Program Studi Teknik Informatika
Sekolah Teknik Elektro dan Informatika
Institut Teknologi Bandung

Nama :…………………………
NIM :…………………………
T.tangan:…………………………

Solusi Kuis ke-3 IF1220 Matematika Diskrit (3 SKS) – Teori Bilangan & Kombinatorika
Dosen: Rinaldi Munir, Rila Mandala, Arrival Dwi Sentosa
Selasa, 26 November 2024
Waktu: 60 menit

1. Di sebuah pesta komunitas seni, panitia ingin membagi semua tamu yang hadir ke dalam kelompok-kelompok untuk berpartisipasi dalam berbagai kegiatan. Namun, pembagian kelompok ini harus memenuhi beberapa aturan unik berdasarkan kebutuhan acara, yaitu: **(NILAI = 20)**

- Jika para tamu dibagi menjadi kelompok yang berisi **7 orang**, maka akan ada **3 orang tersisa** yang tidak masuk kelompok.
- Jika para tamu dibagi menjadi kelompok yang berisi **5 orang**, maka akan ada **2 orang tersisa**.
- Jika para tamu dibagi menjadi kelompok yang berisi **9 orang**, maka akan ada **4 orang tersisa**.

Panitia mengetahui bahwa jumlah tamu di pesta tersebut lebih dari **50 orang**, tetapi tidak lebih dari **200 orang**. Berapa jumlah tamu yang hadir di dalam pesta tersebut?

Jawaban:

Berdasarkan soal didapatkan persamaan sebagai berikut:

$x \equiv 3 \ (mod\ 7)\ ;\ a1 = 3$

$x \equiv 2 \ (mod\ 5)\ ;\ a2 = 2$

$x \equiv 4 \ (mod\ 9)\ ;\ a3 = 4$

$m = 7.5.9 = 315$

$M1 = 5.9 = 45$

$M2 = 7.9 = 63$

$M3 = 7.5 = 35$

$y1 = 5$ karena $45.5 \equiv 1 \ (mod\ 7)$

$y2 = 2$ karena $63.2 \equiv 1 \ (mod\ 5)$

$y3 = 8$ karena $35.8 \equiv 1 \ (mod\ 9)$

$x = a1.M1.y1 + a2.M2.y2 + a3.M3.y3 \ (mod\ m)$

$x = 3.45.5 + 2.63.2 + 4.35.8 \ (mod\ 315)$

$x = 3.45.5 + 2.63.2 + 4.35.8 \ (mod\ 315)$

$x = 2047 \ (mod\ 315)$

$x = 2047 \ (mod\ 315)$

$x = 157$

(Hanya ada satu kemungkinan solusi, yaitu 157 karena 157 + 315 >= 200 dan 157 - 315 <= 50)

2. Diberikan sistem kekongruenan linear berikut. Berapakah sisa pembagian X oleh 120?
Petunjuk: Untuk memudahkan perhitungan, sederhanakan sistem kekongruenan diatas terlebih dahulu! **(NILAI: 20)**

$$\begin{cases} X \equiv 8 \pmod{9} \\ X \equiv 15 \pmod{16} \\ X \equiv 24 \pmod{25} \end{cases}$$

Jawaban:

Untuk memudahkan perhitungan, sederhanakan sistem kekongruenan diatas terlebih dahulu! Amati bahwa karena $120 = 3 \cdot 8 \cdot 5$, akan lebih mudah apabila kita merubah modulus ketiga kekongruenan menjadi ketiga angka tersebut. Tentunya 3, 5, 8 saling relatif prima, maka modulus tersebut akan menghasilkan suatu solusi. Sederhanakan masing-masing kekongruenan seperti berikut

- $X \equiv 8 \pmod{9} \to X = 9K + 8 \to X \equiv 2 \pmod{3}$
- $X \equiv 15 \pmod{16} \to X = 16L + 15 \to X \equiv 7 \pmod{8}$
- $X \equiv 24 \pmod{25} \to X = 25M + 24 \to X \equiv 4 \pmod{5}$

Diperoleh sistem kekongruenan yang lebih sederhana yaitu

$$\begin{cases} X \equiv 2 \pmod{3} \\ X \equiv 7 \pmod{8} \\ X \equiv 4 \pmod{5} \end{cases}$$

Dengan Chinese Remainder Theorem, akan diperoleh

- $M_1 = 8 \cdot 5 = 40 \to y_1 = 1$
- $M_2 = 5 \cdot 3 = 15 \to y_2 = 7$
- $M_3 = 3 \cdot 8 = 24 \to y_3 = 4$

