BAB II
LANDASAN TEORI

2.1 Kekongruenan

Definisi 2.1.1 Bilangan Bulat (Menezes, Oorschot, & Vanstone, 1996)

Himpunan bilangan bulat $\{\dots, -3, -2, -1,0,1,2,3, \dots\}$ dinotasikan dengan simbol $\mathbb{Z}$.

Definisi 2.1.2 Keterbagian (Munir, 2012)

Misalkan $a, b \in \mathbb{Z}$ dengan $a \neq 0$, maka a dikatakan habis membagi b atau $a \mid b$ jika terdapat $c \in \mathbb{Z}$ sedemikian sehingga $b = ac$.

Definisi 2.1.3 Aritmatika Modulo (Munir, 2012)

Misalkan a dan m adalah bilangan bulat dengan $m > 0$. Operasi a **mod** m (dibaca "a modulo m") memberikan sisa jika a dibagi dengan m. Dengan kata lain, a **mod** $m = r$ sedemikian sehingga $a = mq + r$, dengan $0 \leq r < m$. Bilangan m disebut modulus atau modulo, dan hasil aritmatika modulo m terletak di dalam himpunan $\{0, 1, 2, \dots, m-1\}$.

Definisi 2.1.4 Kekongruenan (Munir, 2012)

Misalkan a, b dan m adalah bilangan bulat dengan $m > 0$. Maka $a \equiv b$ (**mod** m) jika m habis membagi $a - b$. Jika a tidak kongruen dengan b dalam modulo m, maka ditulis $a \not\equiv b$ (**mod** m).

Berdasarkan **Definisi 2.1.3**, a **mod** $m = r$ dapat dituliskan sebagai

$$a \equiv r \ (\textbf{mod}\ m)$$

Teorema 2.1.1 Balikan Modulo (Munir, 2012)

Jika a dan m relatif prima, maka dapat ditemukan invers dari a modulo m. Invers dari a (**mod** m), disebut juga invers perkalian atau invers multiplikatif, adalah bilangan bulat a^{-1} sedemikian sehingga

$$aa^{-1} \equiv 1 \ (\mathbf{mod}\ m)$$

Teorema 2.1.2 Kekongruenan Linear (Munir, 2012)

Kekongruenan linear adalah kongruen yang berbentuk

$$ax \equiv b \ (\mathbf{mod}\ m)$$

dengan m adalah bilangan bulat positif, a dan b sembarang bilangan bulat, dan x adalah peubah bilangan bulat.

Definisi 2.1.5 Faktor Persekutuan Terbesar (Munir, 2012)

Misalkan $a, b \in \mathbb{Z}$ dengan salah satu a atau b tidak nol. Faktor Persekutuan Terbesar (FPB) dari a dan b adalah bilangan bulat terbesar d sedemikian sehingga $d|a$ dan $d|b$. Dalam hal ini dikatakan bahwa $\text{FPB}(a, b) = d$.

Teorema 2.1.3 Algoritma Pembagian (Niven, Zuckerman, & Montgomery, 1991)

Diberikan sebarang bilangan bulat a dan b, dengan $a > 0$, terdapat bilangan bulat unik q dan r sedemikian sehingga $b = qa + r, 0 \leq r < a$. Jika $a \nmid b$, maka r memenuhi pertidaksamaan yang lebih kuat $0 < r < a$.

Teorema 2.1.4 Algoritma Euclid (Niven, Zuckerman, & Montgomery, 1991)

Diberikan bilangan bulat b dan $c > 0$, dengan menggunakan Teorema 2.1.4, dapat dibuat perhitungan berulang untuk mendapatkan persamaan-persamaan berikut

$$\begin{aligned}
b &= cq_1 + r_1, && 0 < r_1 < c \\
c &= r_1 q_2 + r_2, && 0 < r_2 < r_1 \\
r_1 &= r_2 q_3 + r_3, && 0 < r_3 < r_2 \\
&\ldots \\
r_{j-2} &= r_{j-1} q_j + r_j, && 0 < r_j < r_{j-1} \\
r_{j-1} &= r_j q_{j+1}
\end{aligned}$$

$\text{FPB}(b, c) = r_j$, di mana r_j merupakan sisa tak nol terakhir dari proses pembagian di atas. Nilai dari x_0 dan y_0 dalam $\text{FPB}(b, c) = bx_0 + cy_0$ dapat diperoleh dengan menuliskan setiap r_j sebagai kombinasi linear dari b dan c.

Definisi 2.1.6 Relasi Ekuivalensi (Buchmann, 2004)

Diberikan relasi ekuivalensi persamaan kongruen modulo m pada himpunan bilangan bulat $\mathbb{Z}$. Kelas ekuivalensi yang memuat $a \in \mathbb{Z}$ adalah:

$$\begin{aligned}\bar{a} &= \{x \in \mathbb{Z} : x \equiv a \ (\mathbf{mod}\ m)\} \\ &= \{a + km : k \in \mathbb{Z}\} \\ &= a + m\mathbb{Z}\end{aligned}$$

Kelas ekuivalensi seperti ini disebut dengan *residue class* a **mod** m.

Definisi 2.1.7 Relatif Prima (Niven, Zuckerman, & Montgomery, 1991)

Bilangan bulat a dan b dikatakan relatif prima jika $\text{FPB}(a, b) = 1$. Dapat dikatakan bahwa $a_1, a_2, \dots, a_n$ relatif prima berpasangan jika $\text{FPB}(a_i, a_j) = 1$ untuk semua $i = 1, 2, \dots, n$ dan $j = 1, 2, \dots, n$ dimana $i \neq j$.

Definisi 2.1.8 Bilangan Prima (Niven, Zuckerman, & Montgomery, 1991)

Bilangan bulat $p > 1$ dikatakan bilangan prima jika tidak ada pembagi d yang memenuhi $1 < d < p$. Jika bilangan bulat $a > 1$ bukan bilangan prima, maka a disebut **bilangan komposit**.

Definisi 2.1.9 Fungsi Totient Euler (Menezes, Oorschot, & Vanstone, 1996)

Untuk bilangan bulat $n \geq 1$, $\phi(n)$ menotasikan banyaknya bilangan bulat pada interval $[1, n]$ yang relatif prima dengan n.

Teorema 2.1.5 Bilangan Komposit (Menezes, Oorschot, & Vanstone, 1996)

Setiap bilangan bulat positif $n \geq 2$ dapat dinyatakan sebagai perkalian satu atau lebih bilangan prima atau dikatakan mempunyai faktorisasi prima berbentuk:

$$n = p_1^{e_1} p_2^{e_2} p_3^{e_3} \cdots p_k^{e_k}$$

di mana p_i adalah bilangan-bilangan prima yang berlainan, dan e_i bilangan bulat positif.

