Mathematical Cryptography

MATH 490

Start

August 26, 2024

Author

Paul Beggs
BeggsPA@Hendrix.edu

Instructor

Prof. Allie Ray, Ph.D.

End

December 2, 2024

TABLE OF CONTENTS

CHAPTER 2

DISCRETE LOGARITHMS AND DIFFIE-HELLMAN

2.1 The Birth of Public Key Cryptography

Definition One-way Function:

A *one-way function* that is easy to computer, but whose inverse is difficult.

Definition Trap-door Function:

A *trap-door function* is a one-way function with an extra piece of information that makes f^{-1} easy.

2.2 Discrete Logarithm Problem (DLP)

Definition Discrete Logarithm Problem:

Let g be a primitive root for $\mathbb{F}_p$ and let h be a nonzero element of $\mathbb{F}_p$. The *Discrete Logarithm Problem* is the problem of finding an exponent x such that

$$g^x \equiv h \pmod{p}.$$

The number x is called the *discrete logarithm* of h to the base g and is denoted by $\log_g(h)$.

Remember the rules of logarithms:

$$\begin{aligned}
\log_b(a \cdot c) &= \log_b(a) + \log_b(c) \\
\log_b(a^c) &= c \cdot \log_b(a) \\
\log_b(a/c) &= \log_b(a) - \log_b(c)
\end{aligned}$$

What is the value of x such that $20^x = 21 \pmod{23} \overset{\text{Brute-f}}{\Longrightarrow} \log_{20} 21 = \boxed{7} \pmod{23}$. (Where 7 is from wolfram.)

Example 2.1: DLP

Find $\log_2(10) \pmod{11}$. In other words, find the value of x such that $2^x \equiv 10 \pmod{11}$.

Solution.

$$
\begin{aligned}
2^1 &= 2 \pmod{11} \\
2^2 &= 4 \pmod{11} \\
2^3 &= 8 \pmod{11} \\
2^4 &= 5 \pmod{11} \\
2^5 &= 10 \pmod{11} \\
\log_2(10) &= \boxed{5} \pmod{11}.
\end{aligned}
$$

2.2.1 Exercises

Exercise 2.3

Let g be a primitive root for $\mathbb{F}_p$.

(b) Prove that $\log_g(h_1 h_2) = \log_g(h_1) + \log_g(h_2)$ for all $h_1, h_2 \in \mathbb{F}_p^*$.

(c) Prove that $\log_g(h^n) = n \log_g(h)$ for all $h \in \mathbb{F}_p^*$ and $n \in \mathbb{Z}$.

Solution.

(b) *Proof.* We know that $g^x \equiv h \pmod{p}$, which means that $x = \log_g(h)$. Similarly, if $g^{x_1} \equiv h_1 \pmod{p}$ and $g^{x_2} \equiv h_2 \pmod{p}$, then $x_1 = \log_g(h_1)$ and $x_2 = \log(h_2)$. Now, we can substitute these values into the first equation to get $g^{x_1+x_2} \equiv h_1 h_2 \pmod{p} \equiv g^{\log_g(h_1)+\log_g(h_2)} \pmod{p}$. Then, from the properties of exponents, we can rewrite this equation as $h_1 \cdot h_2 \pmod{p} \equiv g^{\log_g(h_1 h_2)} \pmod{p}$. Therefore, $\log_g(h_1 \cdot h_2) = \log_g(h_1) + \log_g(h_2)$.

(c) *Proof* Following a similar process to (b), we start with $g^{n \log_g(h)}$. Then, by using the properties of logarithms, we can rewrite this as $g^{\log_g(h^n)}$. Then, because $g^{\log_g}$ cancel out, we see that $g^{\log_g(h^n)} = h^n$. Putting everything together, we have

$$
\begin{aligned}
g^{\log_g(h^n)} &\equiv h^n \pmod{p} \\
\log_g(h^n) &\equiv n \log_g(h) \pmod{p}.
\end{aligned}
$$

Exercise 2.4

Compute the following discrete logarithms.

(a) $\log_2(13)$ for the prime 23, i.e., $p = 23$, $g = 2$, and you must solve the congruence $2^x \equiv 13 \pmod{23}$.

(b) $\log_{10}(22)$ for the prime $p = 47$.

(c) $\log_{627}(608)$ for the prime $p = 941$. (Hint: Look in the second column of Table 2.1 on page 66.)

Solution.

(a) We use Wolfram Alpha to solve for x in the equation $2^x \equiv 13 \pmod{23}$: $x = 7$.

(b) Solving for x we get $x = 11$.

(c) $x = 18$.

2.3 Diffie-Hellman Key Exchange

D-H gives a way for Alice and Bob to get a secret shared key in an unsecure environment (i.e., when Eve is listening). Now, we will follow the steps of D-H below:

1. Alice and Bob choose large prime p and primitive root g and make public $k_{\text{pub}} = (p, g)$.
2. Alice and Bob each pick their own secret integers, a, b such that $k_{\text{priv }A} = a$ and $k_{\text{priv }B} = b$. Compute $g^a \pmod{p} = A$ and $g^b \pmod{p} = B$.
3. Exchange A and B over an insecure channel.
   i. Note that Eve would have to solve DLP if she obtained A and B where $a = \log_g(A)$ and $b = \log_g(B)$.
   ii. Guidelines $\approx 2^{1000} g \approx p/2$.
4. Alice computes $B^a \pmod{p} = A'$ and Bob computes $A^b \pmod{p} = B'$.

