Mathematical Cryptography

MATH 490

Start

August 26, 2024

Author

Paul Beggs
BeggsPA@Hendrix.edu

Instructor

Prof. Allie Ray, Ph.D.

End

December 2, 2024

CHAPTER 6

ELLIPTIC CURVES AND CRYPTOGRAPHY

6.1 Elliptic Curves

Definition Elliptic Curve:

An *elliptic curve* E is the set of solutions to an equation of the form $y^2 = x^3 + ax + b$, together with a point at infinity $\mathcal{O}$, and the condition that $4a^3 + 27b^2 \neq 0$. The last condition is to prevent singular points that cross. In other words, $4a^3 + 27b^2 = 0 \equiv x^3 + ax + b$ having 3 distinct roots.

Adding Two Elliptic Curve Points

We define "$\oplus$" as mapping: $E \times E \to E$. From this, we get $P \oplus Q = R$.

Define a line through $P \oplus Q$. This line will intersect the curve at a third point, R. Then R' is the reflection of R over the y-axis. $P \oplus Q = R'$.

Example 6.1: Adding Two Elliptic Curve Points

Given the elliptic curve E: $y^2 = x^3 - 36x$ with $P = (-3, 9)$, $Q = (-2, 8)$. Find $P \oplus Q$.

Solution.

1. Find slope: $m = \frac{y_2 - y_1}{x_2 - x_1} = \frac{8-9}{-2-(-3)} = -1$.
2. Solve the equation of line: $y = -x + b$. Plug in P: $9 = 3 + b \implies b = 6$. Thus, $y = -x + 6$.
3. Plug y back into given formula:
$$\begin{aligned} (-x+6)^2 &= x^3 - 36x \\ x^2 - 12x + 36 &= x^3 - 36x \\ (-x^3) + x^2 + 24x + 36 &= 0 \\ x^3 - x^2 - 24x - 36 &= 0 \end{aligned}$$
4. Find the roots of the equation: $x = -3, -2, 6$. Thus, $R = (6, 0)$ and $R' = (6, 0)$. Note two important things we did here:
   - We know that two of the roots are 3 and 2 because they are given. We got the third root, -6, by solving for the cubic equation.
   - R and R' are the same value because to find R', we reflect R over the y-axis.

5. Conclude: $P \oplus Q = R' = (6, 0)$.

Theorem: Addition Law Properties

Let E be an elliptic curve. Then, the addition law on E has the following properties:

(a)	$P \oplus \mathcal{O}$	$=$	$\mathcal{O} \oplus P = P$	for all $P \in E$.	(Identity)
(b)	$P \oplus (-P)$	$=$	$(-P) \oplus P = \mathcal{O}$	for all $P \in E$.	(Inverse)
(c)	$(P \oplus Q) \oplus R$	$=$	$P \oplus (Q \oplus R)$	for all $P, Q, R \in E$.	(Associative)
(d)	$P \oplus Q$	$=$	$Q \oplus P$	for all $P, Q \in E$.	(Commutative)

In other words, the addition law makes the points of E into an Abelian group.

Proof.

1. **Identity:** True because $\mathcal{O}$ lies on all vertical lines.
2. **Inverse:** Same reason as Identity. (Also, we defined $\mathcal{O}$ as such.)
3. **Associative:** Ignoring because hard.
4. **Commutative:** Line through $P \oplus Q$ is the same as the line through $Q \oplus P$. Hence, $P \oplus Q = Q \oplus P$.

□

6.1.1 Special Cases for Adding Elliptic Curve Points

Theorem: Elliptic Curve Addition Algorithm

Let

$$E\colon y^2 = x^3 + ax + b$$

be an elliptic curve, and let P_1 and P_2 be points on E.

(a) If $P_1 = \mathcal{O}$, then $P_1 + P_2 = P_2$.

(b) Otherwise, if $P_2 = \mathcal{O}$, then $P_1 + P_2 = P_1$.

(c) Otherwise, write $P_1 = (x_1, y_1)$ and $P_2 = (x_2, y_2)$.

(d) If $x_1 = x_2$ and $y_1 = -y_2$, then $P_1 + P_2 = \mathcal{O}$.

(e) Otherwise, define λ by

$$\lambda = \begin{cases} \dfrac{y_2 - y_1}{x_2 - x_1} & \text{if } P_1 \neq P_2, \\[2ex] \dfrac{3x_1^2 + A}{2y_1} & \text{if } P_1 = P_2, \end{cases}$$

and let

$$x_3 = \lambda^2 - x_1 - x_2 \qquad \text{and} \qquad y_3 = \lambda(x_1 - x_3) - y_1.$$

Then, $P_1 + P_2 = (x_3, y_3)$.

Verbatim From Notes Today In Class

For $P = (x_1, y_1)$, $Q = (x_2, y_2)$.

1. $P = Q$: This means $x_1 = x_2$, and there is no slope because $x_2 - x_2 = 0$. Thus, this "line," is actually a point tangent to the curve. Thus, to find the slope of the line, we need to differentiate.

2. $P = \mathcal{O}$ or $Q = \mathcal{O}$: This means that the line is vertical, and the sum is the other point. In other words, $P \oplus \mathcal{O} = P$.

