Elliptic Curve Cryptography (ECC) - Simplified Notes

1. What is an Elliptic Curve?

- An **elliptic curve** is a set of points (x, y) that satisfy the equation:

  $$y^2 = x^3 + ax + b$$

  where:

  - a and b are constants.
  - The **discriminant condition** must hold:

    $$4a^3 + 27b^2 \neq 0$$

    (This ensures the curve is smooth, with no cusps or self-intersections.)

Example Verification

- Take $a = 3$, $b = 2$, and point $(2, 4)$:

  $$4^2 = 2^3 + 3(2) + 2 \implies 16 = 8 + 6 + 2 \implies 16 = 16$$

  The point satisfies the equation.

2. Types of Elliptic Curves

1. **Over Real Numbers**
   - Points (x, y) where x, y are real numbers.
   - Forms a continuous curve (visualized as a smooth graph).
2. **Over Complex Numbers**
   - More abstract, not commonly used in cryptography.
3. **Over Finite Fields (Used in Cryptography)**
   - Defined as:

     $$y^2 \equiv x^3 + ax + b \pmod{p}$$

     where p is a prime number (finite field size).
   - Only a finite set of points exists.

3. Constructing an Elliptic Curve Over a Finite Field

Example: Curve over $GF(11)$ (Integers mod 11)

- **Equation:**

$$y^2 \equiv x^3 + x + 1 \pmod{11}$$

- **Step 1**: Find all possible (x, y) pairs in $GF(11)$.
- **Step 2**: For each x, compute $x^3 + x + 1 \pmod{11}$.
- **Step 3**: Find y such that $y^2 \equiv \text{result from Step 2} \pmod{11}$.

List of Points on the Curve

$$(0,1), (0,10), (1,5), (1,6), (2,0), (3,3), (3,8), (4,5), (4,6), (6,5), (6,6), (8,2), (8,9)$$

4. Adding Two Points on the Curve

Given two points $P = (x_1, y_1)$ and $Q = (x_2, y_2)$ on the curve, where $P \neq Q$ and $Q \neq -P$:

Formula for Point Addition $R = P + Q = (x_3, y_3)$

1. **Compute slope (Δ):**

$$\Delta = \frac{y_2 - y_1}{x_2 - x_1} \pmod{p}$$

2. **Compute x_3:**

$$x_3 = \Delta^2 - x_1 - x_2 \pmod{p}$$

3. **Compute y_3:**

$$y_3 = \Delta(x_1 - x_3) - y_1 \pmod{p}$$

Example: Adding $P = (3, 8)$ and $Q = (6, 5)$

1. **Compute Δ:**

$$\Delta = \frac{5 - 8}{6 - 3} = \frac{-3}{3} \equiv -1 \equiv 10 \pmod{11}$$

2. **Compute x_3:**

$$x_3 = 10^2 - 3 - 6 = 100 - 9 = 91 \equiv 3 \pmod{11}$$

3. **Compute y_3:**

$$y_3 = 10(3 - 3) - 8 = -8 \equiv 3 \pmod{11}$$

4. **Result:**

$$R = P + Q = (3, 3)$$

Verification: $(3, 3)$ is indeed a point on the curve.

---

5. Key Takeaways

- **Elliptic curves** are defined by $y^2 = x^3 + ax + b$ with a non-zero discriminant.
- **Cryptography uses curves over finite fields** (mod p).
- **Point addition** follows algebraic rules, ensuring the result is also on the curve.
- **ECC** leverages these properties for secure encryption (faster and more efficient than RSA).