Example 2.2: D-H

Let $p = 23$ and $g = 5$. Alice chooses $a = 6$ and Bob chooses $b = 15$. Compute the shared secret key.

Solution.

$$\begin{aligned}A &= 5^6 \pmod{23} = 8\\ B &= 5^{15} \pmod{23} = 19\\ A' &= 19^6 \pmod{23} = 2\\ B' &= 8^{15} \pmod{23} = 2.\end{aligned}$$

Definition Diffie-Hellman Problem:

Let p be a prime number and g an integer. The *Diffie-Hellman Problem* is the problem of computing the value of $g^{ab} \pmod{p}$ from the known values of $g^a \pmod{p}$ and $g^b \pmod{p}$.

2.3.1 Exercises

2.4 Elgamal Public Key Cryptosystem

Alice	Bob
Public parameter creation	
A trusted party chooses and publishes a large prime p and an element g modulo p of large (prime) order.	
Key creation	
Alice	**Bob**
Choose private key $1 \leq a \leq p-1$. Compute $A = g^a \pmod{p}$. Publish the public key A.	
Encryption	
	Choose plaintext m. Choose random element k. Use Alice's public key A to compute $c_1 = g^k \pmod{p}$ and $c_2 = mA^k \pmod{p}$. Send ciphertext c_1, c_2 to Alice.
Decryption	
Compute $(c_1^a)^{-1} \cdot c_2 \pmod{p}$. This quantity is equal to m.	

Table 2.1: Elgamal Key Creation, Encryption, and Decryption

Example 2.3: Elgamal

Let $p = 29$ and $g = 2$. Alice chooses $a = 12$ and Bob chooses $k = 5$ and wants to send secret message $m = 26$. Compute the shared secret key.

Solution. First, we need to calculate Alice's A and Bob's B. Then, we can calculate the ciphertexts c_1 and c_2:

$$\begin{aligned}
A &= g^a \pmod p && = 2^{12} \pmod{29} = 7 \\
B &= g^k \pmod p && = 2^5 \pmod{29} = 3 \\
c_1 &= g^k \pmod p && = 2^5 \pmod{29} = 3 \\
c_2 &= m(A^k) \pmod p && = 26(7^5 \pmod{29}) = 10
\end{aligned}$$

Now, for Alice to decrypt the message, she must compute $(c_1^a)^{-1} \cdot c_2 \pmod p$:

$$(c_1^a)^{-1} \cdot c_2 \pmod p = (3^{12})^{-1} \cdot 10 \pmod{29}$$

The order of operations to compute this is as follows:

1. **Compute** $3^{12} \pmod{29} = 16$;
2. **Compute** $16^{-1} \pmod{29} = 20$;
3. **Finish by multiplying** $20 \cdot 10 \pmod{29} = 26$.

Be aware: You should only use this encryption scheme once. If you use it more than once, it is possible for an attacker to decrypt the message. For example, Eve knows $m_1(c_1, c_2) \to$ Eve finds A by keeping record of the first message, then by solving for d_2 such that c_1, d_2 (where c_1 is the *same* as the first message) and d_2 is the second message. Then, Eve can solve for m_2 by computing $(c_1^d)^{-1} \cdot d_2 \pmod p$.

2.4.1 Exercises

Exercise 2.8

Alice and Bob agree to use the prime $p = 1373$ and the base $g = 2$ for communications using the Elgamal public key cryptosystem.

(a) Alice chooses $a = 947$ as her private key. What is the value of her public key A?

(b) Bob chooses $b = 716$ as his private key, so his public key is

$$B \equiv 2^{716} \equiv 469 \pmod{1373}.$$

Alice encrypts the message $m = 583$ using the random element $k = 877$. What is the ciphertext (c_1, c_2) that Alice sends to Bob?

(c) Alice decides to choose a new private key $a = 299$ with associated public key

$$A \equiv 2^{299} \equiv 34 \pmod{1373}.$$

Bob encrypts a message using Alice's public key and sends her the ciphertext $(c_1, c_2) = (661, 1325)$. Decrypt the message.

(d) Now Bob chooses a new private key and publishes the associated public key $B = 893$. Alice encrypts a message using this public key and sends the ciphertext $(c_1, c_2) = (693, 793)$ to Bob. Eve intercepts the transmission. Help Eve by solving the discrete logarithm problem $2^b \equiv 893 \pmod{1373}$ and using the value of b to decrypt the message.

Solution.

(a) $p = 1373,\ g = 2,\ a = 947 \Rightarrow A \equiv 2^{947} \pmod{1373} \equiv 177.$

(b) $c_1 \equiv 2^{877} \pmod{1373} \equiv 719,\ c_2 \equiv 583 \cdot 469^{877} \pmod{1373} \equiv 623.$ Alice sends "(719, 623)" to Bob.

(c) To decrypt, we can use the EEA to find the inverse of $661^{299} \pmod{1373} \equiv 645^{-1} \equiv 794$. From here, we solve for the message: $1325 \cdot 794 \pmod{1373} \equiv 332$.

(d) Solving for b in $2^b \equiv 893 \pmod{1373}$ gives $b = 219$. Now we can decrypt:

$$(c_1^a)^{-1} \cdot c_2 \equiv (693^{219})^{-1} \equiv 431^{-1} \cdot 793 \equiv 532 \cdot 793 \equiv 365 \pmod{1373}.$$

Alice's private message to Bob is $m = 365$.