Teorema 2.1.6 Fungsi Totient Euler (Menezes, Oorschot, & Vanstone, 1996)

Fungsi totient Euler mempunyai sifat-sifat berikut:

1. Jika n bilangan prima, maka $\phi(n) = n - 1$.
2. Jika FPB$(m, n) = 1$, maka $\phi(mn) = \phi(m)\phi(n)$.
3. Jika $n = p_1^{e_1} p_2^{e_2} p_3^{e_3} \cdots p_k^{e_k}$ merupakan faktorisasi prima dari n, maka

$$\phi(n) = n\left(1 - \frac{1}{p_1}\right)\left(1 - \frac{1}{p_2}\right)\left(1 - \frac{1}{p_3}\right)\cdots\left(1 - \frac{1}{p_k}\right)$$

Teorema 2.1.7 Teorema Fermat (Niven, Zuckerman, & Montgomery, 1991)

Misalkan p sebuah bilangan prima. Jika $p \nmid a$ maka $a^{p-1} \equiv 1 \ (\mathbf{mod}\ p)$ dan $a^p \equiv a \ (\mathbf{mod}\ p), \forall a \in \mathbb{Z}$.

Definisi 2.1.10 ***Quadratic Residue*** (Stinson, 2006)

Diberikan p bilangan prima ganjil dan a sebuah bilangan bulat. a merupakan sebuah ***quadratic residue*** **modulo** p jika $a \not\equiv 0 \ (\mathbf{mod}\ p)$ dan kongruensi $y^2 \equiv a \ (\mathbf{mod}\ p)$ mempunyai solusi $y \in \mathbb{Z}_p$. a merupakan sebuah ***quadratic non-residue*** **modulo** p jika $a \not\equiv 0 \ (\mathbf{mod}\ p)$ dan a bukan merupakan *quadratic residue* modulo p.

Contoh 2.1.1 ***Quadratic Residue***

Pada $\mathbb{Z}_5$, $1^2 = 1$, $2^2 = 4$, $3^2 = 4$ dan $4^2 = 1$. Maka 1 dan 4 merupakan *quadratic residue* modulo 5, sedangkan 2 dan 3 merupakan *quadratic non-residue* modulo 5.

Teorema 2.1.8 Kriteria Euler (Stinson, 2006)

Diberikan p sebuah bilangan prima ganjil. Maka a adalah sebuah *quadratic residue* modulo p jika dan hanya jika

$$a^{\frac{p-1}{2}} \equiv 1 \ (\mathbf{mod}\ p)$$

2.2 Grup, Ring dan Lapangan

Definisi 2.2.1 Operasi Biner (Fraleigh & Katz, 2003)

Operasi biner $*$ pada himpunan S adalah sebuah aturan yang memetakan pasangan terurut $(a, b) \in S \times S$ pada anggota S.

Definisi 2.2.2 Grup (Fraleigh & Katz, 2003)

Sebuah grup $\langle G, * \rangle$ adalah sebuah himpunan G di bawah operasi biner $*$ pada G, sedemikian sehingga syarat-syarat berikut terpenuhi:
$\boldsymbol{G_1}$**:** Operasi biner $*$ asosiatif.
$\boldsymbol{G_2}$**:** Terdapat $e \in G$ sedemikian sehingga $e * x = x * e = x$ untuk setiap $x \in G$. e adalah unsur identitas untuk operasi $*$ pada G.
$\boldsymbol{G_3}$**:** Untuk setiap $a \in G$, terdapat unsur $a' \in G$ sedemikian sehingga $a' * a = a * a' = e$. Selanjutnya dikatakan a' adalah invers dari a di bawah operasi $*$.
Sebuah grup $\langle G, * \rangle$ dikatakan **Abelian** atau **komutatif** jika operasi binernya $*$ komutatif. Selanjutnya, grup $\langle G, * \rangle$ dapat dituliskan sebagai G bila operasi binernya telah diketahui.

Definisi 2.2.3 Grup Berhingga (Fraleigh & Katz, 2003)

Jika G mempunyai banyak anggota yang berhingga, maka G disebut **grup berhingga** dan banyaknya anggota G disebut **order** G, dinotasikan dengan $|G|$.

Definisi 2.2.4 Grup Siklik (Fraleigh & Katz, 2003)

Diberikan sebuah grup G dan $a \in G$, jika $G = \{a^n | n \in Z\}$, maka G disebut grup siklik yang dibangun oleh a, dan a disebut sebagai **generator** dari G dan n disebut **eksponen**.

Teorema 2.2.1 Grup Siklik (Herstein, 1975)

Jika G adalah grup berhingga yang mempunyai order p bilangan prima, maka G merupakan grup siklik.

Teorema 2.2.2 Generator (Fraleigh & Katz, 2003)

Jika a adalah generator dari grup siklik berhingga G dengan order n, maka generator-generator lain dari G berbentuk a^r di mana r relatif prima dengan n.

Definisi 2.2.5 Subgrup (Fraleigh & Katz, 2003)

Diberikan grup $\langle G, * \rangle$. Jika $H \subset G$ tertutup dalam operasi biner $*$ dari grup G, dan jika $\langle H, * \rangle$ membentuk sebuah grup, maka H merupakan **subgrup** dari G. Dapat dinotasikan $H \leq G$ atau $G \geq H$. $H < G$ atau $G > H$ menyatakan bahwa $H \leq G$ namun $H \neq G$.

Definisi 2.2.6 Ring (Fraleigh & Katz, 2003)

Sebuah ring $\langle R, +, * \rangle$ adalah sebuah himpunan R dengan dua operasi biner penjumlahan $(+)$ dan perkalian $(*)$ pada R, sedemikian sehingga syarat-syarat berikut terpenuhi:

$\boldsymbol{\mathcal{R}_1}$**:** $\langle R, + \rangle$ adalah grup abelian.

$\boldsymbol{\mathcal{R}_2}$**:** Operasi perkalian bersifat asosiatif.

$\boldsymbol{\mathcal{R}_3}$**:** Untuk setiap $a, b, c \in R$, maka berlaku:

1. Sifat distributif kiri, $a * (b + c) = (a * b) + (a * c)$, dan;
2. Sifat distributif kanan, $(a + b) * c = (a * c) + (b * c)$.

Definisi 2.2.7 Ring Komutatif (Fraleigh & Katz, 2003)

Suatu ring R yang operasi perkaliannya bersifat komutatif disebut **ring komutatif**. Suatu ring yang mempunyai elemen identitas terhadap operasi perkalian disebut **ring dengan unsur kesatuan**. Elemen identitas terhadap perkalian $1 \in R$ disebut **unsur kesatuan**.

Definisi 2.2.8 Invers Perkalian (Fraleigh & Katz, 2003)

Invers perkalian dari suatu a anggota dari ring R dengan unsur kesatuan $1 \neq 0$ adalah $a^{-1} \in R$ sedemikian sehingga $a * a^{-1} = a^{-1} * a = 1$.

