Problem Sets

Number Theory (เลือกทำระหว่างข้อคู่หรือข้อคี่)

1. จงแสดงวิธีทำและหาค่าดังต่อไปนี้

    a. (177 **mod** 31 + 270 **mod** 31) **mod** 31

    b. (177 **mod** 31 * 270 **mod** 31) **mod** 31

    c. (−133 **mod** 23 + 261 **mod** 23) **mod** 23

    d. $(893 \textbf{ mod } 79)^4$ **mod** 26

2. จงอ่านค่านาฬิกาแบบ 12 ชั่วโมง เมื่อเวลาผ่านไป 100 ชั่วโมงหลังจากเวลา 6:00

3. จงอ่านค่านาฬิกาแบบ 24 ชั่วโมง เมื่อเวลาผ่านไป 168 ชั่วโมงหลังจากเวลา 19:00

4. จงหาเลขจำนวนเต็มมา 5 จำนวนที่ congruent กับ 4 modulo 12

5. จงหาเลขจำนวนเต็มทุกจำนวนระหว่าง −100 และ 100 ที่ congruent กับ −1 modulo 25

6. จงแปลงเลขฐาน 2 ของ $(1\ 0101\ 0101)_2$ เป็นฐาน 10

7. จงแปลงเลขฐาน 16 ของ $(ABBA)_{16}$ เป็นฐาน 2

8. จงบรรยายวิธีการแปลงเลขฐาน 8 เป็นเลขฐาน 16

9. จงแสดงวิธีทำโดยการใช้ Modular exponentiation ในการหาค่า 7^{129} **mod** 99

10. จงแสดงวิธีทำโดยการใช้ Fast Modular exponentiation ในการหาค่า 71^{767} **mod** 3120

11. จงแสดงให้เห็นว่าเลข 251 เป็นจำนวนเฉพาะโดยใช้วิธี Trial division

12. จงหาค่าที่ได้จากการแยกตัวประกอบเฉพาะ (Prime factorisation) ของ 126 และ 729

13. มีเลขจำนวนเต็มบวกใดบ้างที่มีค่าน้อยกว่า 30 และเป็นจำนวนเฉพาะสัมพัทธ์ (Relatively Prime) กับเลข 30

14. จงหา หารร่วมมาก (หรม หรือ gcd) ของคู่จำนวนเต็มต่อไปนี้

    a. $3^7 * 5^3 * 7^3$, $2^{11} * 3^5 * 5^9$

    b. 11 * 13 * 17 , $2^9 * 3^7 * 5^5 * 7^3$

    c. 23^{31}, 23^{17}

    d. 41 * 43 * 53, 41 * 43 * 53

    e. $3^{13} * 5^{17}$, $2^{12} * 7^{21}$

    f. 1111, 0

15. จงใช้ Euclidean algorithm ในการหาค่าดังต่อไปนี้

    a. gcd(111, 201)

    b. gcd(1001, 1331)

c. gcd(12345, 54321)

16. จงหาลำดับของ Pseudorandom numbers ที่ได้จาก Linear congruential generator จากสูตร $x_{n+1} = (3x_n+2)$ **mod** 13 และค่า seed $x_0 = 1$

เลขบัตรประชาชนในประเทศไทยมีจำนวน 13 หลัก $x_1x_2...x_{13}$

- 12 หลักแรกมีไว้ระบุตัวบุคคล
- หลักสุดท้าย x_{13} คือ check digit ที่เข้าสมการข้างล่างนี้

$$s = \sum_{i=1}^{12}(14 - i)x_i \ mod \ 11$$

$$x_{13} = 1 - s, \ if \ s \leq 1$$

$$x_{13} = 11 - s, \ if \ s > 1$$

17. จงหา Check digit ของเลขบัตรดังต่อไปนี้

    i. 5-6500-83524-44-?

    ii. 4-9101-98734-02-?