2.5 An Overview of the Theory of Groups

Definition Group:

A set G along with a binary operation (closure) such that for all $a, b \in G$, $a \times b \in G$ (closure), and there exists an $e \in G$ such that $a \times e = a$ and $e \times a = a$ (identity), for all $a \in G$, there exists $a^{-1} \in G$ such that $a \times a^{-1} = a^{-1} \times a = e$ (inverse), and for all $a, b, c \in G$, $(a \times b) \times c = a \times (b \times c)$ (associativity)

For commutativity, for all $a, b \in G$, $a \times b = b \times a$. Some groups have this, some do not.

Example 2.4: Integer Addition as a Group

Lets check to see addition among the integers are a group: $(\mathbb{Z}, +)$

Solution.

1. True. Let $a, b \in \mathbb{Z}$ $a + b \in \mathbb{Z}$.
2. True. $e = 0 \in \mathbb{Z}$, $a + 0 = a$ and $0 + a = a$
3. True. For all $a \in \mathbb{Z}$, $a^{-1} = -a$ because $a + (-a) = 0 = -a + a$
4. True. For all $a, b, c \in \mathbb{Z}$, $(a + b) + c = a + (b + c)$

Therefore, the additive property of the integers are a group. In fact, because $a+b = b+a$ $\mathbb{Z}$ are a commutative group (abelian group).

Example 2.5: Integer Multiplication

Lets check to see multiplication among the integers are a group: $(\mathbb{Z}, +)$

Solution.

1. True. Let $a, b \in \mathbb{Z}$ $ab \in \mathbb{Z}$.
2. True. $e = 1 \in \mathbb{Z}$, $a * 1 = a$ and $1 * a = a$
3. False. Counterexample: consider $2^{-1} = \frac{1}{2}$ because $2(\frac{1}{2}) = 1$ but $\frac{1}{2} \notin \mathbb{Z}$

Definition Order:

The *order* of an element $a \pmod p$ is the smallest exponent $k \geq 1$ such that $a^k \equiv 1 \pmod p$.

2.5.1 Exercises

Exercise (Additional)

Decide whether each of the following is a group:

(a) `All 2×2 matrices with real number entries` with operation matrix addition

(b) `All 2 × 2 matrices with real number entries` with operation matrix multiplication

Solution.

(a) **Matrix Addition: ✓**

(1) **Closure:** For addition to work between matrices, they must be of dimension $2 \times 2 + 2 \times 2$. Therefore, the dimensions do not change, and it is closed.

(2) **Associativity:** 2×2 matrix addition is associative, as it inherits this property from the properties of matrices.

(3) **Identity Element:** We can add a matrix Z that consists of only 0s to a matrix A. And matrix A will remain unchanged.

(4) **Inverse Element:** True. Consider the matrices, $\begin{bmatrix} a & b \\ c & d \end{bmatrix}$. And $\begin{bmatrix} -a & -b \\ -c & -d \end{bmatrix}$. When we add these two together we get $\begin{bmatrix} 0 & 0 \\ 0 & 0 \end{bmatrix}$. This shows that 2×2 matrices have additive inverses.

(b) **Matrix Multiplication: ✗**

(1) **Closure:** The dimensions will stay the same during multiplication because it is an $n \times n$ matrix.

(2) **Associativity:** 2×2 matrix multiplication is associative, as it inherits this property from the properties of matrices.

(3) **Identity Element:** True. Consider the identity matrix, $I_2 = \begin{bmatrix} 1 & 0 \\ 0 & 1 \end{bmatrix}$. When we multiply a matrix $\begin{bmatrix} a & b \\ c & d \end{bmatrix}$ by I. We get

$$\begin{bmatrix} a & b \\ c & d \end{bmatrix}$$

$\cdot \begin{bmatrix} 1 & 0 \\ 0 & 1 \end{bmatrix} = \begin{bmatrix} a & b \\ c & d \end{bmatrix}$

(4) **Inverse Element:** False. Matrices with a non-zero determinant fail this criteria. Consider the matrix $B = \begin{bmatrix} 1 & 2 \\ 3 & 4 \end{bmatrix}$. The determinant would be $\det((1)(4) - (2)(3) = -2$. Therefore, this matrix would not have an inverse.

Exercise (Additional)

Is `All 2x2 matrices with real number entries` a ring with operations matrix addition and matrix multiplication? Justify your answer.

Solution. ✓

(1) **Additive Closure:** True. (See the previous exercise (a), (1)).

(2) **Additive Associativity:** True. Inherited from the properties of matrices.

(3) **Additive Identity:** True. (See the previous exercise (a), (3)).

(4) **Additive Inverse:** True. You can take the difference between a matrix and its inverted duplicate (e.g., $-[A]$) and get 0.

(5) **Multiplicative Closure:** True. (See the previous exercise (b), (4)).

(6) **Distributive Property:** True. While this will pose an error on a calculator, you can do the equivalent: $[A]([B] + [C]) = [A][B] + [A][C]$. This is true because you are still taking the summation of each a_{ij}. b_{ij} and c_{ij}.

2.7 A Collision Algorithm for the DLP

Recall that the DLP is the problem of finding x such that $g^x \equiv h \pmod p$ for a given value of h.