Definisi 2.2.9 Lapangan (Fraleigh & Katz, 2003)

Diberikan R suatu ring dengan uniti $1 \neq 0$. Sebuah $u \in R$ disebut **unit** dari R jika terdapat invers perkalian dari u. Jika setiap anggota dari $R \setminus \{0\}$ adalah **unit**, maka R disebut **ring pembagian**. Sebuah ring pembagian dengan operasi perkaliannya bersifat komutatif disebut dengan **lapangan**. Suatu lapangan yang mempunyai banyak anggota yang berhingga disebut dengan **lapangan berhingga**.

Definisi 2.2.10 Himpunan Bilangan Bulat Modulo m (Menezes, Oorschot, & Vanstone, 1996)

Untuk m bilangan bulat positif, himpunan bilangan bulat modulo m dinotasikan $\mathbb{Z}_m$, adalah himpunan kelas ekuivalensi dari bilangan bulat $\{0,1,2, \dots, m-1\}$, atau $\mathbb{Z}_m = \{\bar{0}, \bar{1}, \bar{2}, \dots, \overline{m-1}\}$.

Pada himpunan $\mathbb{Z}_m$ berlaku operasi penjumlahan modulo dan perkalian modulo m, yaitu $\forall\, a, b \in \mathbb{Z}_m$ maka $a + b = (a + b) \bmod m$ dan $a \cdot b = (a \cdot b) \bmod m$.

Definisi 2.2.11 Invers Perkalian Modulo m (Menezes, Oorschot, & Vanstone, 1996)

Diberikan $a \in \mathbb{Z}_m$. Invers perkalian dari a modulo m adalah suatu bilangan bulat $x \in \mathbb{Z}_m$ sedemikian sehingga $a \cdot x \equiv 1 \pmod m$. Jika ada x yang memenuhi maka x unik dan a dikatakan invertibel atau merupakan sebuah unit. Invers dari a dinotasikan a^{-1}.

Definisi 2.2.12 Pembagian Modulo m (Menezes, Oorschot, & Vanstone, 1996)

Diberikan $a, b \in \mathbb{Z}_m$. Pembagian a oleh b modulo m adalah perkalian dari a dan b^{-1} modulo m, jika b invertibel modulo m.

Definisi 2.2.13 Ring Bilangan Bulat Modulo m (Buchmann, 2004)

Jika m adalah bilangan bulat dengan $m > 1$, maka $(\mathbb{Z}_m, \cdot, +)$ adalah ring komutatif dengan unsur kesatuan $1 \in \mathbb{Z}_m$. Ring $\mathbb{Z}_m$ seperti ini disebut ring bilangan bulat modulo m.

Definisi 2.2.14 Grup Perkalian $\mathbb{Z}_m$ (Menezes, Oorschot, & Vanstone, 1996)

Grup perkalian $\mathbb{Z}_m$ adalah $\mathbb{Z}_m^* = \{\bar{a} \in \mathbb{Z}_m : \text{FPB}(a, m) = 1\}$. Jika m adalah prima maka $\mathbb{Z}_m^* = \{\bar{a} \mid \bar{1} \leq \bar{a} \leq \overline{m-1}\}$.

Teorema 2.2.3 Invers Modulo m (Buchmann, 2004)

Elemen $a \in \mathbb{Z}_m$ merupakan unit jika dan hanya jika $\text{FPB}(a, m) = 1$. Jika $\text{FPB}(a, m) = 1$, maka invers a tunggal.

Teorema 2.2.4 Teorema Euler (Menezes, Oorschot, & Vanstone, 1996)

Jika $a \in \mathbb{Z}_n^*$, maka $a^{\phi(n)} \equiv 1 \pmod{n}$.

Teorema 2.2.4 Order Grup $\mathbb{Z}_m$ (Buchmann, 2004)

Grup $\mathbb{Z}_m^*$ membentuk grup siklik dengan order $m - 1$.

2.3 Kurva Eliptik

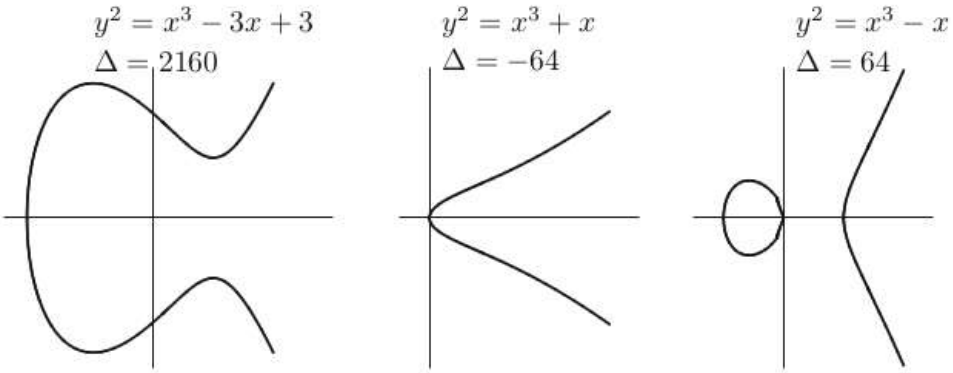
Definisi 2.3.1 Kurva Eliptik pada Bilangan Real (Stinson, 2006)

Diberikan $a, b \in \mathbb{R}$ sedemikian sehingga $4a^3 + 27b^2 \neq 0$. Sebuah kurva eliptik E adalah himpunan solusi yang terdiri atas pasangan-pasangan terurut $(x, y) \in \mathbb{R} \times \mathbb{R}$ yang memenuhi:

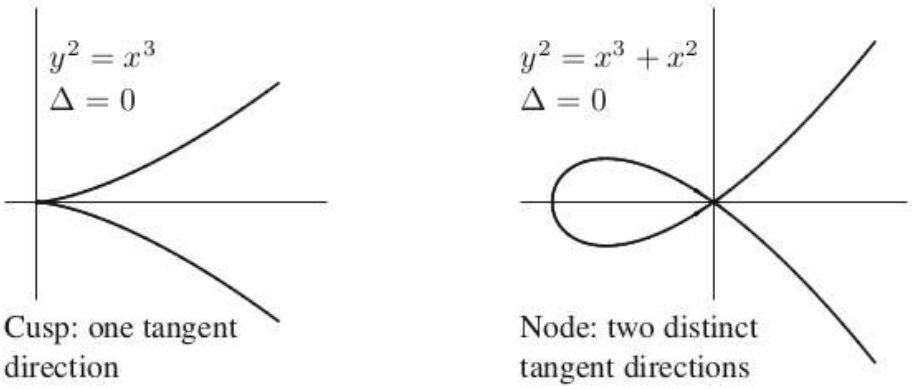
$$y^2 = x^3 + ax + b$$

bersama dengan titik khusus $\mathcal{O}$ yang disebut **titik infinity**.

Contoh-contoh kurva eliptik dapat dilihat pada gambar-gambar berikut.