For the first case, consider the following example:

Example 6.2: Case 1

Solve for R' with the elliptic curve $E\colon y^2 = x^3 - 36x$.

Solution. To solve this we first need to differentiate to get the slope for our equation:

$$\begin{aligned}
y^2 &= x^3 - 36x \\
2y\frac{dy}{dx} &= 3x^2 - 36 \\
\frac{dy}{dx} &= \frac{3x^2 - 36}{2y} \\
\frac{dy}{dx} &= \frac{3(-3)^2 - 36}{2(9)} \\
\frac{dy}{dx} &= \frac{-1}{2}
\end{aligned}$$

From here, we solve $y - y_0 = m(x - x_0)$:

$$\begin{aligned}
y - 9 &= \frac{-1}{2}(x+3) \\
y &= \frac{-1}{2} + \frac{15}{2}
\end{aligned}$$

Now, we can substitute our x and y values back into the original $y^2 = x^3 + ax + b$:

$$\begin{aligned}
\left(\frac{-1}{2}x + \frac{15}{2}\right)^2 &= x^3 - 36x \\
\frac{1}{4}x^2 - \frac{15}{2}x + \frac{225}{4} &= x^3 - 36x \\
x^3 - \frac{1}{4}x^2 - \frac{57}{2}x - \frac{225}{4} &= 0 \\
(x+3)(x+3)(x - \frac{25}{4}) &= 0
\end{aligned}$$

Hence, $x = \frac{25}{4}$ and $y = \frac{-1}{2}(\frac{25}{4}) + \frac{15}{2} - \frac{35}{8}$.

Therefore, $R' = P \oplus P = (\frac{25}{4}, \frac{-35}{8})$. Note that $\frac{35}{8}$ is negative because we flipped it along the y-axis.

6.2 Elliptic Curves over Finite Fields

Example 6.3: Elliptic Addition with Modulo

Given the elliptic curve $E\colon y^2 = x^3 + 2x + 2 \pmod{17}$ with points $P = (5, 1)$ and $Q = (16, 13)$.

(a) Find $P \oplus Q$.

(b) Find $P \oplus P$.

Solution.

(a) First, we need to find lambda. Using the formula for lambda in the Elliptic Curve Addition Algorithm part (e), first condition, we have: $\lambda = \frac{12}{11}$, but remember, we are in modulo, so we need to find the modular inverse of 11. This is 14. Thus, $\lambda = 12 \cdot 14 = 15$. (Note there is a quick trick of subtracting the number by 17 to get a smaller number to work with. For example, 12 and 14 are -5 and -3, respectively. When we multiply these, we get the same answer: 15. Hence, we can use this trick to make our calculations easier.)

Use the formula for x_3 and y_3 to find the point R. For x_3:

$$\begin{aligned} x_3 &\equiv (15)^2 - 5 - 16 \\ &\equiv (-2)^2 - 5 - 16 \\ &\equiv -17 \\ &\equiv 0 \pmod{17} \end{aligned}$$

Then, for y_3:

$$\begin{aligned} y_3 &\equiv 15(5 - 0) - 1 \\ &\equiv (-2)(5) - 1 \\ &\equiv -11 \\ &\equiv 6 \pmod{17} \end{aligned}$$

This gives us the point $R = (0, 6)$.

(b) For $P \oplus P$, we have $P = (5, 1)$. Now, we use the Elliptic Curve Addition Algorithm part (e), second condition, to find lambda. We have

$$\lambda = \frac{3(5)^2 + 2}{2(1)} = 9 \cdot 2^{-1} \equiv 9 \cdot 9 \equiv 13 \pmod{17}.$$

Now, we can find x_3 and y_3:

$$\begin{aligned} x_3 &\equiv 13^2 - 5 - 5 \\ &\equiv 169 - 10 \\ &\equiv 159 \\ &\equiv 6 \pmod{17} \end{aligned}$$

For y_3:

$$\begin{aligned} y_3 &\equiv 13(5-6)-1 \\ &\equiv 13(-1)-1 \\ &\equiv -14 \\ &\equiv 3 \pmod{17} \end{aligned}$$

This gives us the point $R = (6, 3)$.

Example 6.4: Set of Points $E(\mathbb{F}_p)$

Using the same elliptic curve from the last example, $E\colon y^2 = x^3 + 2x + 2 \pmod{17}$ find the set of points $E(\mathbb{F}_{17})$.

Solution. For this problem, we need to find all the squares modulo 17. We can do this by squaring all the numbers from 0 to 16.

1. First, find all the squared values:
   - $0^2 = 0$
   - $1^2 = 1 = 16^2$
   - $2^2 = 4 = 15^2$
   - $3^2 = 9 = 14^2$
   - $4^2 = 16 = 13^2$
   - $5^2 = 8 = 12^2$
   - $6^2 = 2 = 11^2$
   - $7^2 = 15 = 10^2$
   - $8^2 = 13 = 9^2$

   Notice that the squares are symmetric about 8. This is because the curve is symmetric about the y-axis.