Remember that to brute force the DLP, it takes $P - 1$ steps. Recall $g^{p-1} \pmod p \equiv 1$. In computational complexity, **we say that the DLP is $\mathcal{O}(P)$.**

Proposition 2.21:

(Shanks Baby-Step Giant-Step Algorithm) Computational time of $\mathcal{O}(\sqrt{P})$. Below is the algorithm:

1. Let $m = \lceil \sqrt{P} \rceil$.

2. Create two lists:

   (a) Baby steps: $\{g^0, g^1, g^2, \ldots, g^m\}$.

   (b) Giant steps: $\{h, h \cdot g^{-m}, h \cdot g^{-2m}, \ldots, h \cdot g^{-m^2}\}$.

3. Find a match between the two lists: $g^i \equiv hg^{-im} \pmod p$
4. $x = i + jm$ is a solution for $g^x \equiv h \pmod p$ (another way of saying "$x = i + jm$ is a solution for the DLP").

Example 2.6: Baby-step, Giant-step

Use the Baby-step, Giant-step algorithm to solve for $13^x \equiv 5 \pmod{47}$.

Solution.

1. Let $m = \lceil\sqrt{47}\rceil = 7$.
2. Create the two lists:
   (a) Baby steps: $\{13^0, 13^1, 13^2, \ldots, 13^6\} \pmod{47} \equiv \{1, 13, 28, 35, 32, 40, 3, 39\}$.
   (b) Giant steps: $\{5, 5\cdot 13^{-7}, 5\cdot 13^{-14}, \ldots, 5\cdot 13^{-49}\} \pmod{47} \equiv \{5, 17, 39, 1, 48, 36, 19, 27\}$.
3. Find a match between the two lists: 39 and 39, or 1 and 1.
4. Substitute the following variables: $i = 7$, $j = 2$, $n = 7$ for the equation $x = i + jm \Rightarrow x = 7 + 2(7) = \boxed{21}$. So, $13^{21} \equiv 5 \pmod{47}$.

Example 2.7: (From Book) Baby-step, Giant-step

Solve the discrete logarithm problem with these values: $g = 9704, h = 13896, p = 17389$.

Solution. The number 9704 has order 1242 in $\mathbb{F}^*_{17389}$. Set $n = \lceil\sqrt{1242}\rceil = 36$ and $u = g^{-n} = 9704{-}36 = 2494$. Table 2.4 in the book lists the values of g^k and $h \cdot u^k$ for $k = 1, 2 \ldots$. From the table, we find the collision

$$9704^7 = 14567 = 13896 \cdot 2494^{32} \text{ in } \mathbb{F}_{17389}.$$

Using the fact that $2494 = 9704^{-36}$, we compute

$$13896 = 9704^7 \cdot 2494^{-32} = 9704^7 \cdot (9704^{36})^{32} = 9704^{1159} \text{ in } \mathbb{F}_{17389}.$$

Hence, $x = 1159$ solves the problem $9704^x = 13896$ in $\mathbb{F}_{17389}$.

2.7.1 Exercises

Exercise 2.17

Use Shanks's babystep-giantstep method (Proposition 2.21) to solve the following discrete logarithm problems.

(a) $11^x = 21$ in $\mathbb{F}_{71}$.

Solution.

(a)
1. Let $m = \lceil\sqrt{70}\rceil = 9$
2. Create two lists:
   - **Baby steps:**
   $$\{11^0, 11^1, \ldots, 11^9\} \pmod{71} \equiv \{1, \boxed{11}, 50, 53, 15, 23, 40, 14, 12\}$$
   - **Giant steps:**
   $$\{21, 21 \cdot 11^{-9}, 21 \cdot 11^{-18}, \ldots\} \pmod{71} \equiv \{21, 5, 35, 32, \boxed{11} \ldots\}$$
3. Find a match between the two lists: $\boxed{11}$
4. Substitute values for $i + jm = 1 + 4(9) = 37$. So, $11^{37} \equiv 21 \pmod{71}$

2.8 Chinese Remainder Theorem (CRT)

Theorem: Chinese Remainder

Let $n_1, n_2, \ldots, n_k$ be pairwise relatively prime integers. This means that $\gcd(m_i, m_j) = 1$ *for all* $i \neq j$. Then, for any integers $a_1, a_2, \ldots, a_k$, the system of congruences

$$\begin{aligned} x &\equiv a_1 \pmod{n_1} \\ x &\equiv a_2 \pmod{n_2} \\ &\vdots \\ x &\equiv a_k \pmod{n_k} \end{aligned}$$

has a unique solution $c \pmod{n_1 n_2 \ldots n_k}$.

Example 2.8: CRT

Solve the following system of congruences:

$$x \equiv 6 \pmod 7$$
$$x \equiv 4 \pmod 8$$

Solution. Note that $x \equiv 6 \pmod 7$ means

$$\begin{aligned} x &= 7n+6 \\ 7n+6 &\equiv 4 \pmod 8 \\ 7n &\equiv 6 \pmod 8 \\ n &\equiv 6 \cdot 7^{-1} \pmod 8 \\ &\equiv 6 \cdot 7 \pmod 8 \\ &\equiv 2 \pmod 8, \end{aligned}$$

where $2 \pmod 8 = 8m+2 = n$. We plug this back into the following:

$$\begin{aligned} x &= 7(8m+2)+6 \pmod{7 \cdot 8} \\ &= 56m+14+6 \pmod{56} \\ &= 56m+20 \pmod{56}. \end{aligned}$$

Note that $56m$ is a multiple of 56 and so it will always be equal to 0. Thus, $x = 20 \pmod{56}$.