Gambar 1.1 Kurva Eliptik



Gambar 1.2 Bukan Kurva Eliptik

Kurva eliptik E merupakan **grup Abelian** (Silverman, 2009, hal. 51-74; Hankerson, Menezes, & Vanstone, 2004), dengan operasi $\oplus$ (penjumlahan titik) yang didefinisikan sebagai berikut:

1. $\boldsymbol{\mathcal{O}}$ merupakan unsur identitas, sehingga $P \oplus \boldsymbol{\mathcal{O}} = \boldsymbol{\mathcal{O}} \oplus P = P$ untuk setiap $P \in E$.
2. Diberikan $P, Q \in E$, di mana $P = (x_1, y_1)$ dan $Q = (x_1, -y_1)$, maka $P \oplus Q = \boldsymbol{\mathcal{O}}$. Titik Q adalah unsur negatif dari P, dapat ditulis $-P$.
3. Diberikan $P, Q \in E$, di mana $P = (x_1, y_1)$, $Q = (x_2, y_2)$, $P \neq \boldsymbol{\mathcal{O}}$, $Q \neq \boldsymbol{\mathcal{O}}$, dan $Q \neq \pm P$, maka $P \oplus Q = R = (x_3, y_3)$ di mana:

   $$x_3 = \lambda^2 - x_1 - x_2$$

   dan

   $$y_3 = \lambda(x_1 - x_3) - x_2$$

   dengan

   $$\lambda = \frac{-y_3 - y_1}{x_3 - x_1}$$
4. Diberikan $P \in E$, di mana $P = (x_1, y_1)$, maka $P \oplus P = 2P = (x_3, y_3)$, disebut juga dengan penggandaan titik, di mana:

   $$x_3 = \lambda^2 - x_1 - x_3$$

   dan

   $$y_3 = \lambda^2(x_1 - x_3) - x_2$$

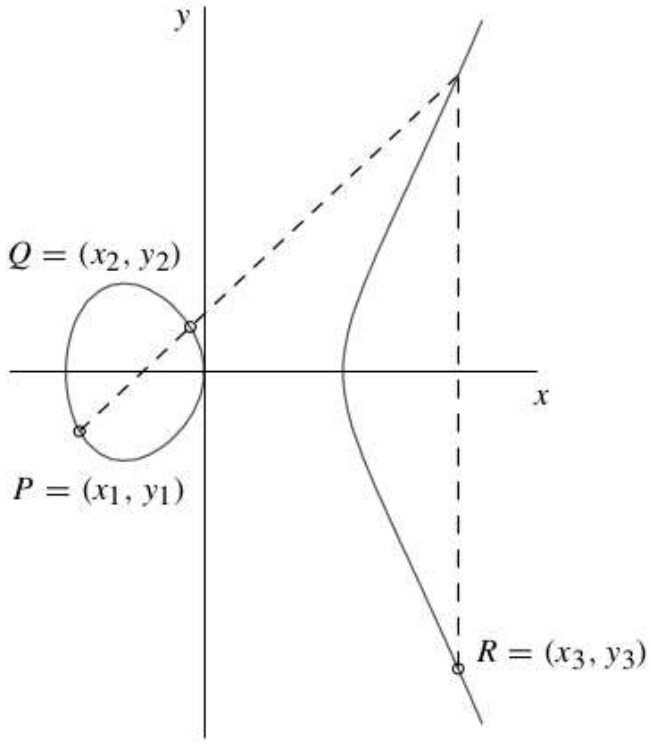
   dengan

   $$\lambda = \frac{3x_1^2 + a}{2y_1}$$

(Silverman, 2009; Stinson, 2006)

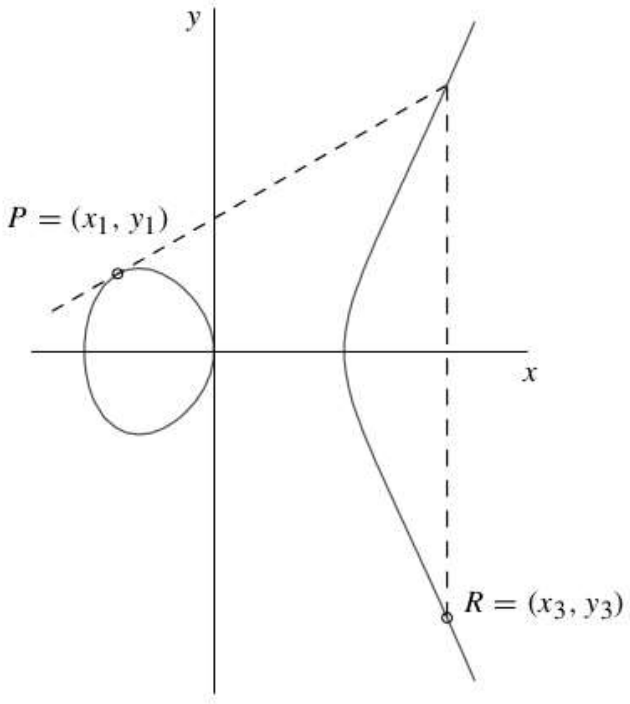
Secara geometris, operasi $\oplus$ dapat direpresentasikan dalam gambar berikut:

1. $R = P \oplus Q$ dengan $Q \neq \pm P$, $P \neq \boldsymbol{\mathcal{O}}$, $Q \neq \boldsymbol{\mathcal{O}}$



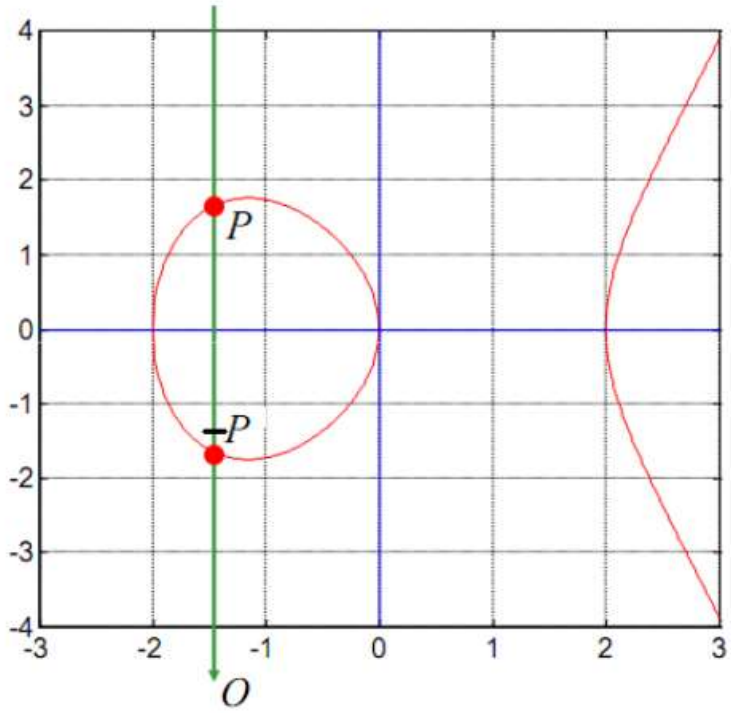
Gambar 1.3 Penjumlahan Titik

2. $R = P \oplus P$



Gambar 1.4 Penggandaan Titik

3. $R = P \oplus -P = \boldsymbol{\mathcal{O}}$



Gambar 1.5 Penjumlahan Titik dengan Inversnya

2.3.1 Kurva Eliptik Pada Lapangan $\mathbb{Z}_p$

Kurva eliptik dapat pula didefinisikan pada lapangan berhingga $\mathbb{Z}_p$ sebagai berikut.