2. We need to find the y-values. We need to test each of the x-values in the equation $y^2 = x^3 + 2x + 2$:
   - $0^3 + 2(0) + 2 = 2$
   - $1^3 + 2(1) + 2 = 5$
   - $2^3 + 2(4) + 2 = 12$
   - $3^3 + 2(9) + 2 = 1$
   - $4 \to 6$
   - $5 \to 1$
   - $6 \to 9$
   - $7 \to 2$
   - $8 \to 3$
   - $9 \to 1$, $10 \to 2$, $11 \to 2$, $12 \to 3$, $13 \to 15$, $14 \to 3$, $15 \to 7$, $16 \to 16$.

3. Now, given a y-value, we can search for the corresponding x-value. For example, $y = 2$ corresponds to $x = 6$ and $x = 11$. We find the pairs to be:

$$\begin{aligned}
&\mathcal{O},\\
&(0,6),(0,11),\\
&(3,1),(3,16),\\
&(5,1),(5,16),\\
&(6,3),(6,14),\\
&(7,6),(7,11),\\
&(9,1),(9,16),\\
&(10,6),(10,11),\\
&(13,7),(13,10),\\
&(16,4),(16,13).
\end{aligned}$$

This yields the set of points $E(\mathbb{F}_{17})$ to be 19 points in total.

Theorem: Hasse

The following formula gives an estimate for the number of points on an elliptic curve over a finite field:

$$p+1-2\sqrt{p} \leq \#E(\mathbb{F}_p) \leq p+1+2\sqrt{p}.$$

6.3 The Elliptic Curve Discrete Logarithm Problem (ECDLP)

The Double-and-Add Algorithm

1. Write n in binary.
2. Repeatedly double the point P up to the highest multiple of 2 in binary representation of n.
3. Take points corresponding to binary expansion of n and add them together.

Example 6.5: Double-and-Add Algorithm

Use the double-and-add algorithm to compute $E\colon y^2 = x^3 + 2x + 2 \pmod{17}$ with $p = (5,1)$ and $n = 11$.

Solution.

1. Write $n = 11$ in binary: $11 = 1011$.
2. Double the point P up to the highest multiple of 2 in the binary representation of

n:

$$\begin{aligned} 1P &= (5,1) \\ 2P &= (6,3) \\ 4P &= (3,1) \\ 8P &= (13,7) \end{aligned}$$

3. Solve for $11P$:

$$\begin{aligned} 11P &= 8P + 2P + P \\ &= (13,7) + (6,3) + (5,1) \\ &= (7,11) + (5,1) \\ &= (13,10). \end{aligned}$$

This algorithm takes $\leq 2n$ "steps" to compute nP.

Ternary Expansion of n

1. Write n in binary.
2. Working from smaller powers of 2 to larger powers when you have 2 or more consecutive powers or 2, we can replace:

$$\begin{aligned} &(2^{s+5}) + 1(2^{s+t-1}) + 1(2^{s+t-2}) + \cdots + 1(2^s) \\ &= 2^{s+t} - 2^s. \end{aligned}$$

This allows us to "cancel out" middle terms of consecutive powers of 2. We take the next largest power of 2, for a string of 2s, and subtract the next smallest power of 2.

Example 6.6: Ternary Expansion

Find the ternary expansion of 11.

Solution.

1. Write 11 in binary: $11 = 1011$.
2. Replace the binary expansion with the ternary expansion:

$$\begin{aligned} 11 &= 8 + 2 + 1 \\ &= 1(8) + 1(4) + 1(2) + 1(1) \\ &= 8 + 4 + 1(\cancel{2}) - 1 \\ &= 11. \end{aligned}$$

6.4 Elliptic Curve Cryptography

6.4.1 Elliptic Curve Diffie-Hellman Key Exchange

Public parameter creation	
A trusted party chooses and publishes a large prime p, an elliptic curve E over $\mathbb{F}_p$ and a point P in $E(\mathbb{F}_p)$.	
Private Computations	
Alice	**Bob**
Chooses a secret integer n_A. Computes the point $Q_A = n_A P$	Chooses a secret integer n_B. Computes the point $Q_B = n_B P$
Public Exchange of Values	
Alice sends Q_A to Bob	
	Bob sends Q_B to Alice
Further Private Computations	
Computes the point $n_A Q_B$.	Computes the point $n_B Q_A$.
Their shared secret value is $n_A Q_B = n_A(n_B P) = n_B(n_A P) = n_B Q_A$.	

Table 6.1: Diffie-Hellman Key Exchange Using Elliptic Curves

Example 6.7: Elliptic Curve Diffie-Hellman Key Exchange

Given the elliptic curve $E\colon y^2 \equiv x^3 + x + 6 \pmod{11}$ with point $p = (5, 9)$, Alice's private key $n_A = 4$, and Bob's private key $n_B = 7$, find the shared secret key. Use this website: Elliptic Curve Calculator.