18. จงตรวจสอบว่าเลขดังต่อไปนี้ ถูกต้องหรือไม่

    i. 9-4096-73431-39-3

    ii. 6-8030-53463-10-7

Cryptography (เลือกทำระหว่างข้อคู่หรือข้อคี่)

19. จงเข้ารหัสข้อความ “DO NOT PASS” โดยการแปลงตัวหนังสือเป็นตัวเลขตาม encryption function ที่กำหนดดังต่อไปนี้ จากนั้นทำการแปลงตัวเลขกลับเป็นตัวอักษรที่เข้ารหัสแล้ว

    a. Caesar cipher

    b. f(p) = (p + 13) mod 26

    c. f(p) = (3p + 7) mod 26

20. จงถอดรหัสข้อความที่เข้ารหัสไว้ “CEBBOXNOB XYG” โดยใช้ Shift cipher ที่มีค่า f(p) = (p + 10) **mod** 26

21. จงถอดรหัสข้อความที่เข้ารหัสไว้ “DY CVOOZ ZOBMRKXMO DY NBOKW” โดยใช้ Shift cipher ที่มีค่า f(p) = (p + k) **mod** 26 ให้ใช้สมมติฐานในการหาค่า k โดยดูจากตัวอักษรที่ใช้บ่อยที่สุดในภาษาอังกฤษ

22. จงเขียน Shift ciphers ในรูปของ Cryptosystem

23. จงเข้ารหัสข้อความ “UPLOAD” โดยใช้ RSA system ที่มีค่า n = 53 * 61 และ e = 17.

    a. แปลงตัวอักษรเป็นเลขจำนวนเต็มก่อนแล้วจึงจับกลุ่ม โดยที่กลุ่มหนึ่งกลุ่มมีตัวเลข 4 ตัว

24. จงหาข้อความต้นฉบับโดยใช้ RSA system ที่มีค่า n = 43 * 59 และ e = 13 โดยที่ข้อความที่เข้ารหัสไว้คือ 0667 1947 0671

a. ในการถอดรหัส ตัว decryption exponent (d) คือค่า inverse ของ e = 13 modulo 42 * 58 = 937

Counting (เลือกทำระหว่างข้อคู่หรือข้อคี่)

25. จงหาจำนวนครั้งของ Print ใน algorithm ข้างล่างนี้

```
for i := 1 to n
    for j := 1 to n
        print "hello"
    for k := 1 to n
        print "hello"
```

26. นักศึกษาแต่ละคนถูกจำแนกอยู่ในชั้นปีที่ 1, 2, 3 หรือ 4 จงหาจำนวนนักศึกษาขั้นต่ำที่จะทำให้มีอย่างน้อย 8 คนที่อยู่ในชั้นปีเดียวกัน

27. ไพ่หนึ่งสำรับจะมีจำนวน 52 ใบ ประกอบด้วยไพ่ 4 ชุด ชุดละ 13 ใบ แต่ละชุดจะมีสัญลักษณ์ได้แก่ โพดำ โพแดง ข้าวหลามตัด และดอกจิก ในชุด 13 ใบ ประกอบด้วยตัวเลข 2 ถึง 10 และมี J (jack) Q (queen หรือ แหม่ม) K (king) A (ace) จงหาจำนวนไพ่ขั้นต่ำที่ต้องจั่วจากสำรับเพื่อให้ได้

    a. อย่างน้อย 3 ใบจาก 1 ชุด

    b. อย่างน้อย 3 aces

    c. Ace ข้าวหลามตัด

28. จงแสดงให้เห็นว่ามีอย่างน้อย 6 คนในรัฐ California ที่มีประชากร 37 ล้านคน มีชื่อที่ขึ้นต้นด้วย 3 ตัวอักษรที่เหมือนกัน และเกิดในวันเดียวกันของปี (ไม่จำเป็นต้องเป็นปีเดียวกัน)

a. ให้สมมติว่าชื่อทุกคนขึ้นต้นด้วย 3 ตัวอักษร และ 1 ปีมี 366 วัน

29. จงแสดงให้เห็นว่ามีอย่างน้อย 6 คนในรัฐ California ที่มีประชากร 37 ล้านคน มีชื่อที่ขึ้นต้นด้วย 3 ตัวอักษรที่เหมือนกัน และเกิดในวันเดียวกันของปี (ไม่จำเป็นต้องเป็นปีเดียวกัน)

30. จงหาค่าของแถวใน Pascal's triangle ที่มีค่า binomial coefficients $C(9, k)$, $0 \le k \le 9$