Definisi 2.3.1.1 Kurva Eliptik Pada Lapangan $\mathbb{Z}_p$ (Stinson, 2006)

Diberikan $p > 3$ bilangan prima. Kurva eliptik $y^2 = x^3 + ax + b$ atas $\mathbb{Z}_p$ adalah himpunan solusi E yang terdiri atas pasangan-pasangan terurut $(x, y) \in \mathbb{Z}_p \times \mathbb{Z}_p$ yang memenuhi:

$$y^2 \equiv x^3 + ax + b \ (\textbf{mod}\ p)$$

di mana $a, b \in \mathbb{Z}_p$ memenuhi $4a^3 + 27b^2 \not\equiv 0 \ (\textbf{mod}\ p)$, bersama dengan titik khusus $\boldsymbol{\mathcal{O}}$ yang disebut **titik *infinity***.

Kurva eliptik pada lapangan $\mathbb{Z}_p$ membentuk **grup Abelian**, dengan operasi $\oplus$ (penjumlahan titik), yang didefinisikan sebagai berikut:

1. $\boldsymbol{\mathcal{O}}$ merupakan unsur identitas, sehingga $P \oplus \boldsymbol{\mathcal{O}} = \boldsymbol{\mathcal{O}} \oplus P = P$ untuk setiap $P \in E$.
2. Diberikan $P, Q \in E$, di mana $P = (x_1, y_1)$ dan $Q = (x_1, -y_1)$, maka $P \oplus Q = \boldsymbol{\mathcal{O}}$. Titik Q adalah unsur negatif dari P, dapat ditulis $-P$.
3. Diberikan $P, Q \in E$, di mana $P = (x_1, y_1)$, $Q = (x_2, y_2)$, $P \neq \boldsymbol{\mathcal{O}}$, $Q \neq \boldsymbol{\mathcal{O}}$, dan $Q \neq \pm P$, maka $P \oplus Q = R = (x_3, y_3)$ di mana:

   $$x_3 = \lambda^2 - x_1 - x_2 \ (\textbf{mod}\ p)$$

   dan

   $$y_3 = \lambda(x_1 - x_3) - x_2 \ (\textbf{mod}\ p)$$

   dengan

   $$\lambda = (-y_3 - y_1)(x_3 - x_1)^{-1}$$
4. Diberikan $P \in E$, di mana $P = (x_1, y_1)$, maka $P \oplus P = 2P = (x_3, y_3)$, disebut juga dengan penggandaan titik, di mana:

   $$x_3 = \lambda^2 - x_1 - x_3 \ (\textbf{mod}\ p)$$

   dan

   $$y_3 = \lambda^2(x_1 - x_3) - x_2 \ (\textbf{mod}\ p)$$

   dengan

   $$\lambda = (3x_1^2 + a)(2y_1)^{-1} \ (\textbf{mod}\ p)$$

(Silverman, 2009; Stinson, 2006)

Selain operasi penjumlahan, pada kurva eliptik pada lapangan $\mathbb{Z}_p$ dapat didefinisikan **multiplikasi titik** dengan aturan:

$$nP = \underbrace{P \oplus P \oplus P \oplus \cdots \oplus P}_{n}$$

dengan $n \in \mathbb{Z}$ dan $P \in E$.

Definisi 2.3.1.2 ***Elliptic Curve Disrete Logarithm Problem*** (Hankerson, Menezes, & Vanstone, 2004)

Elliptic Curve Discrete Logarithm Problem adalah sebagai berikut: diberikan sebuah kurva eliptik E atas lapangan berhingga $\mathbb{Z}_p$, sebuah titik $P \in E$ dengan order n dan sebuah titik $Q \in \langle P \rangle$ maka tentukan nilai bilangan bulat $l \in [0, n-1]$ sedemikian sehingga $Q = lP$. Bilangan bulat l disebut ***discrete logarithm* dari Q dengan basis P**, dinotasikan $l = \log_P Q$.

2.3.2 Kurva Eliptik P-256

Pada tahun 1999, *National Institute of Standards and Technology* (NIST) merilis daftar kurva-kurva eliptik yang direkomendasikan untuk digunakan dalam *Elliptic Curve Cryptography*. Salah satu kurva yang direkomendasikan adalah kurva P-256. Kurva eliptik P-256 dapat didefinisikan sebagai berikut.

Definisi 2.3.2.1 Kurva Eliptik P-256 (National Insitute of Standards and Technology, 1999)

Kurva eliptik P-256 adalah kurva eliptik E pada lapangan bilangan prima $\mathbb{Z}_p$ yang dihasilkan dari solusi-solusi persamaan

$$y^2 = x^3 - 3x + b \ (\mathbf{mod}\ p)$$

dengan

$$b = 41058363725152142129326129780047268409114$$
$$44101599372555483525631403946740129 1$$

dan

$$p = 11579208921035624876269744694940757353008614$$
$$34152903141955336313088670978539 51$$

dan

$$r = 11579208921035624876269744694940757352999695$$
$$52241357603424222590610685120443 69$$

merupakan order dari E. Untuk mempermudah implementasi, NIST memberikan sebuah titik $G = (G_x, G_y) \in E$ generator dari E, dengan

$$G_x = 48439561293906451759052585252797914202762949$$
$$52604174799584408071708240463528 6$$
$$G_y = 36134250956749795798585127919587881956611106$$
$$72985015071877198253568414405109$$

2.4 Kriptosistem

Definisi 2.4.1 Kriptosistem (Stinson, 2006)

Kriptosistem adalah 5-tuple $(\mathcal{P}, \mathcal{C}, \mathcal{K}, \mathcal{E}, \mathcal{D})$, yang memenuhi kondisi-kondisi berikut:

1. $\mathcal{P}$ adalah himpunan berhingga dari *plaintext*
2. $\mathcal{C}$ adalah himpunan berhingga dari *ciphertext*
3. $\mathcal{K}$ adalah *keyspace* yaitu himpunan berhingga dari kunci-kunci
4. Untuk setiap $K \in \mathcal{K}$, terdapat aturan enkripsi $e_K \in \mathcal{E}$ yang berkorespondensi dengan aturan dekripsi $d_K \in \mathcal{D}$. Setiap $e_K : P \to C$ dan $d_K : C \to P$ adalah suatu fungsi sedemikian sehingga $d_K(e_K(x)) = x$ untuk setiap $x \in \mathcal{P}$.

