Modul 9: Teori Bilangan & Kriptografi

Keamanan Informasi, Aritmatika Modular, dan Enkripsi RSA

Kusuma Web

June 18, 2026

Fondasi Aritmatika Modular

Pembagian Integer & Modulo

Misalkan $a \in \mathbb{Z}$ dan $d \in \mathbb{Z}^+$. Pembagian a oleh d menghasilkan hasil bagi $q \in \mathbb{Z}$ dan sisa $r \in \mathbb{Z}$ unik sedemikian rupa sehingga:

$$a = d \cdot q + r \quad \text{di mana } 0 \leq r < d$$

Kita menuliskan $a \bmod d = r$. Sisa pembagian ini disebut operasi modulo.

Konsep Kongruensi Linier

Dua bilangan bulat a dan b dikatakan **kongruen modulo** m jika sisa pembagian keduanya oleh m bernilai sama, atau dengan kata lain m habis membagi $(a - b)$:

$$a \equiv b \pmod{m} \iff m \mid (a - b)$$

Sifat Aljabar Kongruensi: Jika $a \equiv b \pmod{m}$ dan $c \equiv d \pmod{m}$, maka:

- $a + c \equiv b + d \pmod{m}$

Algoritma Euclid & Balikan Modulo (Modular Inverse)

Pencarian FPB (GCD) - Algoritma Euclid

Prosedur rekursif tercepat untuk menghitung Faktor Persekutuan Terbesar (FPB) antara dua bilangan bulat besar berbasis modulo:

$$\text{FPB}(a, b) = \text{FPB}(b, a \bmod b) \quad \text{dengan basis } \text{FPB}(a, 0) = a$$

Balikan Perkalian Modular (Modular Multiplicative Inverse)

Balikan modulo dari a modulo m adalah bilangan bulat x sedemikian rupa sehingga:

$$a \cdot x \equiv 1 \pmod{m}$$

Balikan ini dipastikan **ada** jika dan hanya jika a dan m relatif prima ($\text{FPB}(a, m) = 1$). Balikan modulo dihitung secara efisien menggunakan **Extended Euclidean Algorithm**.

Teorema Teoretis: Fermat & Euler

Teorema Kecil Fermat (Fermat's Little Theorem)

Jika p adalah bilangan prima dan a adalah bilangan bulat yang tidak habis dibagi oleh p, maka:

$$a^{p-1} \equiv 1 \pmod{p}$$

Fungsi Totient Euler ($\phi(n)$)

$\phi(n)$ mendefinisikan jumlah bilangan bulat positif kurang dari n yang relatif prima dengan n.

- Jika p prima, maka $\phi(p) = p - 1$.
- Jika p dan q keduanya prima, maka $\phi(p \cdot q) = (p - 1)(q - 1)$.

Teorema Euler

Merupakan generalisasi dari Teorema Fermat. Jika FPB$(a, n) = 1$, maka:

$$a^{\phi(n)} \equiv 1 \pmod{n}$$

Aplikasi Utama: Algoritma Kriptografi RSA

Algoritma enkripsi kunci publik (asimetris) paling populer di dunia:

Algoritma Pembangkitan Kunci RSA

1. Pilih dua bilangan prima acak berukuran sangat besar, p dan q.
2. Hitung modulus kunci $n = p \cdot q$ dan fungsi totient $\phi(n) = (p-1)(q-1)$.
3. Pilih bilangan bulat e sebagai eksponen enkripsi dengan syarat $1 < e < \phi(n)$ dan $\text{FPB}(e, \phi(n)) = 1$.
4. Hitung kunci rahasia dekripsi d menggunakan Extended Euclid agar memenuhi $e \cdot d \equiv 1 \pmod{\phi(n)}$.
5. **Kunci Publik:** (e, n), **Kunci Privat:** (d, n).

Proses Enkripsi & Dekripsi

- **Enkripsi Pesan M menjadi Ciphertext C:** $C = M^e \bmod n$
- **Dekripsi Ciphertext C kembali menjadi M:** $M = C^d \bmod n$