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

Nama :……
NIM :……
T.tangan:……

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 $0 \le x_1 \le 2$, $x_2 > 1$, dan $x_3 \ge 0$! **(Nilai = 25)**
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)**
3. Misalkan *x* adalah sisa pembagian 2019^{63} oleh 31. Tentukan *x* dengan bantuan teorema Fermat. **(Nilai = 25)**
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)**

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

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

Jawaban setiap soal ditulis di bawah ini. Gunakan halaman dibalik atau kertas tambahan jika diperlukan.