2.4.1 Kriptosistem RSA

Seperti yang telah disebutkan sebelumnya, kriptosistem RSA ditemukan oleh tiga orang peneliti dari Massachusetts Institute of Technology (MIT) yaitu Ron Rivest, Adi Shamir dan Leonard Adleman pada tahun 1977. Kriptosistem RSA termasuk ke dalam kriptografi asimetri dikarenakan kriptosistem ini menggunakan dua kunci yang berbeda untuk melakukan proses enkripsi dan dekripsi. Keamanan kriptosistem RSA didasarkan pada tingkat kesulitan untuk memfaktorkan suatu bilangan menjadi dua buah bilangan prima. Pembangkitan kunci menggunakan konsep algoritma pembagian dan bilangan prima. Kunci publik digunakan untuk mengenkripsi *plaintext* dan kunci privat digunakan untuk mendekripsi *ciphertext*. Kriptosistem RSA dapat didefinisikan sebagai berikut:

Definisi 2.4.1.1 Kriptosistem RSA (Stinson, 2006)

Diberikan $n = pq$, di mana p dan q merupakan bilangan prima. Diberikan $\mathcal{P} = \mathcal{C} = \mathbb{Z}_n$, didefinisikan:

$$\mathcal{K} = \{(n, p, q, a, b) : ab \equiv 1 \ (\mathbf{mod}\ \phi(n))\}$$

Untuk $K = (n, p, q, a, b)$, didefinisikan:

$$e_K(x) = x^b \ \mathbf{mod}\ n$$

dan

$$d_K(y) = y^a \ \mathbf{mod}\ n$$

dengan $x, y \in \mathbb{Z}_n$. Nilai-nilai n dan b membentuk kunci publik, dan nilai-nilai p, q dan a membentuk kunci privat.

Algoritma-algoritma yang digunakan dalam kriptosistem RSA adalah sebagai berikut:

Algoritma 2.4.1.1 Pembangkitan Kunci (Stinson, 2006)

OUTPUT: Kunci publik dan kunci privat

1. Bangkitkan dua buah bilangan prima p dan q dengan $p \neq q$
2. $n \leftarrow pq$ dan $\phi(n) \leftarrow (p-1)(q-1)$
3. Pilih bilangan prima acak b, $1 < b < \phi(n)$, sedemikian sehingga $\text{FPB}\big(b, \phi(n)\big) = 1$
4. $a \leftarrow b^{-1} \bmod \phi(n)$
5. Kunci publik adalah (n, b) dan kunci privat adalah (p, q, a)

Algoritma 2.4.1.2 Enkripsi (Menezes, Oorschot, & Vanstone, 1996)

SUMMARY: Bob mengenkripsi pesan m untuk Alice

1. Bob mendapatkan kunci publik Alice (n, b)
2. Representasikan pesan sebagai bilangan bulat m pada interval $[0, n-1]$
3. $y \leftarrow x^b \bmod n$
4. Kirimkan *ciphertext* y kepada Alice

Algoritma 2.4.1.3 Dekripsi (Menezes, Oorschot, & Vanstone, 1996)

SUMMARY: Alice mendekripsi *ciphertext* c yang Bob kirimkan

1. $x \leftarrow y^a \bmod n$
2. Ubah bilangan bulat x menjadi *plaintext* sebenarnya

Hasil dari proses dekripsi dapat dibuktikan merupakan *plaintext* sebagai berikut:

Karena $ab \equiv 1 \ (\textbf{mod}\ \phi(n))$, terdapat bilangan bulat k sedemikian sehingga $ab = 1 + k \cdot \phi(n)$. Perhatikan bahwa $m \in [0, n-1]$, dan p bilangan prima, akibatnya, $\text{FPB}(m, p) = 1$. Maka, berdasarkan teorema Fermat (Teorema 2.1.8),

$$m^{p-1} \equiv 1 \ (\textbf{mod}\ p) \Rightarrow m^{k(p-1)(q-1)} \equiv 1^{k(q-1)} \ (\textbf{mod}\ p) \equiv 1 \ (\textbf{mod}\ p)$$

$$\Rightarrow m \cdot m^{k(p-1)(q-1)} \equiv m \cdot 1 \ (\textbf{mod}\ p)$$

$$\Rightarrow m^{1+k(p-1)(q-1)} \equiv m \ (\mathbf{mod}\ p)$$

Di pihak lain, karena p dan q bilangan prima, maka berdasarkan Teorema 2.1.7, $\phi(n) = (p-1)(q-1)$. Akibatnya,

$$m^{ba} \equiv m \ (\mathbf{mod}\ p)$$

Dengan menggunakan teknik yang sama untuk q, diperoleh,

$$m^{ba} \equiv m \ (\mathbf{mod}\ q)$$

Sehingga, karena p dan q adalah bilangan-bilangan prima yang berbeda, dan $n = pq$, didapat

$$m^{ba} \equiv m \ (\mathbf{mod}\ n)$$

dan akibatnya,

$$c^a \equiv (m^b)^a \equiv m \ (\mathbf{mod}\ n)$$

■

Contoh proses pembangkitan kunci, enkripsi dan dekripsi pada kriptosistem RSA adalah sebagai berikut: Misalkan Alice ingin mengirimkan *plaintext* "PESAN". Alice memecah *plaintext* menjadi blok-blok *plaintext* berdasarkan karakter pada *plaintext*. Bob kemudian membangkitkan dua buah bilangan prima $p = 7$ dan $q = 13$, kemudian menghitung nilai $n = pq = 7 \cdot 13 = 91$ dan nilai $\phi(n) = (p-1)(q-1) = 6 \cdot 12 = 72$. Bob kemudian memilih suatu bilangan $b = 5$ yang relatif prima terhadap $\phi(n)$. Bob kemudian menghitung nilai $a = 29$ menggunakan algoritma Euclid yang diperluas. Maka diperoleh kunci publik Bob adalah $(91, 5)$ dan kunci privat Bob adalah $(7, 13, 29)$. Bob kemudian mengirimkan kunci publiknya kepada Alice. Alice kemudian merepresentasikan blok-blok *plaintext* sebagai bilangan bulat dengan menggunakan sistem ASCII. Maka *plaintext* menjadi blok-blok bilangan bulat:

$$x_1 = 80$$
$$x_2 = 69$$
$$x_3 = 83$$
$$x_4 = 65$$
$$x_5 = 78$$

yang berada pada interval $[0, n-1]$. Alice kemudian mengenkripsi blok-blok *plaintext* menggunakan kunci publik Bob. Blok-blok *ciphertext* hasil enkripsi adalah:

$$y_1 = 80^5 \pmod{91} = 19$$
$$y_2 = 69^5 \pmod{91} = 62$$
$$y_3 = 83^5 \pmod{91} = 83$$
$$y_4 = 65^5 \pmod{91} = 39$$
$$y_5 = 78^5 \pmod{91} = 78$$

Ciphertext yang didapat kemudian diubah menggunakan sistem ASCII menjadi "DC3>'SN". Alice kemudian mengirim *ciphertext* kepada Bob.