Solution. First, we need to find Q_A and Q_B. For Q_A, we have $n_A = 4$, so we need to find $4P$. Using the double-and-add algorithm, we have $n = 4 = 100$. Now, we need to solve for $2P$ and $4P$:

$$\lambda = \frac{3(5)^2 + 1}{2(9)} = \frac{76}{18} = 10 \cdot 18^{-1} \equiv -1 \cdot 7 \equiv -7 \equiv 4 \pmod{11}$$

Now we can find x_3 and y_3. First, x_3:

$$\begin{aligned} x_3 &\equiv 4^2 - 5 - 5 \\ &\equiv 16 - 10 \\ &\equiv 6 \pmod{11}. \end{aligned}$$

For y_3:

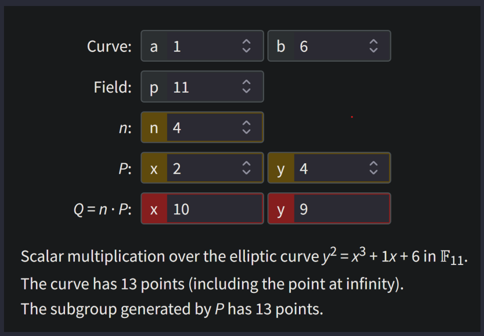
$$\begin{aligned} y_3 &\equiv 4(5-6)-9 \\ &\equiv 4(-1)-9 \\ &\equiv -4-9 \\ &\equiv 9 \pmod{11}. \end{aligned}$$

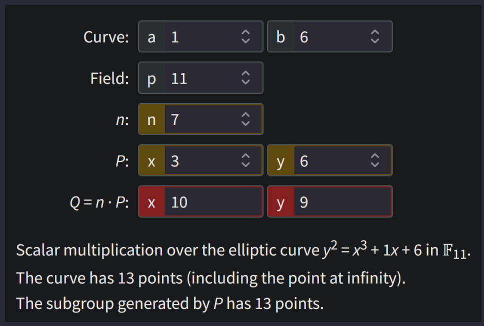
Thus, $2P = (6,9)$. Using the same process, we find that $Q_A = 2(2P) = 2(6,9) = (3,6)$.

$$\begin{aligned} 1P &= (5,9) \\ 2P &= (6,9) \\ 4P &= (3,6). \end{aligned}$$

Similarly, for $7Q_B \Rightarrow 7P = (2,4)$.

From the image below, we can see that when we take the point $n_A Q_B \Rightarrow 4 \cdot (2,4)$, we get the point $(10,9)$. Then, when we take the point $n_B Q_A \Rightarrow 7 \cdot (3,6)$, we get the point $(10,9)$. Thus, the shared secret key is $(10,9)$.





6.4.2 Elgamal Encryption Using Elliptic Curves

Public parameter creation	
A trusted party chooses and publishes a large prime p, an elliptic curve E over $\mathbb{F}_p$, and a point P in $E(\mathbb{F}_p)$.	
Key creation	
Alice	**Bob**
Choose private key n_A. Compute $Q_A = n_A P$ in $E(\mathbb{F}_p)$. Publish the public key Q_A.	
Encryption	
	Choose plaintext $M \in E(\mathbb{F}_p)$. Choose random element k. Use Alice's public key Q_A to compute $C_1 = kP \in E(\mathbb{F}_P)$ and $C_2 = M + kQ_A \in E(\mathbb{F}_P)$. Send ciphertext (C_1, C_2) to Alice.
Decryption	
Compute $C_2 - n_A C_1 \in E(\mathbb{F}_P)$. This quantity is equal to M.	

Table 6.2: Elgamal Key Creation, Encryption, and Decryption with Elliptic Curves

Example 6.8: Elgamal Encryption Using Elliptic Curves

Given the elliptic curve $E\colon y_2 \equiv x_3 + 7x + 4 \pmod{17}$ with $P = (3, 1)$, $n_A = 15$, $M = (16, 8)$, and $(K = 5)$, find Q_A, and encrypt and decrypt the message.

Solution. We find Q_A to be $(11, 16)$

$$C_1 = 5(3, 1) = (0, 15).$$

Then,

$$c_2 = (16, 8) + 5(11, 16) = (3, 1).$$

Alice can decrypt the message by computing:

$$(3, 1) \ominus 15(0, 15) = (3, 1) \ominus (2, 14) = (3, 1) \oplus (2, 3) = (16, 8).$$

(Note the subtraction is just taking $-y$.)

Exercise 5.10

Encrypt each of the following Vigenère plaintexts using the given keyword and the Vigenère tableau (Table 5.1 in book).

1. Keyword: `hamlet`

   Plaintext: `To be, or not to be, that is the question.`

Solution.

1. Hamlet is made up of 6 letters, so we repeat the keyword to match the length of the plaintext:

   `tobeor | nottobe | thatis | theque | stion`

   Then, find the row that starts with the key-letter. For instance, since `hamlet` starts with `h`, we go down to the 8^{th} row in Table 5.1. Then, we go right until we reach the column of our plaintext. So, for `t`, that would be the 20^{th} column.

   See the table below for the full encryption. Note that $\mathcal{P}, \mathcal{K}$, and $\mathcal{C}$ indicate the plaintext, keyword, and ciphertext, respectively:

$\mathcal{P}$	tobeor	nottobe	thatis	theque	stion
$\mathcal{K}$	hamlet	hamlet	hamlet	hamlet	hamlet
$\mathcal{C}$	aonpsk	uofesu	lttlxb	zttpun	lsftsg

Exercise 5.11

Decrypt each of the following Vigenère ciphertexts using the given keyword and the Vigenère tableau (Table 5.1 in book).

