DISCRETE MATHEMATICS AND APPLICATIONS

Number Theory 3

Intan Sabariah Sabri (intansabariah@ump.edu.my)
Siti Zanariah Satari (zanariah@ump.edu.my)
Adam Shariff Adli Aminuddin (adamshariff@ump.edu.my)

Faculty of Industrial Sciences & Technology

Chapter Description

- Chapter outline
  1.6 Euclidean Algorithm
  1.7 Extended Euclidean Algorithm
  1.8 Modular Arithmetic
- Aims
  – Find the Greatest Common Divisor of two integers by using Euclidean Algorithm
  – Find the linear equation between two numbers and their Greatest Common Divisor
  – Solve modular arithmetic problems

References

- Rosen K.H., Discrete Mathematics & Its Applications, (Seventh Edition), McGraw-Hill, 2011
- Epp S.S, Discrete Mathematics with Applications, (Fourth Edition), Thomson Learning, 2011
- Ram Rabu, Discrete Mathematics, Pearson, 2012
- Walls W.D., A beginner's guide to Discrete Mathematics, Springer, 2013
- Chandrasekaren, N. & Umaparvathi, M., Discrete Mathematics, PHI Learning Private Limited, Delhi, 2019

Euclidean algorithm

- Euclidean algorithm is another method to determine GCD
- This method is efficient than prime factorization especially if the given integers are large
- The algorithm steps is given as follows

  Step 1: Initialize. Let two integers a and b

  Step 2: If a>b, then use division algorithm to determine b=qa+r. Else a=qb+r

  Step 3: q will becomes new dividend and r becomes new divisor

  Step 4: Repeat Step 2 until r=0

  Step 5: The last divisor is the GCD(a,b)

Adam Shariff Adli Aminuddin
http://ocw.ump.edu.my/course/view.php?id=443

Euclidean algorithm: Example

Determine GCD(190,34) by using Euclidean algorithm.

Let a =190 and b = 34. As 34<190 then,

divide 190 by 34,	$190 = 5(34) + 20$
divide 34 by 20,	$34 = 1(20) + 14$
divide 20 by 14,	$20 = 1(14) + 6$
divide 14 by 6,	$14 = 2(6) + 2$
divide 6 by 2,	$6 = 3(2) + 0$, r=0 STOP

2 is the last divisor

GCD(190,34)=2

Extended Euclidean Algorithm

Theorem

Let a and b be positive integers, then there exist integers s and t such that

$$GCD(a,b)=sa+tb$$

The theorem states that the GCD for a and b can be expressed as a linear combination of a and b

Adam Shariff Adli Aminuddin

http://ocw.ump.edu.my/course/view.php?id=443

Extended Euclidean Algorithm: Example

Express gcd(252, 198) = 18 as a linear combination of 252 and 198.

Use Euclidean algorithm first to produce these linear equations

252 = 1(198) + 54

198 = 3(54) + 36

54 = 1(36) + 18

36 = 2(18)

Adam Shariff Adli Aminuddin
http://ocw.ump.edu.my/course/view.php?id=443

Extended Euclidean Algorithm: Example

$54 = 252 – 1(198)$

$36 = 198 – 3(54)$

$= 198 – 3[252-1(198)]$

$= 198 – 3(252) +3(198)$

$= 4(198) – 3(252)$

$18 = 54 – 1(36)$

$= 252 – 1(198) -1[4(198)-3(252)]$

$= 252 – 198 – 4(198) + 3(252)$

$= 4(252) – 5(198)$

Thus, $18 = 4(252) – 5(198)$

Adam Shariff Adli Aminuddin
http://ocw.ump.edu.my/course/view.php?id=443

Modular arithmetic

In some real life situation which involves repeated trend or cycle of a process, we can represent it by using modular arithmetic. Modular arithmetic only concern on the calculation of the remainder only. For example:

If the time is now 9 o'clock, what time will it be 100 hours from now?

Let 9 + 100 = 109 and we use 24 hour system. Therefore the divisor will be 24

109 = 4(24) + 13

The remainder is 13

In 100 hours it will be 1300 or 1 p.m

Adam Shariff Adli Aminuddin

Modular arithmetic: Example

a) 17 mod 3

$$17 = 5(3) + 2$$

$$r = 2$$

b) 133 mod 9

$$-133 = -15(9) + 2$$

$$r = 2$$

c) 2004 mod 101

$$2004 = 19(101) + 85$$

$$r = 85$$

d) 29 mod 5

$$29 = 5(5) + 4$$

$$r = 4$$

Adam Shariff Adli Aminuddin

Congruence

$$m = qn + r$$

$$m \not\equiv r \pmod{n}$$

m and r not congruent modulo n

$$m \equiv r \pmod{n}$$

$$m \bmod n = r \bmod n$$

congruent to r modulo n

$$n \mid (m - r)$$

n is modulus

Example

a) $29 = 5(5) + 4 \Rightarrow 29 \equiv 4 \pmod{5}$

b) $3 = 0(6) + 3 \Rightarrow 3 \equiv 3 \pmod{6}$

Mod-n Function

For each $n \in Z^{+}$, we define a function f_n, the mod-n function, as follows: If z is a nonnegative integer, then

$$f_n(z) = r, \text{ with } z = r(\text{mod } n) \text{ and } 0 \le r < n.$$

Example:

$f_3(16) = 1$ because 16 = 5(3) + 1 and $16 \equiv 1(\text{mod } 3)$

$f_7(156) = 2$ because 156 = 22(7) + 2 and $156 \equiv 2(\text{mod } 7)$

$f_3(14) = 2$ because 14 = 4(3) + 2 and $14 \equiv 2(\text{mod } 3)$

$f_7(153) = 6$??????

- If f is the mod-7 function, solve $f(z) = 2$.

Solution:

$$f_7(z) = 2 \Leftrightarrow z \equiv 2 \pmod 7$$
$$\Leftrightarrow z = q(7) + 2$$

$$\text{if } q = 0; \quad z = 0(7) + 2 = 2$$
$$\text{if } q = 1; \quad z = 1(7) + 2 = 9$$
$$\text{if } q = 2; \quad z = 2(7) + 2 = 16$$
$$\text{if } q = 3; \quad z = 3(7) + 2 = 23$$

Therefore, the solution of $f(z) = 2$ is $\{2, 9, 16, 23, \ldots\}$