31. ให้ $b_n = 2b_{n-1} + n - 2^n$ and $b_0 = 5$ จงแสดงความสัมพันธ์ของ

    a. b_{n-1} ในรูปของ b_{n-2}

    b. b_n ในรูปของ b_{n-2}

    c. b_n ในรูปของ b_{n-3}

32. จงหาสมการของความสัมพันธ์เวียนเกิด (Recurrence Relation) $a_n = 2a_{n-1} + 2^n$, $a_0 = 1$ โดยใช้ recursive method

33. นางสาว P มีเงินเริ่มต้น 1000 บาท นางสาว P ลงทุนและได้ผลตอบแทน 5% ต่อปี (ดอกเบี้ยทบต้น หรือ Compound Interest) แต่ตอนท้ายปีทุกครั้งจะทำการถอนเงิน 100 บาท หลังจากที่ได้รับดอกเบี้ย ตัวอย่างเช่น สิ้นปีที่ 1 จำนวนเงินที่คงเหลือคือ 1000 + 0.05(1000) – 100 = 950

    a. จงสร้าง ความสัมพันธ์เวียนเกิด (Recurrence Relation) และเงื่อนไขเริ่มต้น (Initial condition) สำหรับจำนวนเงินที่นางสาว P ควรมีหลังจากเวลาผ่านไป n ปี

        i. นิยามให้ a_0 และ a_n โดยที่ a_n สำหรับ $n > 0$ เป็นจำนวนเงินในบัญชีคงเหลือ ณ สิ้นปี n

b. นางสาว P จะมีจำนวนเงินเหลือในบัญชีเท่าไรหลังจากที่ถอนเงิน 100 บาท ณ สิ้นปีที่ 3

c. จงสร้างสมการสำหรับ a_n ที่ไม่รวม ความสัมพันธ์เวียนเกิด (หรือ a_n) ในฝั่งขวาของสมการ

i. $$a + ar + ar^2 + ar^3 + \cdots + ar^{n-1} = \sum_{k=0}^{n-1} ar^k = a\left(\frac{1-r^n}{1-r}\right),$$

d. ใช้สมการที่ได้จากข้อที่แล้วในการหาว่าต้องใช้เวลากี่ปีก่อนที่จะถอนเงินจนเหลือ 0 บาท

34. จงหาจำนวนเต็มตั้งแต่ 1 ถึง 400 ที่

a. หารด้วย 6 ลงตัว

b. หารด้วย 6 ไม่ลงตัว

c. หารด้วย 7 และ 9 ไม่ลงตัว

d. หารด้วย 7 หรือ 9 ไม่ลงตัว

35.มีจำนวนสมาชิกเท่าไรใน $A_1 \cup A_2$ ถ้า A_1 มีสมาชิก 12 ตัว และ A_2 มีสมาชิก 18 ตัวและ

a. $A_1 \cap A_2 = \varnothing$

b. $|A_1 \cap A_2| = 6$

c. $A_1 \subseteq A_2$

36. แบบสำรวจครัวเรือนในประเทศไทยเปิดเผยว่า ประชากร 96% มีทีวีอย่างน้อย 1 ตัว, 98% มีโทรศัพท์ในบ้าน และ 95% มีทั้งทีวีอย่างน้อย 1 ตัวและมีโทรศัพท์ในบ้าน จงหาว่ามีกี่ % ที่ไม่มีทั้งทีวีและโทรศัพท์บ้าน

Relations (เลือกทำ 7 ข้อ)

37. จงเขียนคู่อันดับทั้งหมดใน relation R จาก A = {0,1,2,3,4} ไปยัง B={0,1,2,3}, โดยที่ (a, b) ∈ R เมื่อ

    a. a = b.

    b. a + b = 4.

    c. a > b.

    d. a | b.

    e. gcd(a, b) = 1.

    f. lcm(a, b) = 2.