In general, to solve for CRT such that $x \equiv a_1 \pmod{m_1} \dots, x \equiv a_k \pmod{m_k}$ we follow the algorithm below:

1. Let $m = m_1 \cdot m_2 \cdots m_k$.
2. Take $n_i = \frac{m}{m_i}$.
3. Check to see if there is a solution, y_i. $y_i = n_i^{-1} \pmod{m_i}$. Note that the inverse exists because m_i and n_i are relatively prime.
4. Compute $x = a_1n_1y_1 + a_2n_2y_2 + \cdots + a_kn_ky_k \pmod m$.

Example 2.9: CRT with New Algorithm

Solve the following system of congruences: $x \equiv a_1 \pmod{m_1}$ and $x \equiv a_2 \pmod{m_2}$ where $a_1 = 6, m_1 = 7, a_2 = 4, m_2 = 8$.

Solution.

1. Let $m = 7 \cdot 8 = 56$.
2. Compute $n_1 = 8$ and $n_2 = 7$.
3. Compute $y_1 = 8^{-1} \pmod 7 = 1$ and $y_2 = 7^{-1} \pmod 8 = 7$.
4. Compute

$$\begin{aligned} x &= 6 \cdot 8 \cdot 1 + 4 \cdot 7 \cdot 7 \pmod{56} \\ &= 48 + 196 \pmod{56} \\ &= 244 \pmod{56} \\ &= \boxed{20}. \end{aligned}$$

2.8.1 Exercises

Exercise 2.18

Solve each of the following simultaneous systems of congruences (or explain why no solution exists).

(b) $x \equiv 137 \pmod{423}$ and $x \equiv 87 \pmod{191}$.

(d) $x \equiv 5 \pmod 9$, $x \equiv 6 \pmod{10}$, and $x \equiv 7 \pmod{11}$.

Solution.

(b)
1. Let $m = 423 \cdot 191 = 80793$.
2. Compute $n_1 = \frac{m}{m_1} = \frac{80793}{423} = 191$, and $n_2 = \frac{80793}{191} = 423$
3. Compute $y_1 = 191^{-1} \pmod{423} \equiv 392$ and $y_2 = 423^{-1} \pmod{191} \equiv 14$.
4. Compute $x = (137)(191)(392) + (87)(423)(14) \pmod{80793} \equiv 27209$

(d)
1. Let $m = 9 \cdot 10 \cdot 11 = 990$.
2. Compute $n_1 = \frac{990}{9} = 110,\ n_2 = \frac{990}{10} = 99,$ and $n_3 = \frac{990}{11} = 90$.
3. Compute $y_1 = 110^{-1} \pmod 9 \equiv 5,\ y_2 = 99^{-1} \pmod{10} \equiv 9$, and $y_3 = 90^{-1} \pmod{11} \equiv 6$
4. Compute $x = (5)(110)(5) + (6)(99)(9) + (7)(90)(6) \pmod{990} = 986$

Exercise 2.20

Let a, b, m, n be integers with $\gcd(m, n) = 1$. Let

$$c \equiv (b - a) \cdot m^{-1} \pmod{n}.$$

Prove that $x = a + cm$ is a solution to

$$x \equiv a \pmod{m} \quad \text{and} \quad x \equiv b \pmod{n}, \tag{2.24}$$

and that every solution to (2.24) has the form $x = a + cm + ymn$ for some $y \in \mathbb{Z}$.

Proof. Let $a, b, m, n \in \mathbb{Z}$ with $\gcd(m, n) = 1$. Let $c \equiv (b - a)m^{-1} \pmod{n}$. Review the following:

$$\begin{aligned} x &\equiv a \pmod{m} \\ a + cm &\equiv a \pmod{m} \\ a &\equiv a \pmod{m} - cm. \end{aligned}$$

Then, because cm is a multiple of m, when we take the mod of $a - cm \pmod{m}$, we will always get a. Hence, $a \equiv a \pmod{m}$. For the other equation, we will be using the def of c in our proof:

$$\begin{aligned} a + cm &\equiv b \pmod{n} \\ cm &\equiv b - a \pmod{n} \\ c &\equiv (b - a)m^{-1} \pmod{n}. \end{aligned}$$

So, now when we multiply by m on both sides, we get $cm \equiv b - a \pmod{n}$. Rearranging, we see $cm + a \equiv b \pmod{n}$, so x is a solution.

For the second half of the proof, suppose we have x' as the solution for $x' \equiv a \pmod{m}$ and $x' \equiv b \pmod{n}$. We want to show that $x' = x$. Thus, we subtract x from x' and get the following:

$$x' - x \equiv a - a = 0 \pmod{m}, \text{ which implies } x' - x = km \text{ for some } k \in \mathbb{Z}.$$

This is the outcome because we know that for anything to be equal to 0 in modulus, the number itself must be a multiple of the modulus, m. We can follow the same logic for b, and see that $x' - x \equiv b - b = lm$ for some $l \in \mathbb{Z}$. Since $\gcd(m, n) = 1$, $x' - x$ must be a multiple of m and n, meaning $x' - x = ymn$ for some $y \in \mathbb{Z}$. Therefore, $x' = x + ymn, = a + cm + ymn$. $\square$

