Matematika Diskrit

Reza Pulungan

Jurusan Ilmu Komputer
Universitas Gadjah Mada
Yogyakarta

March 31, 2011

Teori Bilangan (Number Theory)

Keterbagian (Divisibility)

Pada bagian ini kita hanya akan berbicara mengenai bilangan bulat (integer).

Definisi (Divisibility)

Kita sebut a membagi (bulat) b jika terdapat sebuah integer k sedemikian sehingga $ak = b$, dan ini kita lambangkan dengan $a \mid b$.

Catatan Penting!

- *Setiap bilangan bulat membagi bulat 0.*
- *Jika $a \mid b$, maka b disebut kelipatan dari a.*

Keterbagian (Divisibility)

Lemma

Pernyataan-pernyataan berikut benar:

1. *Jika $a \mid b$, maka $a \mid bc$ untuk semua c.*
2. *Jika $a \mid b$ dan $b \mid c$, maka $a \mid c$.*
3. *Jika $a \mid b$ dan $a \mid c$, maka $a \mid (sb + tc)$ untuk semua s dan t.*
4. *Untuk semua $c \neq 0$, $a \mid b$ jika dan hanya jika $ca \mid cb$.*

Bukti: di papan tulis.

Definisi (Bilangan Prima)

Sebuah bilangan $p > 1$ yang tidak memiliki pembagi positif kecuali 1 dan dirinya sendiri disebut prima. Bilangan yang bukan prima disebut composite.

Keterbagian (Divisibility)

Bagaimana kalau satu bilangan tidak membagi bulat bilangan lain?

Teorema (Division Theorem)

Andaikan n dan b adalah integer dan $d > 0$. Maka terdapat sepasang integer unik q dan r sedemikian sehingga $n = qd + r$ dan $0 \leq r < d$.

Sisa r pada division theorem kita tuliskan dengan n **rem** d, ini melambangkan bahwa r adalah sisa (remainder) pembagian bulat antara n dengan d.

Linear Combination

Definisi (Kombinasi Linier Bulat)

Untuk sembarang integer a dan b, maka:

$$sa + tb,$$

di mana s dan r adalah integer, disebut kombinasi linier (bulat) dari a dan b.

Greatest Common Divisor (GCD)

Di Indonesia ini disebut dengan Faktor Persekutuan Terbesar.

Definisi (Greatest Common Divisor (GCD))

Greatest common divisor (GCD) dari a dan b adalah bilangan terbesar yang membagi bulat baik a maupun b, dan ini kita lambangkan dengan $gcd(a, b)$.

Teorema

Greatest common divisor dari a dan b sama dengan kombinasi linier positif yang terkecil dari a dan b.

Bukti: di papan tulis.

Corollary

Setiap kombinasi linier dari a dan b adalah kelipatan dari $gcd(a, b)$, dan sebaliknya.

Greatest Common Divisor (GCD)

Lemma

Pernyataan-pernyataan berikut benar:

1. *Setiap faktor persekutuan dari a dan b membagi bulat $gcd(a, b)$.*
2. $gcd(ka, kb) = k \cdot gcd(a, b)$ *untuk semua* $k > 0$.
3. *Jika* $gcd(a, b) = 1$ *dan* $gcd(a, c) = 1$, *maka* $gcd(a, bc) = 1$.
4. *Jika* $a \mid bc$ *dan* $gcd(a, b) = 1$, *maka* $a \mid c$.
5. $gcd(a, b) = gcd(b, a \textbf{ rem } b)$.

Bukti: di papan tulis.

Algoritma Euclid dan “The Pulverizer” (kuttak).

Teorema Fundamental Aritmetika

Lemma

Jika p bilangan prima dan $p \mid ab$, maka $p \mid a$ atau $p \mid b$.

Lemma

Andaika p bilangan prima. Jika $p \mid a_1 a_2 \cdots a_n$, maka p membagi bulat suatu a_i.

Teorema (Teorema Fundamental Aritmetika)

Setiap integer positif n dapat adalah perkalian unik dari beberapa bilangan prima.

Bukti: di papan tulis.

Aritmetika Modular

Definisi (Congruence)

Integer a congruent dengan b modulo n jika $n \mid (a - b)$, dan ini dilambangkan dengan $a \equiv b \pmod{n}$.

Catatan Penting!