1. Keyword: `condiment`

   Ciphertext: `r s g h z  b m c x t  d v f s q  h n i g q  x r n b m  p d n s q  s m b t r  k u`

Solution.

1. Reversing the method from Exercise 5.10, we have:

$\mathcal{C}$	`rsghzbmcx`	`tdvfsqhni`	`gpxrnbmpd`	`nsqsmbtrk`	`u`
$\mathcal{K}$	`condiment`	`condiment`	`condiment`	`condiment`	`c`
$\mathcal{P}$	`peterpipe`	`rpickedap`	`eckofpick`	`ledpepper`	`s`

we find the decrypted ciphertext to be:

`peter piper picked a peck of pickled peppers`

Exercise 5.13

Let

$$s = \text{“I am the very model of a modern major general.”}$$
$$t = \text{“I have information vegetable, animal, and mineral.”}$$

1. Make frequency tables for s and t.
2. Compute IndCo(s) and IndCo(t).

	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z
Freq s	4	0	0	2	6	1	1	1	1	1	0	2	4	2	4	0	0	4	0	1	0	1	0	0	1	0
Freq t	8	1	0	1	4	1	1	1	5	0	0	3	3	5	2	0	0	2	0	2	0	2	0	0	0	0

Table 5.3: Frequency Distribution for s and t

Solution.

1. The frequency table for s and t is shown in Table 5.1.
2. We find the index of coincidence for s to be:

$$\begin{aligned}
\text{IndCo}(s) &= \frac{1}{n(n-1)} \sum_{i=0}^{25} F_i(F_i - 1) \\
&= \frac{1}{36(35)}(4 \cdot 3 + 2 \cdot 1 + 6 \cdot 5 + \cdots + 0 \cdot 0) \\
&= \frac{84}{1260} \\
&\approx 0.0667.
\end{aligned}$$

Then, for t, we have:

$$\begin{aligned}\text{IndCo}(t) &= \frac{1}{n(n-1)}\sum_{i=0}^{25} F_i(F_i - 1)\\ &= \frac{1}{41(40)}(8\cdot 7 + 4\cdot 3 + \cdots + 0\cdot 0)\\ &= \frac{128}{1640}\\ &\approx 0.0780.\end{aligned}$$

Exercise 5.15

1. One of the following two strings was encrypted using a simple substitution cipher, while the other is a random string of letters. the index of coincidence of each string and use the results to guess which is which.

$$s_1 = \texttt{RCZBWBFHSLPSCPILHBGZJTGBIBJGLYIJIBFHCQQFZBYFP},$$
$$s_2 = \texttt{KHQWGIZMGKPOYRKHUITDUXLXCWZOTWPAHFOHMGFEVUEJJ}.$$

	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z
Freq s_1	0	7	3	0	0	4	3	3	4	3	0	3	0	0	0	3	2	1	2	1	0	0	1	0	2	3
Freq s_2	1	0	1	1	2	2	3	4	2	2	3	1	2	0	3	2	1	1	0	2	3	1	3	2	1	2

Table 5.4: Frequency Distribution for s_1 and s_2

Solution.

1. See the table below for the frequency distribution of s_1 and s_2 in Table 5.2. We find the index of coincidence for s_1 to be:

$$\begin{aligned}\text{IndCo}(s_1) &= \frac{114}{45(44)}\\ &\approx 0.0576.\end{aligned}$$

Then, for s_2, we have:

$$\begin{aligned}\text{IndCo}(s_2) &= \frac{60}{45(44)}\\ &\approx 0.0303.\end{aligned}$$

Since the index of coincidence for s_1 is higher than that of s_2, we can guess that s_1 was encrypted using a simple substitution cipher.

Exercise 5.17

We applied a Kasiski test to the Vigenère ciphertext listed below and found that the key length is probably 5. Use Excel to find the plaintext and the key.

```
togmg gbymk kcqiv dmlxk kbyif vcuek cuuis vvxqs pwwej koqgg
phumt whlsf yovww knhhm rcqfq vvhkw psued ugrsf ctwij khvfa
thkef fwptj ggviv cgdra pgwvm osqxg hkdvt whuev kcwyj psgsn
gfwsl jsfse ooqhw tofsh aciin gfbif gabgj adwsy topml ecqzw
asgvs fwrqs fsfvq rhdrs nmvmk cbhrv kblxk gzi
```

Solution. From the problem, I knew the key size was 5. Thus, I used the IndCo keysize 5 sheet. This is my order of operations:

1. Change the Ciphertext: Capitalize letters and remove spaces.
2. Paste this into A1.
3. Confirm the IndCo value is appropriate (IndCo $= 0.064$, so it is).
4. Copy the concatenated string from C122 into first the first Excel sheet we did.
5. Find the lowest χ^2 value, so I know what value to subtract 26 by.
6. Go to rot13 and paste the string in, then rotate it by 26 minus the value we found in the previous step.
7. Record this string in the Excel sheet.
8. Repeat step 4-7 for the rest of the concatenated strings.

We end up with 5 decrypted strings. Now, we need to read them from top to bottom. To concatenate the strings, I used the following python code in Listing 5.1. Once I ran the code, I got the following plaintext:

> Radio, envisioned by its inventor as a great humanitarian contribution, was seized upon by the generals soon after its birth and impressed as an instrument of war. But radio turned over to the commander a copy of every enemy cryptogram it conveyed. Radio made cryptanalysis an end in itself.[1]

To find the key, I used the following python code in Listing 5.2. The key was found to be `CODES`.