2.9 Pohlig-Hellman Algorithm

This algorithm is used to solve $g^x \equiv h \pmod p$ for p prime and g primitive root. This has computational time of $\mathcal{O}(\sqrt{p-1})$. Order of g is $p-1$ is composite. This is most efficient when $p-1$ has small prime factors. Look below for the algorithm:

1. Factor $p-1 = n_1^{e_1} \cdot n_2^{e_2} \cdots n_k^{e_k}$. (Note that $\gcd(q_j, q_i) = 1\ \forall i \neq j$.)
2. For each $1 \leq i \leq k$, let $m_i = \frac{p-1}{n_i^{e_i}}$.
3. Solve $g^{x_i} \equiv h^{m_i} \pmod p$ for x_i. (Note this DLP is easier because order of g_i is way less than the order of g.)
4. Use CRT to find x such that $x \equiv x_1 \pmod{q_1^{e+1}}, \ldots, x_i \pmod{n_i^{e_i}}$.

Example 2.10: Pohlig-Hellman Algorithm

Solve the following DLP: $106^x \equiv 12375 \pmod{24691}$.

Solution. To use the Pohlig-Hellman algorithm, we need to find the order of the prime number $p = 24691$. Since it is prime, we know the order to be $\varphi(24691) = 24690$. We can factor this number to $30 \cdot 823$. Let $x = a_0 + 30a_1$:

$$(106^{a_0+30a_1})^{823} \equiv 12375^{823} \pmod{24691} \tag{2.1}$$
$$(106^{823a_0+24690a_1}) \equiv 24143 \pmod{24691} \tag{2.2}$$
$$(106^{823a_0} \cdot 106^{24690a_1}) \equiv 24143 \pmod{24691} \tag{2.3}$$
$$(106^{823})^{a_0} \cdot (106^{24690})^{a_1} \equiv 24143 \pmod{24691} \tag{2.4}$$
$$(1410)^{a_0} \equiv 24143 \pmod{24691} \tag{2.5}$$

For (1), we got the expression by substituting x for a_0+30a_1 for the exponent in $g^x \equiv \ldots$. From there, (2) — (4) is simple algebra. Then for (5), because 106^{a_1} is congruent to 1, $(106^{a_1})^{24690} = 1$. Additionally, we take $106^{823} \pmod{24691}$ to get 1410^{a_0}. Then, we do the same thing for the other side of the equation. Now, we can brute force this by setting $a_0 = \{0, 1, 2, 3, \ldots, 823\}$. We find that when $a_0 = 12$, $1410^{a_0} \equiv 24143 \pmod{24691}$. Seeing that we have a_0, we need to find b_0:

$$(106^{b_0+823b_1})^{30} \equiv 12375^{30} \pmod{24691}$$
$$15097^{b_0} \equiv 7229 \pmod{24691}$$

Thus, through brute force, we find that $b_0 = 171$. We can take our a_0 and b_0 to solve for x_1, x_2:

$$x_1 = a_0 + 30a_1$$
$$x_1 = 12 \pmod{30}$$

and

$$x_2 = b_0 + 823b_1$$
$$x_2 = 171 \pmod{823}$$

At this point, we can solve the Chinese Remainder Theorem.

1. Let $m = 30 \cdot 823 = 24690$.
2. Compute $n_1 = \frac{24690}{30} = 823$ and $n_2 = \frac{24690}{823} = 30$.
3. Compute $y_1 = 823^{-1} \pmod{30} \equiv 7$ and $y_2 = 30^{-1} \pmod{823} \equiv 631$.
4. Compute $x = (12)(823)(7) + (171)(30)(631) \pmod{24690} \equiv 22392$.

Therefore, $a = 22392$

2.9.1 Exercise

Exercise 2.28

Use the Pohlig-Hellman algorithm to solve the discrete logarithm problem $g^x = a$ in $\mathbb{F}_p$ in each of the following cases.

(a) $p = 433$, $g = 7$, $a = 166$.

Solution. We start by writing the given information into an equation that we can work with. Thus, $7^x \equiv 166 \pmod{433}$. Since 433 is prime, $\varphi(433) = 432$, which we can factor to $16 \cdot 27$. Let $x = a_0 + 16a_1$:

$$(7^{a_0+16a_1})^{27} \equiv 166^{27} \pmod{433} \tag{2.6}$$
$$(7^{27a_0+432a_1}) \equiv \tag{2.7}$$
$$(7^{27a_0} \cdot 7^{432a_1}) \equiv \tag{2.8}$$
$$(7^{27})^{a_0}(7^{a_1})^{432} \equiv \tag{2.9}$$
$$(265)^{a_0} \equiv 250 \pmod{433} \tag{2.10}$$

For (3.1), we got the expression by substituting x for $a_0 + 16a_1$ for the exponent in $g^x \equiv \ldots$. From there, (3.2) — (3.4) is simple algebra. Then for (3.5), because 7^{a_1} is congruent to 1, $(7^{a_1})^{432} = 1$. Additionally, we take $7^{27} \pmod{432}$ to get 265^{a_0}. Then, we do the same thing for the other side of the equation. Now, we can brute force this by setting $a_0 = \{0, 1, 2, 3, \ldots, 27\}$. We find that when $a_0 = 15$, $265^{a_0} \equiv 250 \pmod{433}$. Seeing that we have a_0, we need to find b_0:

$$(7^{b_0+27b_1})^{16} \equiv 166^{16} \pmod{433}$$
$$374^{b_0} \equiv 335 \pmod{433}$$

Thus, through brute force, we find that $b_0 = 20$. We can take our a_0 and b_0 to solve for x_1, x_2:

$$x_1 = a_0 + 16a_1$$
$$x_1 = 15 \pmod{16}$$

and

$$x_2 = b_0 + 27b_1$$
$$x_2 = 20 \pmod{27}$$

At this point, we can solve the CRT.