- $\equiv$ *"mirip" dengan* $=$. $\pmod{n}$ *di atas menjelaskan "sense" di mana* a *dan* b *"sama".*
- *Congruence modulo* n *mendefinisikan sebuah partisi pada himpunan bilangan bulat ke* n *buah blok sedemikian sehingga integer-integer yang congruent berada di blok yang sama.*
- *Hasil akhirnya adalah bahwa ketika aritmetika dilakukan pada modulo* n*, maka hanya ada* n *jenis bilangan yang benar-benar berbeda yang perlu kita tangani.*

Sifat-Sifat Congruence

Lemma (Sifat-Sifat Congruence)

Pernyataan-pernyataan berikut berlaku untuk $n \geq 1$*:*

1. $a \equiv a \pmod{n}$.
2. $a \equiv b \pmod{n} \implies b \equiv a \pmod{n}$.
3. $a \equiv b \pmod{n} \wedge b \equiv c \pmod{n} \implies a \equiv c \pmod{n}$.
4. $a \equiv b \pmod{n} \implies a + c \equiv b + c \pmod{n}$.
5. $a \equiv b \pmod{n} \implies ac \equiv bc \pmod{n}$.
6. $a \equiv b \pmod{n} \wedge c \equiv d \pmod{n} \implies a + c \equiv b + d \pmod{n}$.
7. $a \equiv b \pmod{n} \wedge c \equiv d \pmod{n} \implies ac \equiv bd \pmod{n}$.

Bukti: di papan tulis.

Congruence dan Remainder

Lemma (Congruence dan Remainder)

Pernyataan-pernyataan berikut berlaku:

1. $a \equiv (a \textbf{ rem } n) \pmod{n}$.
2. $a \equiv b \pmod{n} \iff (a \textbf{ rem } n) = (b \textbf{ rem } n)$.

Bukti: di papan tulis.

Multiplicative Inverse

Definisi (Multiplicative Inverse)

Multiplicative inverse (Invers perkalian) dari suatu bilangan x adalah bilangan x^{-1} sedemikian sehingga $xx^{-1} = 1$.

Multiplicative inverse terdefinisi dengan baik untuk himpunan bilangan real, namun tidak untuk himpunan bilangan bulat.

Namun yang mengejutkan adalah multiplicative inverse terdefinisi dengan baik jika kita bekerja pada modulo p, di mana p adalah bilangan prima.

Lemma

Jika p adalah prima dan k bukan kelipatan dari p, maka k memiliki multiplicative inverse module p

Cancellation

Lemma

Andaikan p adalah prima dan k bukan kelipatan dari p, maka:

$$ak \equiv bk \pmod{p} \Longrightarrow a \equiv b \pmod{p}.$$

Bukti: di papan tulis.

Lemma

Andaikan p adalah prima dan k bukan kelipatan dari p, maka barisan:

$$(0 \cdot k) \textbf{ rem } p, (1 \cdot k) \textbf{ rem } p, (2 \cdot k) \textbf{ rem } p, \cdots, ((p-1) \cdot k) \textbf{ rem } p,$$

adalah permutasi dari barisan: $0, 1, 2, \cdots, (p-1)$.

Bukti: di papan tulis.

Fermat's Theorem

Teorema (Fermat's Theorem)

Andaikan p adalah prima dan k bukan kelipatan dari p, maka:

$$k^{p-1} \equiv 1 \pmod{p}.$$

Bukti: di papan tulis.

Relatively Prime dan Totient Function

Definisi (Relatively Prime)

Integer a dan b disebut relatively prime jika $gcd(a, b) = 1$.

Definisi (Totient Function)

Andaikan n adalah integer positif. Maka fungsi totient $\phi(n)$ melambangkan banyaknya integer dalam $\{0, 1, 2, \cdots, n-1\}$ yang relatively prime dengan n.

Sifat Totient Function

Teorema

Fungsi ϕ mematuhi hubungan berikut:

1. *Jika a dan b relatively prime, maka $\phi(ab) = \phi(a)\phi(b)$.*
2. *Jika p adalah prima, maka $\phi(p^k) = p^k - p^{k-1}$, untuk $k \geq 1$.*

Integer a dan b disebut relatively prime jika $gcd(a, b) = 1$.

Aritmetika Modulo Non-Prima

Lemma

Andaikan n adalah integer positif. Jika k relatively prime terhadap n, maka k memiliki multiplicative inverse module n. Dengan demikian terdapat k^{-1} sedemikian sehingga $kk^{-1} \equiv 1 \pmod{n}$.

Lemma

Andaikan n adalah integer positif dan k relatively prime terhadap n, maka:

$$ak \equiv bk \pmod{n} \Longrightarrow a \equiv b \pmod{n}.$$

Aritmetika Modulo Non-Prima

Lemma

Andaikan n adalah integer positif dan k relatively prime terhadap n. Andaikan $k_1, k_2, \cdots, k_r$ adalah semua integer yang relatively prime terhadap n di dalam $0 \leq k_i < n$, maka barisan:

$$(k_1 \cdot k) \textbf{ rem } n, (k_2 \cdot k) \textbf{ rem } n, (k_3 \cdot k) \textbf{ rem } n, \cdots, (k_r \cdot k) \textbf{ rem } n,$$

adalah permutasi dari barisan: $k_1, k_2, \cdots, k_r$.

Bukti: di papan tulis.

Aritmetika Modulo Non-Prima

Teorema (Euler's Theorem)

Andaikan n adalah integer positif dan k relatively prime terhadap n, maka:

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

Bukti: di papan tulis.