38. จงเขียนคู่อันดับทั้งหมดใน relation R = {(a, b) | a divides b} บน set {1,2,3,4,5,6}

    a. แสดงความสัมพันธ์เชิงกราฟ

    b. แสดงความสัมพันธ์ในรูปตาราง

39. จากความสัมพันธ์ R บน set {1, 2, 3, 4} จงหาว่ามีคุณสมบัติ reflexive, symmetric, antisymmetric, transitive หรือไม่

    a. {(2,2),(2,3),(2,4),(3,2),(3,3),(3,4)}

    b. {(1,1),(1,2),(2,1),(2,2),(3,3),(4,4)}

    c. {(2,4),(4,2)}

    d. {(1,2),(2,3),(3,4)}

e. {(1,1),(2,2),(3,3),(4,4)}

f. {(1,3),(1,4),(2,3),(2,4),(3,1),(3,4)}

40. จากความสัมพันธ์ R บน set ของทุกคน จงหาว่ามีคุณสมบัติ reflexive, symmetric, antisymmetric, transitive หรือไม่

a. นาย a สูงกว่านาย b

b. นาย a กับนาย b เกิดวันเดียวกัน

41. จากความสัมพันธ์ R บน set ของจำนวนจริงทุกตัว จงหาว่ามีคุณสมบัติ reflexive, symmetric, antisymmetric, transitive หรือไม่

a. $x + y = 0$.

b. $x = \pm y$.

c. $x = 2y$.

d. $xy \geq 0$.

e. $xy = 0$.

f. $x = 1$.

g. $x = 1$ or $y = 1$

42. จงแสดงความสัมพันธ์เหล่านี้บนเซต {1, 2, 3} ด้วย matrix

a. {(1, 1), (1, 2), (1, 3)}

b. {(1, 2), (2, 1), (2, 2), (3, 3)}

c. {(1, 1), (1, 2), (1, 3), (2, 2), (2, 3), (3, 3)}

d. {(1, 3), (3, 1)}

e. จงวาด directed graph ของแต่ละความสัมพันธ์ในข้อ a, b, c, d.

43. จงเขียนคู่อันดับทั้งหมดในความสัมพันธ์บนเซต {1, 2, 3} ที่สอดคล้องกับ matrix ดังต่อไปนี้

a) $\begin{bmatrix} 1 & 0 & 1 \\ 0 & 1 & 0 \\ 1 & 0 & 1 \end{bmatrix}$ **b)** $\begin{bmatrix} 0 & 1 & 0 \\ 0 & 1 & 0 \\ 0 & 1 & 0 \end{bmatrix}$

c) $\begin{bmatrix} 1 & 1 & 1 \\ 1 & 0 & 1 \\ 1 & 1 & 1 \end{bmatrix}$

44. ให้ R เป็นความสัมพันธ์ที่แสดงด้วย matrix ดังนี้

$$\mathbf{M}_R = \begin{bmatrix} 0 & 1 & 0 \\ 0 & 0 & 1 \\ 1 & 1 & 0 \end{bmatrix}.$$

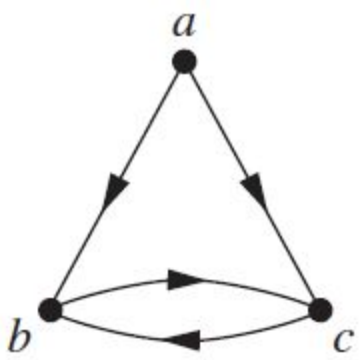
จงเขียน matrix ที่ได้จาก

a. R^2

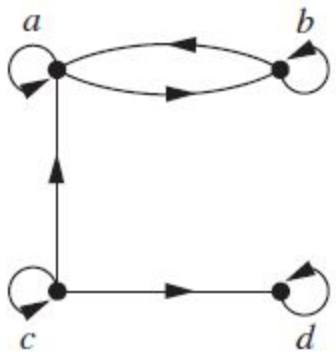
b. R^3

c. R^4

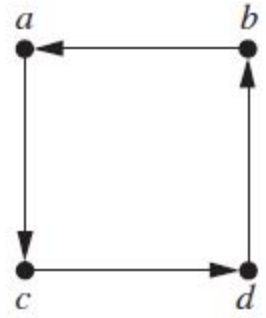
45. จงเขียนคู่อันดับทั้งหมดของความสัมพันธ์ที่แสดงอยู่ใน directed graphs และ จงหาว่ามีคุณสมบัติ reflexive, symmetric, antisymmetric, transitive หรือไม่



a.



b.



c.