1. Let $m = 16 \cdot 27 = 432$.
2. Compute $n_1 = \frac{432}{16} = 27$ and $n_2 = \frac{432}{27} = 16$.
3. Compute $y_1 = 27^{-1} \pmod{16} \equiv 3$ and $y_2 = 16^{-1} \pmod{27} \equiv 22$.
4. Compute $x = (27)(15)(3) + (20)(16)(22) \pmod{432} = 47$

I relied on this video heavily.

CHAPTER 4

DIGITIAL SIGNATURES

4.1 What Is a Digital Signature?

We used RSA and Elgamal for confidentiality, whereas we use digital signatures for authentication. A digital signature is a way to ensure that a message is authentic, has not been tampered with, and is from the person who claims to have sent it.

4.2 RSA Digital Signatures

Recall RSA encryption and decryption. We have public key $(N = pq, e)$ where N is the modulus, e is the public exponent, and p, q are the prime factors of N. We also have private key p, q where e has the following property: $\gcd(e, (p-1)(q-1)) = 1$. This ensures a d exists such that $d \equiv e^{-1} \pmod{(p-1)(q-1)}$.

Note: To gain a bit of efficiency, choose a d and e to satisfy

$$de \equiv 1 \left(\text{mod} \frac{(p-1)(q-1)}{\gcd(p-1, q-1)}\right)$$

To sign a document D, which we assume to be an integer in the range $1 < D < N$, we compute the signature S as follows:

$$S \equiv D^d \pmod{N}$$

To verify this signature, we compute:

$$D \equiv S^e \pmod{N}$$

Example 4.1: RSA Digital Signature

Given the following (p, q, a) as $(1223, 1987, 2430101)$ with the verification exponent $e = 948074$, publish a document and verify its signature.

Solution. Samantha computers her private signing key d using secret values of p and q to compute $(p-1)(q-1) = 1222 \cdot 1986 = 2426892$ and then solving the congruence

$$ed \equiv 1 \pmod{(p-1)(q-1)}, \quad 948074d \equiv 1 \pmod{2426892}$$

She finds that $d = 1051235$. Samantha selects a digital document to sign,

$$D = 1070777 \quad \text{with} \quad 1 \leq D < N.$$

She computes the digital signature

$$S \equiv D^d \pmod{N}, \quad S \equiv 1070777^{1051235} \equiv 153337 \pmod{2430101}.$$

She then publishes the document and signature

$$D = 1070777, \quad S = 153337.$$

To verify the signature, the recipient computes

$$S^e \pmod{N}, \quad 153337^{948074} \equiv 1070777 \pmod{2430101}.$$

He verifies that the value of S^e modulo N is the same as the value of the digital document $D = 1070777$.

Key creation	
Samantha	**Victor**
Choose secret primes p and q. Choose encryption exponent e with $\gcd(e, (p-1)(q-1)) = 1$. Publish $N = pq$ and e.	
Signing	
Compute d satisfying $ed \equiv 1 \pmod{(p-1)(q-1)}$. Sign document D by computing $S \equiv D^d \pmod{N}$.	
Verification	
	Compute $S^e \pmod{N}$ and verify that it equals D.

Table 4.1: RSA Digital Signatures

4.3 Elgamal Digital Signatures

Elgamal digital signatures are similar to RSA digital signatures. We have public key (p, g, A). Where A is the public key from the expression $A \equiv g^a \pmod{p}$ and private key a. To sign a document D, where $1 < D < p$, choose a random k with $\gcd(k, p-1) = k$. Compute

$$S_1 \equiv g^k \pmod{p} \quad \text{and} \quad S_2 \equiv (D - aS_1)k^{-1} \pmod{p-1}.$$

Victor verifies the signature by checking that

$$A^{S_1} S_1^{S_2} \pmod{p} \text{ is equal to } g^D \pmod{p}.$$

Example 4.2: Elgamal Digital Signature

Given the following (p, g, a) as $(21739, 7, 15140)$, sign a document and verify its signature.

Solution. First, we need to calculate A:

$$A \equiv g^a \pmod{p}, \quad A \equiv 7^{15140} \pmod{21739} \equiv 17702.$$

Next, we sign the digital document $D = 5331$ using the random element $k = 10727$ by computing

$$S_1 \equiv g^k \equiv 7^{10727} \equiv 15775 \pmod{21739},$$
$$S_2 \equiv (D - aS_1)k^{-1} \equiv (5331 - 15140 \cdot 15775) \cdot 6353 \equiv 10727 \pmod{21739}.$$

Verify the signature by computing

$$A^{S_1} S^{S_2} \equiv 17702^{15775} \cdot 15775^{10727} \equiv 7^{5331} \equiv 13897 \pmod{21739}$$

and verifying that it agrees with

$$g^D \equiv 7^{5331} \equiv 13897 \pmod{21739}.$$

Public parameter creation	
A trusted party chooses and publishes a large prime p and an element g modulo p of large (prime) order.	
Key creation	
Samantha	**Victor**
Choose secret signing key $1 \leq a \leq p-1$. compute $A = g^a \pmod{p}$. Publish the verification key A.	
Signing	
Choose document $D \pmod{p}$. Choose random element $1 < k < p$ satisfying $\gcd(k, p-1) = 1$. Compute signature $S_1 \equiv g^k \pmod{p}$ and $S_2 \equiv (D - aS_1)k^{-1} \pmod{p-1}$.	
Verification	
	Compute $A^{S_1} S_1^{S_2} \pmod{p}$ Verify that it is equal to $g^D \pmod{p}$.