Bob kemudian melakukan dekripsi terhadap *ciphertext* yang ia terima dari Alice. Pertama, Bob merepresentasikan *ciphertext* menjadi bilangan bulat menggunakan sistem ASCII. Menggunakan kunci privat Bob, blok-blok plaintext hasil dekripsi adalah:

$$x_1 = 19^{29} \pmod{91} = 80$$
$$x_2 = 62^{29} \pmod{91} = 69$$
$$x_3 = 83^{29} \pmod{91} = 83$$
$$x_4 = 39^{29} \pmod{91} = 65$$
$$x_5 = 78^{29} \pmod{91} = 78$$

Plaintext yang didapat kemudian diubah menggunakan sistem ASCII sehingga didapat pesan asli yang berisi "PESAN".

2.4.2 *Elliptic Curve Cryptography*

Elliptic Curve Cryptography (ECC) diperkenalkan oleh Neal Koblitz dan Victor Miller pada tahun 1985. Keamanan skema-skema kriptografi yang bergantung pada ECC didasarkan pada sulitnya memecahkan *Elliptic Curve Discrete Logarithm Problem* (ECDLP). Sekarang ini, algoritma termangkus yang dapat menyelesaikan ECDLP mempunyai kompleksitas eksponensial, sementara itu algoritma termangkus untuk menyelesaikan masalah pemfaktoran bilangan bulat kompleksitasnya subeksponensial. Ini menyebabkan tingkat keamanan yang diinginkan dapat diperoleh menggunakan ukuran kunci yang lebih kecil

dibandingkan dengan kriptosistem RSA. ECC menggunakan kurva eliptik yang didefinisikan pada lapangan berhingga. Secara umum, implementasi ECC telah dilakukan menggunakan kurva eliptik pada lapangan berhingga $\mathbb{F}_{2^n}$ dan $\mathbb{Z}_p$. Pada penelitian ini digunakan kurva eliptik pada lapangan berhingga $\mathbb{Z}_p$.

2.4.3 Kriptosistem S-ECIES

Pada umumnya, skema ECC mengimplementasikan kriptosistem ElGamal pada sebuah kurva eliptik. Kriptosistem ECC ElGamal menggunakan titik-titik pada kurva eliptik E sebagai representasi *plaintext*. Sayangnya, sangat sulit untuk memetakan *plaintext* ke dalam titik-titik pada kurva eliptik E, dikarenakan belum adanya algoritma deterministik yang mangkus untuk membangkitkan titik-titik pada E (Stinson, 2006).

Kriptosistem S-ECIES (*Simplified* ECIES) merupakan simplifikasi dari kriptosistem *Elliptic Curve Integrated Encryption Scheme* (ECIES). S-ECIES lebih mudah diimplementasikan daripada ECC ElGamal, karena *plaintext* hanya disembunyikan (*masking*) pada titik-titik pada kurva eliptik E. Nilai x dari sebuah titik (x, y) pada kurva eliptik digunakan untuk *masking* sehingga *plaintext* tidak harus berada dalam kurva eliptik E.

Kriptosistem S-ECIES menggunakan *point compression* (kompresi titik) untuk meminimalisasi penggunaan memori yang digunakan untuk menyimpan titik pada kurva eliptik yang digunakan. Kompresi titik ini dapat dijabarkan sebagai berikut: Sebuah titik $P \neq \boldsymbol{\mathcal{O}}$ pada kurva eliptik E adalah pasangan terurut (x, y), di mana $y^2 = x^3 + ax + b$ (**mod** p). Jika diberikan nilai x, terdapat dua nilai y yang mungkin. Kedua nilai tersebut jika dijumlahkan modulo p menghasilkan 0 (**mod** p). Karena p ganjil, maka salah satu nilai yang mungkin adalah ganjil dan satunya lagi genap. Maka, dapat ditentukan sebuah titik yang unik $P = (x, y) \in E$ hanya dengan mengetahui nilai x dan y **mod** 2. Nilai $(x, y \bmod 2)$ inilah yang merupakan hasil kompresi titik dari (x, y) (Stinson, 2006).

Kompresi titik ini dapat mengurangi memori yang digunakan hingga hampir 50%, namun dengan kelemahan harus ditambahkan langkah komputasi untuk

merekonstruksi kembali y. Secara matematis, kompresi titik dapat didefinisikan sebagai berikut.

Definisi 2.4.3.1 Kompresi Titik (Stinson, 2006)

Kompresi titik adalah fungsi

$$\text{POINT-COMPRESS} : E \setminus \{\mathcal{O}\} \to \mathbb{Z}_p \times \mathbb{Z}_2$$

yang didefinisikan sebagai berikut:

$$\text{POINT-COMPRESS}(P) = (x, y \bmod 2), \text{ dengan } P = (x, y) \in E \setminus \{\mathcal{O}\}$$

Operasi dekompresi titik yang digunakan untuk merekonstruksi $P = (x, y) \in E$ dari $(x, y \bmod 2)$, dapat diimplementasikan sebagai algoritma berikut.

Algoritma 2.4.3.1 Dekompresi Titik (Stinson, 2006)

PROGRAM POINT-DECOMPRESS(x, i)
INPUT: (x, i)
OUTPUT: $P = (x, y) \in E$

$z \leftarrow x^3 + ax + b \bmod p$
if z adalah sebuah *quadratic non-residue* modulo p **then return** "Gagal"
else
    $y \leftarrow \sqrt{z} \bmod p$
    if $y \equiv i \bmod 2$ **then return** (x, y)
    else return $(x, p - y)$

Jika $p \equiv 3 \pmod 4$ dan z adalah *quadratic residue* modulo p atau $z = 0$, maka, berdasarkan kriteria Euler, $\sqrt{z}$ dapat dihitung sebagai $z^{\frac{p+1}{4}} \bmod p$ (Stinson, 2006).

Kriptosistem S-ECIES didefinisikan sebagai berikut.

Definisi 2.4.3.2 Kriptosistem S-ECIES (Stinson, 2006)

Diberikan E sebuah kurva eliptik pada lapangan $\mathbb{Z}_p$ ($p > 3$ bilangan prima) sedemikian sehingga terdapat $H = \langle P \rangle$ subgrup dari E dengan order n bilangan prima. Diberikan $\mathcal{P} = \mathbb{Z}_p^*$, $\mathcal{C} = \left(\mathbb{Z}_p \times \mathbb{Z}_2\right) \times \mathbb{Z}_p^*$, didefinisikan

$$\mathcal{K} = \{(E, P, m, Q, n) : Q = mP\}$$

Nilai-nilai P, Q dan n adalah kunci publik dan $m \in \mathbb{Z}_n^*$ adalah kunci privat.

Untuk $K = (E, P, m, Q, n)$, untuk sebuah bilangan bulat acak rahasia $k \in \mathbb{Z}_n^*$, dan untuk $x \in \mathbb{Z}_p^*$, didefinisikan fungsi enkripsi

$$e_K(x, k) = (\text{POINT-COMPRESS}(kP), xx_0 \bmod p)$$

di mana $kQ = (x_0, y_0)$ dan $x_0 \neq 0$.