Solusi sistem diatas adalah

$$X = 2 \cdot 40 \cdot 1 + 7 \cdot 15 \cdot 7 + 4 \cdot 24 \cdot 4 = 1199 \equiv 119 \pmod{120}$$

Oleh karena itu, disimpulkan bahwa sisa pembagian X dengan 120 adalah 119

3. Seorang pustakawan menemui sebuah buku dengan kode ISBN yang tidak lengkap. Buku tersebut memiliki kode seperti berikut: 3-83**p**5-4128-**q**. **Dengan algoritma Euclidian**, tentukan kode ISBN tersebut apabila diketahui bahwa **p** adalah balikan dari -23 (mod 7). **(NILAI = 20)**

Jawaban:

Dari algoritma Euclidian, diperoleh:

- 23 = - 4 . 7 + 5 (i)
7 = 1 . 5 + 2 (ii)
5 = 2 . 2 + 1 (iii)
2 = 2 . 1 + 0 (iv)

Susun persamaan menjadi:

1 = 5 - 2 . 2 (iii)
1 = 5 - 2 . (7 - 1 . 5) (ii)
1 = ((-23) + 4 . 7) - 2 . (7 - 1 . ((-23) + 4 . 7)) (i)
1 = 10 . 7 + 3 . (-23) atau 3 . (-23) + 10 . 7 ≡ 1 (mod 7)

Karena 10 . 7 ≡ 0 (mod 7), maka
3 . (-23) ≡ 1 (mod 7)

Sehingga diperoleh **p = 3**

Dicari karakter uji untuk kode ISBN 3-8335-4128:
$\sum_{i=1}^{9} ix_i$= (1)(3) + (2)(8) + (3)(3) + (4)(3) + (5)(5) + (6)(4) + (7)(1) + (8)(2) + (9)(8) = 184
$\sum_{i=1}^{9} ix_i$ mod 11 = 8

Sehingga diperoleh kode ISBN = **3-8335-4128-8**

4. Andi merupakan *social media influencer* yang mendapat *endorse* dari sebuah merek makanan. Ia diminta untuk membuat 20 postingan dalam kurun waktu satu minggu. Minimal jumlah *post* tiap harinya adalah satu kali. Ada aturan tambahan pada kontrak yang mewajibkan bahwa jumlah postingan saat *weekend* (Sabtu/Minggu) harus berjumlah dua atau empat kali tiap harinya. Berapa variasi cara memposting yang mungkin dilakukan Andi? **(NILAI = 15)**

Jawaban:

1. $x1 + x2 + x3 + x4 + x5 + x6 + x7 = 20$
2. $x1, x2, x3, x4, x5 \in \{x \mid x >= 1\}$
3. $x6, x7 \in \{2, 4\}$

Karena tiap hari minimal satu, langsung saja distribusikan 1 postingan untuk tiap harinya, maka konstrain berubah menjadi

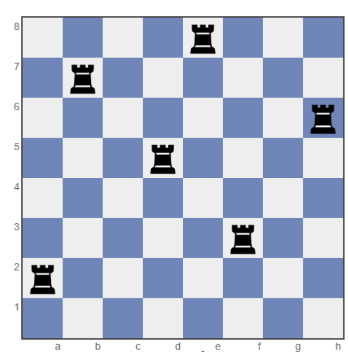
Konstrain:

1. $x1 + x2 + x3 + x4 + x5 + x6 + x7 = 13$
2. $x1, x2, x3, x4, x5 \in \{x \mid x >= 0\}$
3. $x6, x7 \in \{1, 3\}$

Kasus 1 : x6 = 1 & x7 = 1
    Sisa = 13 - 1 - 1 = 11
    Cara = (11+4)!/(11!4!) = 1365
Kasus 2 : x6 = 1 & x7 = 3
    Sisa = 13 - 1 - 3 = 9
    Cara = (9+4)!/(9!4!) = 715
Kasus 3 : x6 = 3 & x7 = 1
    Sisa = 13 - 3 - 1 = 9
    Cara = (9+4)!/(9!4!) = 715
Kasus 4 : x7 = 3 & x7 = 3
    Sisa = 13 - 3 - 3 = 7
    Cara = (7+4)!/(7!4!) = 330

Total cara = 3125

5. Pada sebuah papan catur 8x8, tentukanlah berapa banyak cara untuk meletakan enam (6) benteng(rook) sedemikian sehingga tidak ada benteng yang saling menyerang! (benteng saling menyerang bila terletak secara horizontal dan vertikal) **(NILAI = 15)**



