
|(8,1)| &= 6 \\
|(8,12)| &= 8 \\
|(9,5)| &= 8 \\
|(9,8)| &= 8 \\
|(10,5)| &= 8 \\
|(10,8)| &= 8 \\
|(12,4)| &= 4 \\
|(12,9)| &= 4
\end{aligned}
$$

For all $(x,y) \in \mathcal{E}$, $\langle (x,y) \rangle \neq \mathcal{E}$.

### 9.4

Given $g = (1,3)$, $a \cdot g = (8,12)$, and $b \cdot g = (7,8)$, I will compute $K = a \cdot B = b \cdot A$.

Using the answer from part $(b)$, I can compute the $\mathrm{DLOG}(g, a \cdot g)$, and $\mathrm{DLOG}(g, b \cdot g)$.

$$
\begin{aligned}
\mathrm{DLOG}\big((1,3),(8,12)\big) &= 3 \\
\mathrm{DLOG}\big((1,3),(7,8)\big) &= 6
\end{aligned}
$$

By finding the discrete log of both Alice and Bobs public key, I can find thier shared key as follows

$$3 \cdot (7, 8) = 6 \cdot (8, 12) = (7, 5)$$

Alice and Bobs shared key is $(7, 5)$

## 10

Given elliptic curve $\mathcal{E}$ defined by the equation $y^2 = x^3 + 3x + 4$ over $\mathbb{Z}_{11}$ and the following information

$$\begin{aligned} g &= (5, 1) \\ A &= (9, 10) \\ c1 &= (7, 7) \\ c2 &= (9, 1) \end{aligned}$$

I can compute $m$ with the equation $m = c2 - a \cdot c1$.

First, using the multiples of $g$ shown below, I can find $a$ in the equation $A = a \cdot g$

$$(9, 10) = 5 \cdot (5, 1)$$

Because I have the multiples of $g$ computed, I well find $j$ in the equation $c1 = j \cdot g$ so that I can compute $a \cdot c1 = (aj) \cdot g$.

$$(7, 7) = 3 \cdot (5, 1)$$

Finally, $m = c2 - a \cdot c1$ can be computed as follows

$$\begin{aligned} m &= c2 - a \cdot c1 \\ &= c2 - (aj) \cdot g \\ &= (9, 1) - (3 \cdot 5) \cdot (5, 1) \\ &= (9, 1) - (15) \cdot (5, 1) \\ &= (9, 1) - (5, 1) \\ &= 9 \cdot (5, 1) + -1 \cdot (5, 1) \\ &= 8 \cdot (5, 1) \\ &= (0, 9) \end{aligned}$$

$m = (0, 9)$

multiples of $g$

$$\begin{aligned} g &= (5, 1) \\ 2 \cdot g &= (4, 5) \\ 3 \cdot g &= (7, 7) \\ 4 \cdot g &= (8, 1) \\ 5 \cdot g &= (9, 10) \\ 6 \cdot g &= (0, 2) \\ 7 \cdot g &= (10, 0) \\ 8 \cdot g &= (0, 9) \\ 9 \cdot g &= (9, 1) \\ 10 \cdot g &= (8, 10) \\ 11 \cdot g &= (7, 4) \\ 12 \cdot g &= (4, 6) \\ 13 \cdot g &= (5, 10) \\ 14 \cdot g &= \mathcal{O} \end{aligned}$$

Here are the first couple computations of $g$, but I wrote a program to do the rest
$2 \cdot g$

$$(x_1, y_1) = (x_2, y_2) = (5, 1)$$

$x_1 = x_2$ and $y_1 = y_2$ means I will use Case II

$$\begin{aligned}\lambda &= \frac{3 \cdot (5)^2 + 3}{2 \cdot 1} \\ &= \frac{3 \cdot 3 + 3}{2} \\ &= \frac{1}{2} \\ &= 6 \cdot 1 \\ &= 6\end{aligned}$$

Next, I will find $x_3 = \lambda^2 - x_1 - x_2$

$$\begin{aligned}x_3 &= 6^2 - 5 - 5 \\ &= 3 - 10 \\ &= 3 + 1 \\ &= 4\end{aligned}$$

And for $y_3 = \lambda \cdot (x_1 - x_3) - y_1$

$$\begin{aligned}y_3 &= 6(5 - 4) - 1 \\ &= 6 - 1 \\ &= 5\end{aligned}$$

$2 \cdot g = (4, 5)$
Then I will find $3 \cdot g$ by computing $g + 2 \cdot g$

$$(x_1, y_1) = (4, 5)$$
$$(x_2, y_2) = (5, 1)$$

$x_1 \neq x_2$ means I will use Case I

$$\begin{aligned}\lambda &= \frac{1 - 5}{5 - 4} \\ &= \frac{7}{1} \\ &= 7\end{aligned}$$

Next, I will find $x_3 = \lambda^2 - x_1 - x_2$

$$\begin{aligned}x_3 &= 7^2 - 4 - 5 \\ &= 5 - 9 \\ &= 5 + 2 \\ &= 7\end{aligned}$$

And for $y_3 = \lambda \cdot (x_1 - x_3) - y_1$

$$\begin{aligned}y_3 &= 7(4 - 7) - 5 \\ &= 12 - 5 \\ &= 7\end{aligned}$$

$3 \cdot g = (7, 7)$
Code to generate multiples of $g$ written in **golang**

```
package main

import (
"math"
"fmt"
)

var m int = 11
var a int = 3
var b int = 4

func mod(v int) int {
out := int(math.Mod(float64(v), float64(m)))
if out < 0 {
out += m
}
return out
}

func inv(v int) int {
for i := 0; i < m; i++ {
if mod(i*v) == 1 {
return i
}
}
return -1
}
func pow(b int, p int) int {
out := 1
for i := 0; i < p; i++ {
out *= b
}
return out
}

func add(x1 int, y1 int, x2 int, y2 int) (bool, int, int) {
if (x1 == x2) && (y2 != y1) {
return true, 0, 0
}
if (x1 == x2) && (y1 == 0) && (y2 == 0) {
return true, 0, 0
}
var lambda int
if (x1 == x2) {
top := mod(3*pow(x1,2) + a)
bottom := mod(2*y1)
lambda = mod(top*inv(bottom))
} else {
top := mod(y2 - y1)
bottom := mod(x2 - x1)
lambda = mod(top*inv(bottom))
}
x3 := mod(pow(lambda, 2)-x1-x2)
y3 := mod(lambda*(x1-x3) - y1)
```

```
return false, x3, y3
}

func main() {
gX := 7
gY := 7
curX := 7
curY := 7
var check bool
for {
check, curX, curY = add(curX, curY, gX, gY)
if check {
break
}
fmt.Println(curX, curY)
}
}
```