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

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

Solusi Kuis ke-3 IF2120 Teori Bilangan, Kombinatorial
Dosen: Rinaldi Munir, Harlili, Fariska Zakhralativa
Kamis, 31 Oktober 2019
Waktu: 50 menit

---

1. Tentukan banyaknya solusi bilangan bulat dari $x_1 + x_2 + x_3 = 10$ jika diberi syarat $0 \leq x_1 \leq 2$, $x_2 > 1$, dan $x_3 \geq 0$! **(Nilai = 25)**

Jawaban: Analogikan dengan membagi 10 buah bola yang identik ke dalam 3 buah kotak, sebut saja kotak x_1, x_2, dan x_3.

x_1 ada kemungkinan berisi 0 (tak berisi), 1, atau 2. Untuk masing-masing nilai x1, diperinci perhitungannya sebagai berikut.

a. Kasus $x_1 = 0$, berarti $x_2 + x_3 = 10$. Isikan 2 bola ke dalam kotak x_2 (karena syaratnya $x_2 > 1$). Bagikan 8 bola sisanya ke kotak x_2 dan x_3, semuanya ada $C(2+8-1,8) = C(9,8) = 9$ cara.
b. Kasus $x_1 = 1$, berarti $x_2 + x_3 = 9$. Isikan 2 bola ke dalam kotak x_2 (karena syaratnya $x_2 > 1$). Bagikan 7 bola sisanya ke kotak x_2 dan x_3, semuanya ada $C(2+7-1,7) = C(8,7) = 8$ cara.
c. Kasus $x_1 = 2$, berarti $x_2 + x_3 = 8$. Isikan 2 bola ke dalam kotak x_2 (karena syaratnya $x_2 > 1$). Bagikan 6 bola sisanya ke kotak x_2 dan x_3, semuanya ada $C(2+6-1,6) = C(7,6) = 7$ cara.

Jumlah solusi seluruhnya adalah $\underline{9 + 8 + 7} = \underline{24}$

2. Kota Bandung dan sekitarnya menggunakan kode plat kendaraan "D". Plat kendaraan di Indonesia memiliki format <kode daerah> <angka> <huruf>. Angka pada plat kendaraan minimal berisi 1 angka dan maksimal 4 angka (tidak ada kendaraan yang angka pada platnya hanya "0"), sedangkan untuk hurufnya minimal 1 huruf dan maksimal 3 huruf. Tentukan banyaknya plat kendaraan yang mungkin dapat dibuat untuk daerah Kota Bandung dan sekitarnya! **(Nilai = 25)**

Jawaban:
Format kode plat kendaraan Kota Bandung dan sekitarnya adalah D <angka> <huruf>

Banyaknya angka yang dapat dibuat adalah 1 - 9999 yang berarti terdapat 9999

Banyaknya huruf yang dapat dibuat :
a. Untuk 1 huruf adalah A - Z yang berarti terdapat 26
b. Untuk 2 huruf adalah AA - ZZ yang berarti terdapat 26x26 = 676
c. Untuk 3 huruf adalah AAA - ZZZ yang berarti terdapat 26x26x26 = 17576

Total = 26 + 676 + 17576 = 18278

Banyaknya plat kendaraan yang mungkin dapat dibuat untuk Kota Bandung dan sekitarnya adalah <u>1 x 9999 x 18278</u> = <u>182761722</u>

3. Misalkan x adalah sisa pembagian 2019^{63} oleh 31. Tentukan x dengan bantuan teorema Fermat.

(Nilai = 25)

Jawaban:

Menurut teorema fermat, jika p bilangan prima dan PBB(a, p) = 1, maka berlaku

$$a^{p-1} \equiv 1 \pmod p$$

Karena 31 bilangan prima dan PBB(2019, 31) = 1, maka berlaku

$$2019^{30} \equiv 1 \pmod{31}$$

Perhatikan bahwa

$$2019 \equiv 4 \pmod{31}$$

Oleh karena itu,

$$2019^{63} \equiv (2019^{30})^2 \,.\, 2019^3 \bmod 31$$

$$2019^{63} \equiv (1)^2 \,.\, 4^3 \bmod 31$$

$$2019^{63} \equiv 64 \bmod 31$$

$$2019^{63} \equiv 2 \bmod 31$$

Jadi, sisa pembagian 2019^{63} oleh 31 adalah 2

4. Salah satu penggunaan *Chinese Remainder Problem* adalah *Secret sharing* yang merupakan salah satu metode kriptografi. Misal terdapat sebuah rahasia *S*, maka rahasia tersebut dibagi menjadi beberapa bagian (*shares*). Rahasia S dapat dibangun kembali hanya jika seseorang memiliki set *shares* yang valid. Salah satu implementasi *secret sharing* adalah skema **Asmuth-Bloom.** Rahasia S akan dibagi ke dalam beberapa I_0 , I_1, I_2 , … I_n *shares*. Bagian terakhir dari skema ini adalah mendapatkan nilai *S* dengan persamaan $S = x_0 \bmod p_0$, p_0 adalah sebuah bilangan yang ditentukan saat pembagian *shares*. Kemudian, diberikan sebuah baris bilangan m_0 , m_1, … m_k yang masing-masing saling relatif prima, maka x_0 merupakan solusi unik modulo ($m_0 \,.\, m_1 \,.\, m_2 \,.\, ... \,.\, m_n$) dari persamaan: **(Nilai = 25)**

$$x \equiv I_1 \bmod m_1 \,,\; x \equiv I_2 \bmod m_2 \,,\; x \equiv I_3 \bmod m_3 \;.....\; x \equiv I_n \bmod m_n$$

Untuk $p_o = 5$, $\{(I_k , m_k)\} = \{(1,7),(9,11),(5,13)\}$, tentukan nilai rahasia dari *secret sharing* !

Jawaban: Cukup jelas bahwa permasalahan ini berkaitan dengan menyelesaikan persamaan Chinese Remainder Theorem.

Sistem persamaan CRT yang disoalkan adalah :

$$\begin{cases} x \equiv 1 \mod 7 \\ x \equiv 9 \mod 11 \\ x \equiv 5 \mod 13 \end{cases}$$

Ada dua cara menyelesaikan CRT berdasarkan *slide* Teori Bilangan, akan tetapi hanya satu solusi yang akan dibahas pada pembahasan ini. Solusi lain dianggap benar, namun tidak dibahas.

Dari $x \equiv 1 \bmod 7$, misalkan $x = 7k_1 + 1$….(1)

Kemudian substitusi (1) ke $x \equiv 9 \bmod 11$, sehingga :

$x = 7k_1 + 1 \equiv 9 \bmod 11$, sehingga $7k_1 \equiv 8 \bmod 11$. $k_1 \equiv 9 \bmod 11$, misalkan $k_1 = 11k_2 + 9$

Maka $x = 7k_1 + 1 = 7(11k_2 + 9) + 1 = 77k_2 + 64$….(2)

Kemudian, substitusi (2) ke $x \equiv 5 \bmod 13$, sehingga

$X = 77k_2 + 64 \equiv 5 \bmod 13$. $77k_2 \equiv 6 \bmod 13$. Maka $k_2 \equiv 7 \bmod 13$, misalkan $k_2 = 13k_3 + 7$
Maka, $x = 77k_2 + 64 = 77(13k_3 + 7) + 64 = 1001k_3 + 603$.
Solusi unik adalah $1001k_3 + 603 \bmod (7.11.13) = 603$.

Oleh karenanya, rahasia S adalah $603 \bmod 5 = 3$.