Jawaban:
Suatu papan memiliki 8 baris(1-8) dan 8 kolom(a-h). Agar tidak ada benteng yang saling menyerang maka posisi banteng pada papan harus unik secara baris dan kolomnya. Karena terdapat 6 benteng maka kita memilih 6 dari 8 baris.

$$baris = C(8,6) = \frac{8!}{6! \cdot 2!} = 28$$

Sehingga jumlah **susunan rangkaian posisi benteng** yang mungkin

$$= C(8,6) \times 8 \times 7 \times 6 \times 5 \times 4 \times 3 = 564.480$$

Atau alternatifnya: $= C(8,6) \times C(8,6) \times 6! = 28 \times 28 \times 720 = 564.480$

Jika **IDENTIK** → semua benteng dianggap sama, sehingga urutan tidak berpengaruh!

Maka, hasil tidak dipengaruhi oleh urutan benteng. Sehingga total susunan:

$$total = \mathbf{564.480}$$

Jika **TIDAK IDENTIK**→ satu benteng berbeda dengan benteng lain. Ibaratkan setiap benteng memiliki warna yang berbeda. Sehingga urutan benteng berpengaruh!

Susunan 6 benteng yang dapat dibuat $= 6! = 720$
Sehingga total susunan 6 benteng sedemikian tidak ada yang saling menyerang:

$$total = 564.480 \times 6! = \mathbf{406.425.600}$$

Atau alternatifnya: $total = P(8,6) \times P(8,6) = 406.425.600$

6. Tentukan suku ketiga dan keempat dari $(x - 6y)^6$ **(NILAI = 10)**

Jawaban:
Suku ketiga: C(6,2)$x^{6-2} + (-6y)^2 = 15 \,.\, x^4 .36\text{y}^2 = 540x^4y^2$
Suku keempat: C(6,3)$x^{6-3} + (-6y)^3 = 20 \,.\, x^3 \,.-216y^3 = -4320x^3y^3$

7. (BONUS, TIDAK WAJIB) Seorang bangsawan ingin berkomunikasi secara rahasia dengan anak buahnya. Bangsawan ini memutuskan untuk menggunakan algoritma kriptografi RSA untuk membantu komunikasi. Sang bangsawan menggunakan public key yaitu (26, 7) yang berbentuk (n, e). Kemudian, anak buahnya mengirimkan pesan terenkripsi yaitu ”HBVO”. Bantu sang bangsawan untuk mendekripsi pesan yang ia terima! Ubah setiap huruf pada pesan menjadi angka dengan A = 0, B = 1, C = 2, dan seterusnya, lalu dekripsi masing-masing angka secara independen sebelum diubah kembali menjadi huruf yang bersesuaian. **(NILAI = 10)**

Jawaban:

Karena *public key* yang digunakan memiliki $n = 26 = 2 \cdot 13$, diperoleh $m = (2 - 1)(13 - 1) = 12$. *Private key* sang bangsawan dapat dicari menggunakan

$$d = \frac{1 + 12k}{7}$$

dimana nilai k terkecil agar d bilangan bulat adalah $k = 4$. Sehingga, nilai d terkecil yang mungkin adalah $d = 7$ (Nilai d lain seperti 19, 31, 43, ... juga memenuhi, namun kita dapat memilih d terkecil). Dengan merubah masing-masing huruf pada plaintext menjadi angka didapat ”7 1 21 14”. Proses dekripsi dengan algoritma RSA yaitu $p \equiv c^d \pmod n$ adalah sebagai berikut:

- **c=7** $\rightarrow p \equiv 7^7 \equiv (7^2)^3 \cdot 7 \equiv (-3)^3 \cdot 7 \equiv -1 \cdot 7 \equiv 19 \pmod{26}$
- **c=1** $\rightarrow p \equiv 1^7 \equiv 1 \pmod{26}$
- **c=21** $\rightarrow p \equiv 21^7 \equiv ((-5)^2)^3 \cdot -5 \equiv (-1)^3 \cdot -5 \equiv 5 \pmod{26}$
- **c=14** $\rightarrow p \equiv 14^7 \equiv (14^2)^3 \cdot 14 \equiv 14^3 \cdot 14 \equiv (14^2)^2 \equiv 14 \pmod{26}$

Hasil dekripsinya adalah ”19 1 5 14”. Oleh karena itu, pesan yang dikirimkan anak buah sang bangsawan adalah TBFO