[1] A Google search with the decrypted words led me to the plaintext in proper grammatical form without capitalization and proper spacing.

Listing 5.1: Python Code to Concatenate Strings

```python
cipher_text = [
    "REIBITATNINUWIPTNSAIRDEANMFUINEHMRYEEYRCYDDPLAIE",
    "ANOYNOGHIATTAZOHESFTTISSSEWTOEREAAORMPAOEIETYNNL",
    "DVNIVRRUTNRISENEROTSHMSATNARTDTCNCFYYTMNDOCASEIF",
    "IIETEAEMACIOSDBGAOEBAPENRTRAUOOODOEECOIVRMRNINT",
    "OSDSNSAAROBNEUYELNRINRDIUOBDRVTMEPVNRGTEAAYASDS",
]

# Number of rows and columns
num_rows = len(cipher_text)
num_cols = min(len(row) for row in cipher_text)

# Read the text column by column
decoded_text = ""
for col in range(num_cols):
    for row in range(num_rows):
        decoded_text += cipher_text[row][col]

# Print the result
print("Decoded text (column-by-column):")
print(decoded_text)
```

Listing 5.2: Python Code to Find Key

```python
# Plaintext and Ciphertext have been omitted because they would not fit in the page.
plaintext = "..."
ciphertext = "..."

# Known key length
key_length = 5

# Helper function to convert letters to alphabetical index (A=0, B=1, ..., Z=25)
def letter_to_index(letter):
    return ord(letter) - ord('A')

# Helper function to convert index back to a letter
def index_to_letter(index):
    return chr(index + ord('A'))

# Calculate the key by determining the shift for each character in the key
key = []
for i in range(key_length):
    # Compute the shift for each position in the key
    shift = (letter_to_index(ciphertext[i]) - letter_to_index(plaintext[i])) % 26
    key.append(index_to_letter(shift))

# Join the key characters into a string
key_word = ''.join(key)
print("Derived key:", key_word)
```

Exercise 6.1

Let E be the elliptic curve $E : Y^2 = X^3 - 2X + 4$ and let $P = (0, 2)$ and $Q = (3, -5)$. (You should check that P and Q are on the curve E.)

1. Compute $P \oplus Q$.
2. Compute $P \oplus P$ and $Q \oplus Q$.

Solution. We have $E\colon Y_2 = X^3 - 2X + 4$ with $P = (0, 2)$ and $Q = (3, -5)$.

1. For $P \oplus Q$, we need to find lambda:
$$\lambda = \frac{-5 - 2}{3 - 0} = -\frac{7}{3}.$$
Using λ, we can find the X-coordinate of $P \oplus Q$:
$$X_3 = \left(-\frac{7}{2}\right)^2 - 0 - 3 = \frac{22}{9},$$
and for the y-coordinate:
$$\left(-\frac{7}{3}\right)\left(0 - \frac{22}{9}\right) - 2 = \frac{100}{27}.$$
Hence, $P \oplus Q = \left(\frac{22}{9}, \frac{100}{27}\right)$.

2. For $P \oplus P$, we need to find lambda:
$$\lambda = \frac{3(0)^2 - 2}{2 \cdot 2} = -\frac{1}{2}.$$
For X_3:
$$X_3 = \left(-\frac{1}{2}\right)^2 - 0 - 0 = \frac{1}{4},$$
and for Y_3:
$$Y_3 = \left(-\frac{1}{2}\right)\left(0 - \frac{1}{4}\right) - 2 = -\frac{15}{8}.$$
Hence, $P \oplus P = \left(\frac{1}{4}, -\frac{15}{8}\right)$.

Exercise 6.2

Check that the points $P = (-1, 4)$ and $Q = (2, 5)$ are points on the elliptic curve $E : Y^2 = X^3 + 17$.

1. Compute the points $P \oplus Q$ and $P \ominus Q$.
2. Compute the points $P \oplus P$ and $Q \oplus Q$.

Solution. We have $E\colon Y^2 = X^3 + 17$ with $P = (-1, 4)$ and $Q = (2, 5)$.

1. For $P \oplus Q$, we need to find λ, X_3, and Y_3:

$$\lambda = \frac{5-4}{2-(-1)} = \frac{1}{3}, \qquad X_3 = \left(\frac{1}{3}\right)^2 - (-1) - 2 = -\frac{8}{9},$$

$$Y_3 = \left(\frac{1}{3}\right)\left(-1 - \left(-\frac{8}{9}\right)\right) - 4 = -\frac{109}{27}.$$

Hence, $P \oplus Q = \left(-\frac{8}{9}, -\frac{109}{27}\right)$.

For $P \ominus Q$, note $-Q = (2, -5)$. Now, we need to find λ, X_3, and Y_3:

$$\lambda = \frac{-5-4}{2-(-1)} = -3, \qquad X_3 = (-3)^2 - (-1) - 2 = 8,$$

$$Y_3 = (-3)(-1-8) - 4 = 23.$$

Hence, $P \ominus Q = (8, 23)$.

