Introduction to Number Theory

Part B.

- Congruence
- Unique Factorisation

Nikenasih B, M.Si
Mathematics Educational Department
Faculty of Mathematics and Natural Science
State University of Yogyakarta

Contents all part

- Preliminary
- Divisibility
- Congruence
- Unique Factorisation
- Linear Diophantine Equation
- Arithmetic Functions

Congruence Definition

- Konsep kekongruenan bilangan dikembangkan berdasarkan konsep bahwa setiap bilangan bulat positif dapat dinyatakan ke dalam bentuk $N = pq + r$ atau $N - r = pq$ dengan p, q, r adalah bilangan bulat dan r berada pada $0 \leq r < p$. Persamaan $N = pq + r$ dengan p menyatakan pembagi, q menyatakan hasil bagi dan r menyatakan sisa.

- Persamaan di atas sering pula ditulis $N \equiv r \pmod{p}$
  (*dibaca N kongruen modulo p terhadap r*)
  Dari hal tersebut didapat definisi bahwa $a \equiv b \pmod{m}$
  jika $m \mid (a - b)$ untuk bilangan bulat a, b dan m.

- Contoh :
  - (1) $25 \equiv 1 \pmod{4}$ sebab $4 \mid 24$
  - (2) $1 \equiv -3 \pmod{4}$ sebab $4 \mid 4$

Congruence Properties 1

- Beberapa sifat berkaitan dengan modulo adalah sebagai berikut. Misalkan a, b, c, d dan m adalah bilangan-bilangan bulat dengan $d > 0$ dan $m > 0$, berlaku :
  i. $a \equiv a \pmod{m}$
  ii. Jika $a \equiv b \pmod{m}$ dan $b \equiv c \pmod{m}$ maka $a \equiv c \pmod{m}$
  iii. Jika $a \equiv b \pmod{m}$ dan $d|m$ maka $a \equiv b \pmod{d}$
  iv. Jika $a \equiv b \pmod{m}$ maka $a^k \equiv b^k \pmod{m}$ untuk semua k bilangan asli
  v. Jika $a \equiv b \pmod{m}$ dan $f(x) = a_n x^n + a_{n-1} x^{n-1} + \cdots + a_o$ maka $f(a) \equiv f(b) \pmod{m}$

Congruence Properties 2

Beberapa sifat berkaitan dengan modulu adalah sebagai berikut. Misalkan a, b, c, d dan m adalah bilangan-bilangan bulat dengan $d > 0$ dan $m > 0$, berlaku :

i. Jika $a \equiv b \pmod m$ dan $c \equiv d \pmod m$ maka $a + c \equiv b + d \pmod m$
ii. Jika $a \equiv b \pmod m$ dan $c \equiv d \pmod m$ maka $ac \equiv bd \pmod m$
iii. $(am + b)^k \equiv b^k \pmod m$ untuk semua k bilangan asli
iv. $(am + b)^k \cdot (cm + d)^n \equiv b^k \cdot d^n \pmod m$ untuk semua k dan n bilangan asli
v. Misalkan $n \in N$ dan S(n) adalah penjumlahan digit-digit dari n maka berlaku $n \equiv S(n) \pmod 9$.
vi. $n^5 \equiv n \pmod{10}$ untuk setiap $n \in N$.

Congruence

177 Example Find the remainder when 6^{1987} is divided by 37.

Solution: $6^2 \equiv -1 \mod 37$. Thus $6^{1987} \equiv 6 \cdot 6^{1986} \equiv 6(6^2)^{993} \equiv 6(-1)^{993} \equiv -6 \equiv 31 \mod 37$.

178 Example Prove that 7 divides $3^{2n+1} + 2^{n+2}$ for all natural numbers n.

Solution: Observe that $3^{2n+1} \equiv 3 \cdot 9^n \equiv 3 \cdot 2^n \mod 7$ and $2^{n+2} \equiv 4 \cdot 2^n \mod 7$. Hence

$$3^{2n+1} + 2^{n+2} \equiv 7 \cdot 2^n \equiv 0 \mod 7,$$

for all natural numbers n.

Unique Factorization

The Fundamental Theorem of Arithmetic

Every integer greater than 1 can be written uniquely in the form

$$p_1^{\alpha_1} p_2^{\alpha_2} \ldots p_k^{\alpha_k}$$

Where the p_i are distinct primes and the α_i are positive integers.

GCD and LCM

- The greatest common divisor of two positive integers a and b is the greatest positive integer that divides both a and b, which we denote by gcd(a, b), and similarly, the lowest common multiple of a and b is the least positive integer that is a multiple of both a and b, which we denote by lcm(a, b).
- We say that a and b are relatively prime if gcd(a, b) = 1.
- For integers a1, a2,. . . , an, gcd(a1, a2, . . . , an) is the greatest positive integer that divides all of a1, a2, . . . , an, and lcm(a1, a2, . . . , an) is defined similarly.

Useful Facts

- For all a, b, $\gcd(a,b) \cdot \operatorname{lcm}(a,b) = ab$.
- For all a, b, and m, $\gcd(ma,mb) = m\gcd(a,b)$ and $\operatorname{lcm}(ma,mb) = m\operatorname{lcm}(a,b)$.
- If $d \mid \gcd(a,b)$, then

$$\gcd\left(\frac{a}{d},\frac{b}{d}\right) = \frac{\gcd(a,b)}{d}.$$

In particular, if $d = \gcd(a,b)$, then $\gcd(a/d,b/d) = 1$; that is, a/d and b/d are relatively prime.

- If $a \mid bc$ and $\gcd(a, c) = 1$, then $a \mid b$.
- For positive integers a and b, if d is a positive integer such that $d \mid a$, $d \mid b$, and for any d', $d' \mid a$ and $d' \mid b$ implies that $d' \mid d$, then $d = \gcd(a, b)$. This is merely the assertion that any common divisor of a and b divides $\gcd(a, b)$.
- If $a_1 a_2 \cdots a_n$ is a perfect k^{th} power and the a_i are pairwise relatively prime, then each a_i is a perfect k^{th} power.
- Any two consecutive integers are relatively prime.

Theorem

Let *b*,*n* and *r* be positive integers, then

$$GCD(bn + r, n) = GCD(n, r)$$

As we had learned on secondary school that we can use prime factorization method to find the greatest common divisor of two integer *m* and *n*.

Using this Theorem, we can find the greatest common divisor of two integer *m* and *n* with another way.

Theorem

- Let m and n be positive integers where $0 < n < m$. From division algorithm, we know that there exist integers b and r such that

$$m = bn + r, 0 < r < n$$

Therefore

$$GCD(m, n) = GCD(bn + r, n) = GCD(n, r)$$

- Because *n* and *r* are positive integers where 0 < r < n, we know that there exist integers b_1 and r_1 such that

$$n = b_1 r + r_1,\ 0 < r_1 < r$$

- Therefore,

$$GCD(n, r) = GCD(b_1 r + r_1, r) = GCD(r, r_1)$$

- If we continu this process, then there exist integers $r_2, r_3, \ldots, r_s$ such that

$$GCD(m, n) = GCD(n, r) = GCD(r, r_1) = GCD(r_1, r_2) = \cdots = GCD(r_{s-1}, r_s) = r_s$$