Untuk *ciphertext* $y = (y_1, y_2)$, di mana $y_1 \in \mathbb{Z}_p \times \mathbb{Z}_2$ dan $y_2 \in \mathbb{Z}_p^*$, didefinisikan fungsi dekripsi

$$d_K(y) = y_2 \cdot (x_0)^{-1} \bmod p$$

di mana

$$(x_0, y_0) = m \cdot \text{POINT-DECOMPRESS}(y_1)$$

Contoh pembangkitan kunci, enkripsi dan dekripsi pada kriptosistem S-ECIES adalah sebagai berikut: Misalkan Alice ingin mengirimkan *plaintext* berupa bilangan bulat $x = 9$. Bob kemudian memilih kurva eliptik E yang didefinisikan sebagai himpunan (x, y) yang memenuhi $y^2 = x^3 + x + 6$ pada $\mathbb{Z}_{11}$. Perhatikan bahwa agar (x, y) memenuhi $y^2 = x^3 + x + 6 \pmod{11}$, berdasarkan Definisi 2.1.10 haruslah $x^3 + x + 6$ merupakan *quadratic residue* modulo 11. Perhatikan juga bahwa untuk $p \equiv 3 \pmod 4$, dapat ditentukan akar kuadrat dari sebuah *quadratic residue* modulo p sebagai berikut: Misalkan y adalah sebuah *quadratic residue* modulo p, dimana $p \equiv 3 \pmod 4$. Maka, menggunakan kriteria Euler (Teorema 2.1.9):

$$\begin{aligned}\left(\pm y^{\frac{p+1}{4}}\right)^2 &\equiv y^{\frac{p+1}{2}} \pmod p \\ &\equiv y^{\frac{p-1}{2}} \cdot y \pmod p \\ &\equiv y \pmod p\end{aligned}$$

menggunakan kongruensi ini, didapatkan akar-akar dari sebuah *quadratic residue* modulo p dengan $p \equiv 3 \pmod 4$ adalah $\pm y^{\frac{p+1}{4}} \pmod p$. Menggunakan rumus ini, didapat $y \equiv \pm(x^3 + x + 6)^{\frac{11+1}{4}} \pmod{11} \equiv \pm(x^3 + x + 6)^3 \pmod{11}$. Hasil (x, y) disajikan pada tabel berikut.

Tabel 1.1 Titik-titik Pada Kurva E

x	$x^3 + x + 6$	*Quadratic Residue* modulo 11	y
0	6	Tidak	
1	8	Tidak	
2	5	Ya	$4, 7$
3	3	Ya	$5, 6$
4	8	Tidak	
5	4	Ya	$2, 9$
6	8	Tidak	
7	4	Ya	$2, 9$
8	9	Ya	$3, 8$
9	7	Tidak	
10	4	Ya	$2, 9$

Karena $|E| = 13$ merupakan bilangan prima, maka berdasarkan Teorema 2.2.1, E merupakan grup siklik dan seluruh titik pada E kecuali $\boldsymbol{\mathcal{O}}$ merupakan generator dari E. Bob kemudian mengambil sebuah generator $P = (2, 7)$ dan sebuah bilangan bulat acak $m = 7 \in \mathbb{Z}_{13}$. Bob kemudian menghitung $Q = mP = 7(2, 7) = \underbrace{P \oplus P \oplus P \oplus \ldots \oplus P}_{7} = (7, 2)$. Maka diperoleh kunci publik Bob adalah $((2, 7), (7, 2), 13)$ dan kunci privat Bob adalah 7. Bob kemudian mengirimkan kunci publiknya kepada Alice. Alice kemudian memilih sebuah bilangan bulat acak $k = 6 \in \mathbb{Z}_{13}$. Alice kemudian menghitung nilai $(x_0, y_0) = kQ = 6(7, 2) = (8, 3)$. Alice kemudian mengenkripsi *plaintext* menggunakan kunci publik Bob. Hasil enkripsi adalah:

$$\begin{aligned} y &= (\text{POINT-COMPRESS}(kP), xx_0 \ \textbf{mod}\ p) \\ &= (\text{POINT-COMPRESS}\big(6(2, 7)\big), 9 \cdot 8 \ \textbf{mod}\ 11) \\ &= ((\text{POINT-COMPRESS}(7, 9), 6) \\ &= ((7, 1), 6) \end{aligned}$$

Alice kemudian mengirimkan *ciphertext* kepada Bob. Bob kemudian mendekripsi *ciphertext* menggunakan kunci privat Bob. Bob kemudian menghitung $(x_0, y_0) = m \cdot \text{POINT-DECOMPRESS}\big((7,1)\big) = 7 \cdot (7,9) = (8,3)$. Hasil dekripsi adalah:

$$\begin{aligned} x &= y_2 \cdot x_0^{-1} \pmod{p} \\ &= 6 \cdot 8^{-1} \pmod{11} \\ &= 9 \end{aligned}$$

Maka Bob mendapatkan pesan asli adalah $x = 9$.

2.5 Sistem ASCII

Sistem ASCII (*American Standard Code for Information Interchange*) atau **Kode Standar Amerika untuk Pertukaran Informasi** adalah suatu standar internasional dalam sistem pengodean huruf dan simbol yang bersifat universal. Dalam kriptografi, perhitungan yang dilakukan baik dalam proses enkripsi, dekripsi maupun pembangkitan kunci dilakukan menggunakan angka, sedangkan *plaintext* biasanya berbentuk teks atau tulisan. Sistem ASCII bertugas untuk mengodekan huruf dan simbol ke dalam bentuk angka.

Sistem ASCII memiliki komposisi 7 digit bilangan biner dimulai dari 0000000 hingga 1111111 yang ekuivalen dengan bilangan desimal 0 sampai 127, sehingga menyebabkan total kombinasi berjumlah 128 buah karakter. Dalam penelitian ini, sistem ASCII yang digunakan merupakan sistem *Extended* ASCII yang merupakan perluasan sistem ASCII dengan menambah jumlah digit menjadi 8. Hal ini menyebabkan total kombinasi menjadi 256 buah karakter. Lebih jelasnya dapat dilihat pada tabel ASCII yang ada di bagian lampiran.

2.6 Bahasa Pemrograman Python

Bahasa pemrograman Python dikembangkan oleh Guido van Rossum dan dirilis pertama kali pada tahun 1991. Python termasuk ke dalam bahasa pemrograman tingkat tinggi, yang berarti sintaks Python mendekati bahasa manusia. Python mendukung kompilasi kode sumber dan pemrograman *scripting* di mana kode dijalankan oleh interpreter tanpa harus dikompilasi terlebih dahulu. Python juga mendukung *object-oriented programming* dan memiliki GUI *toolkit* untuk merancang tampilan antarmuka program serta mendukung operasi-operasi

matematika dengan bilangan yang sangat besar. Kelebihan inilah yang menjadikan Python salah satu bahasa pemrograman yang paling populer saat ini. Saat ini, Python terdiri atasu dua versi rilis mayor yaitu versi 2.7.x dan 3.x.x dimana “x” merujuk pada versi rilis minor.