2. For $P \oplus P$, we need to find λ, X_3, and Y_3:

$$\lambda = \frac{3(-1)^2 + 0}{2(4)} = \frac{3}{8}, \qquad X_3 = \left(\frac{3}{8}\right)^2 - (-1) - (-1) = \frac{137}{64},$$

$$Y_3 = \frac{3}{8}\left(-1 - \frac{137}{64}\right) - 4 = -\frac{2651}{512}.$$

Hence, $P \oplus P = \left(\frac{137}{64}, -\frac{2651}{512}\right)$.

For $Q \oplus Q$, we need to find λ, X_3, and Y_3:

$$\lambda = \frac{3(2^2) + 0}{2(5)} = \frac{6}{5}, \qquad X_3 = \left(\frac{6}{5}\right)^2 - 2 - 2 = -\frac{64}{25},$$

$$Y_3 = \frac{6}{5}\left(2 - \left(-\frac{64}{25}\right)\right) - 5 = \frac{59}{125}.$$

Hence, $Q \oplus Q = \left(-\frac{64}{25}, \frac{59}{125}\right)$.

Exercise 6.3

Suppose that the cubic polynomial $X^3 + AX + B$ factors as

$$X^3 + AX + B = (X - e_1)(X - e_2)(X - e_3).$$

Prove that $4A^3 + 27B^2 = 0$ if and only if two (or more) of e_1, e_2, and e_3 are the same. (Hint. Multiply out the right-hand side and compare coefficients to relate A and B to e_1, e_2, and e_3.)

Solution. Let $X^3 + AX + B = (X - e_1)(X - e_2)(X - e_3)$. Expanding the right-hand side, we get

$$X^3 - (e_1 + e_2 + e_3)X^2 + (e_1e_2 + e_1e_3 + e_2e_3)X - e_1e_2e_3.$$

This implies $e_1 + e_2 + e_3 = 0$, $e_1e_2 + e_1e_3 + e_2e_3 = A$, and $-e_1e_2e_3 = B$.

Suppose that $e_2 = e_3$. Then we have,

$$e_1 + 2e_2 = 0, \qquad 2e_1e_2 + e_2^2 = A, \qquad e_1e_2^2 = B.$$

So, $e_1 = -2e_2$, and substituting this into the second equation gives

$$-3e_2^2 = A, \qquad -2e_2^3 = B.$$

Hence, $4A^3 + 27B^2 = 4(-3e_2^2)^3 + 27(-2e_2^3)^2 = 0$.

Conversely, suppose that $4A^3 + 27B^2 = 0$. Substituting the expressions for A and B from above and multiplying it out gives:

$$\begin{aligned} 4A^3 + 27B^2 = (4e_2^3 + 12e_3e_2^2 + 4e_3^3)e_1^3 &+ (12e_3e_2^3 + 51e_3^2e_2^3 + 12e_3^3e_2^2)e_1 \\ &+ (12e_3^2e_2^3 + 12e_3^3e_2^2)e_1 \\ &+ 4e_3^3e_2^3 \end{aligned}$$

Substituting $e_1 = -e_2 - e_3$, we get

$$4A^3 + 27B^2 = -4e_2^6 - 12e_3e_2^5 + 3e_3^2e_2^4 + 26e_3^3e_2^3 + 3e_3^4e_2^2 - 12e_3^5e_2 - 4e_3^6.$$

Because this expression is divisible by $e_2 + 2e_3$, $(e_2 + 2e_3)^2$, and $(e_3 + 2e_2)^2$. So, we find that

$$4A^3 + 27B^2 = -(e_2 - e_3)^2(e_2 + 2e_3)^2(e_3 + 2e_2)^2.$$

Hence, using the fact that $e_1 + e_2 + e_3 = 0$, we find that

$$4A^3 + 27B^2 = 0 \qquad \text{if and only if} \qquad (e_2 - e_3)^2(e_1 - e_3)^2(e_1 - e_2)^2 = 0.$$

Exercise 6.5

For each of the following elliptic curves E and finite fields $\mathbb{F}_p$, make a list of the set of points $E(\mathbb{F}_p)$.

1. $E : Y^2 = X^3 + 3X + 2$ over $\mathbb{F}_7$.
2. $E : Y^2 = X^3 + 2X + 7$ over $\mathbb{F}_{11}$.

Solution.

1. We have $E\colon Y^2 = X^3 + 3X + 2$ on $\mathbb{F}_7$.

   First, list of squares modulo 7: $0^2 = 0, 1^2 = (-1)^2 = (6)^2 = 1, 2^2 = 5^2 = 4, 3^2 = 4^2 = 2$. Now, we can list the points on the curve:

$$\begin{aligned}
0^3 + 3(0) + 2 &= 2 \\
1^3 + 3(1) + 2 &= 6 \\
2^3 + 3(2) + 2 &= 2 \\
3^3 + 3(3) + 2 &= 3 \\
4^3 + 3(4) + 2 &= 1 \\
5^3 + 3(5) + 2 &= 2 \\
6^3 + 3(6) + 2 &= 5.
\end{aligned}$$

   Hence, the points on the curve are $\{(0,3),(0,4);(2,3),(2,4);(4,1),(4,6);(5,3),(5,4);\mathcal{O}\}$. Therefore, there are 9 total points on the curve.