Table 4.2: The Elgamal Digital Signature Algorithm

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.

(a) Find slope: $m = \frac{y_2 - y_1}{x_2 - x_1} = \frac{8-9}{-2-(-3)} = -1$.

(b) Solve the equation of line: $y = -x + b$. Plug in P: $9 = 3 + b \implies b = 6$. Thus, $y = -x + 6$.

(c) Plug y back into given formula:

$$
\begin{aligned}
(-x + 6)^2 &= x^3 - 36x \\
x^2 - 12x + 36 &= x^3 - 36x \\
(-x^3) + x^2 + 24x + 36 &= 0 \\
x^3 - x^2 - 24x - 36 &= 0
\end{aligned}
$$

(d) 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.

(e) 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. (a) **Identity:** True because $\mathcal{O}$ lies on all vertical lines.

(b) **Inverse:** Same reason as Identity. (Also, we defined $\mathcal{O}$ as such.)

(c) **Associative:** Ignoring because hard.

(d) **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.

(a) 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

(a) Write n in binary.

(b) Repeatedly double the point P up to the highest multiple of 2 in binary representation of n.

(c) 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.

(a) Write $n = 11$ in binary: $11 = 1011$.

(b) Double the point P up to the highest multiple of 2 in the binary representation of

n:

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

(c) 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

(a) Write n in binary.

(b) 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.

(a) Write 11 in binary: $11 = 1011$.

(b) Replace the binary expansion with the ternary expansion:

$$\begin{aligned}11 &= 8 + 2 + 1\\ &= 1(8) + 1(4) + 1(2) + 1(1)\\ &= 8 + 4 + 1(\not{2}) - 1\\ &= 11.\end{aligned}$$

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:

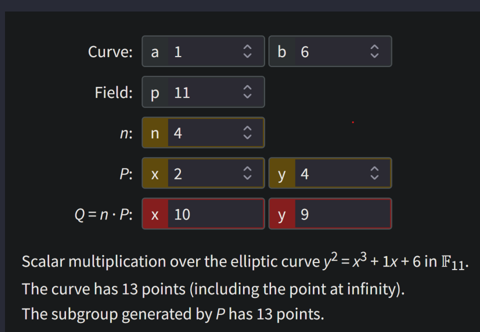
$$\begin{aligned} y_3 &\equiv 4(5-6)-9 \\ &\equiv 4(-1)-9 \\ &\equiv -4-9 \\ &\equiv 9 \pmod{11}. \end{aligned}$$

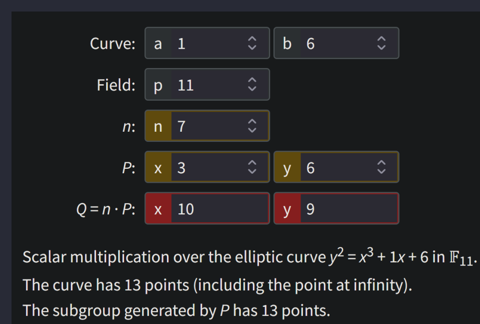
Thus, $2P = (6,9)$. Using the same process, we find that $Q_A = 2(2P) = 2(6,9) = (3,6)$.

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

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

From the image below, we can see that when we take the point $n_AQ_B \Rightarrow 4 \cdot (2,4)$, we get the point $(10,9)$. Then, when we take the point $n_BQ_A \Rightarrow 7 \cdot (3,6)$, 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 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.)

(a) Compute $P \oplus Q$.

(b) Compute $P \oplus P$ and $Q \oplus Q$.

Solution. We have $E\colon y_2 = x^3 - 2x + 4$ with $P = (0, 2)$ and $Q = (3, -5)$.

(a) 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, $P \oplus Q = \left(\frac{22}{9}, \frac{100}{27}\right)$.

(b) 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 $E : y^2 = x^3 + 17$.

(a) Compute the points $P \oplus Q$ and $P \ominus Q$.

(b) 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 $Q = (2, 5)$.

(a) For $P \oplus Q$, we need to find lambda, 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 lambda, 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, $P \ominus Q = (8, 23)$.

(b) For $P \oplus P$, we need to find lambda, 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 lambda, 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

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

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 $E(\mathbb{F}_p)$.

(a) $E : y^2 = x^3 + 3x + 2$ over $\mathbb{F}_7$.

(b) $E : y^2 = x^3 + 2x + 7$ over $\mathbb{F}_{11}$.

Solution.

(a) 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.

(b) 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.

(a) $E : y^2 = x^3 + 23x + 13$, $p = 83$, $P = (24,14)$, $n = 19$;

(b) $E : y^2 = x^3 + 143x + 367$, $p = 613$, $P = (195,9)$, $n = 23$;

Solution.

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

(b) 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

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

(a) 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?

(b) What is their secret shared value?

(d) 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.

(a) 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.

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

(d) $n_B P = Q_B = 875(1980, 431) = (161, 2040) \Rightarrow x_B = 161$ 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.