2. We have $E\colon Y^2 = X^3 + 2X + 7$ on $\mathbb{F}_{11}$.

   We list the squares modulo 11: $0^2 = 0, 1^2 = (-1)^2 = (10)^2 = 1, 2^2 = 9^2 = 4, 3^2 = 8^2 = 9, 4^2 = 7^2 = 5, 5^2 = 6^2 = 3$. Now, we can list the points on the curve:

$$\begin{aligned}
0^3 + 2(0) + 7 &= 7 \\
1^3 + 2(1) + 7 &= 10 \\
2^3 + 2(2) + 7 &= 8 \\
3^3 + 2(3) + 7 &= 7 \\
4^3 + 2(4) + 7 &= 2 \\
5^3 + 2(5) + 7 &= 10 \\
6^3 + 2(6) + 7 &= 4 \\
7^3 + 2(7) + 7 &= 1 \\
8^3 + 2(8) + 7 &= 7 \\
9^3 + 2(9) + 7 &= 6 \\
10^3 + 2(10) + 7 &= 4.
\end{aligned}$$

Hence, the points on the curve are $\{(6,2),(6,9);(7,1),(7,10);(10,2),(10,9);\mathcal{O}\}$. Therefore, there are 7 total points on the curve.

Exercise 6.8

Let E be the elliptic curve

$$E : Y^2 = X^3 + X + 1$$

and let $P = (4,2)$ and $Q = (0,1)$ be points on E modulo 5. Solve the elliptic curve discrete logarithm problem for P and Q, that is, find a positive integer n such that $Q = nP$.

Solution. We have $E\colon Y^2 = X^3 + X + 1$ with $P = (4,2)$ and $Q = (0,1)$ on $\mathbb{F}_5$. Solve $Q = nP$:

$$\begin{aligned} 1P &= (4,2) \\ 2P &= (3,4) \\ 3P &= (2,4) \\ 4P &= (0,4) \\ 5P &= (0,1). \end{aligned}$$

$n = 5$.

Exercise 6.11

Use the double-and-add algorithm (Table 6.3) to compute nP in $E(\mathbb{F}_p)$ for each of the following curves and points, as we did in Fig. 6.4.

1. $E : Y^2 = X^3 + 23X + 13$, $p = 83$, $P = (24,14)$, $n = 19$;
2. $E : Y^2 = X^3 + 143X + 367$, $p = 613$, $P = (195,9)$, $n = 23$;

Solution.

1. We have $E\colon Y^2 = X^3 + 23X + 13$ with $p = 83$, $P = (24,14)$, and $n = 19$. We can compute nP using the double-and-add algorithm:
    1. $n = 19 = 16 + 2 + 1$.

2.

$$\begin{aligned}
1P &= (24, 14)\\
2P &= (30, 8)\\
4P &= (24, 69)\\
8P &= (30, 75)\\
16P &= (24, 14)
\end{aligned}$$

3. $19P = (24, 14) + (30, 8) + (24, 14) = (24, 69)$.

2. We have $E\colon Y^2 = X^3 + 143X + 367$ with $p = 613$, $P = (195, 9)$, and $n = 23$. We can compute nP using the double-and-add algorithm:

1. $n = 23 = 16 + 4 + 2 + 1$.

2.

$$\begin{aligned}
1P &= (195, 9)\\
2P &= (407, 428)\\
4P &= (121, 332)\\
8P &= (408, 110)\\
16P &= (481, 300)
\end{aligned}$$

3. $23P = (481, 300) + (121, 332) + (407, 428) + (195, 9) = (485, 573)$.

Exercise 6.14

Alice and Bob agree to use elliptic Diffie-Hellman key exchange with the prime, elliptic curve, and point

$$p = 2671, \quad E : Y^2 = X^3 + 171X + 853, \quad P = (1980, 431) \in E(\mathbb{F}_{2671}).$$

1. Alice sends Bob the point $Q_A = (2110, 543)$. Bob decides to use the secret multiplier $n_B = 1943$. What point should Bob send to Alice?

2. What is their secret shared value?

4. Alice and Bob decide to exchange a new piece of secret information using the same prime, curve, and point. This time Alice sends Bob only the X-coordinate $X_A = 2$ of her point Q_A. Bob decides to use the secret multiplier $n_B = 875$. What single number modulo p should Bob send to Alice, and what is their secret shared value?

Solution.

1. We have $p = 2671$, $E\colon Y^2 = X^3 + 171X + 853$, and $P = (1980, 431)$ on $\mathbb{F}_{2671}$. Alice sends $Q_A = (2110, 543)$ to Bob. Bob uses $n_B = 1943$. We calculate $n_B P = Q_B = 1943(1980, 431) = (1432, 667)$ to be sent to Alice.

2. $n_B Q_A = 1943(2110, 543) = (2424, 911)$ is the shared secret value.

4. $n_B P = Q_B = 875(1980, 431) = (161, 2040) \Rightarrow X_B = 161$ to be sent to Alice. Now calculate $n_B X_A = 875(2, 96) = (1707, 1252)$ which gives $X = 1708$ as the shared secret value.