UNIVERSITI SAINS MALAYSIA

First Semester Examination
2011/2012 Academic Session

January 2012

MGM 502 – Number Theory
[Teori Nombor]

Duration : 3 hours
[Masa : 3 jam]

Please check that this examination paper consists of FOUR pages of printed material before you begin the examination.

[Sila pastikan bahawa kertas peperiksaan ini mengandungi EMPAT muka surat yang bercetak sebelum anda memulakan peperiksaan ini.]

Instructions: Answer **all three** [3] questions.

*[**Arahan:** Jawab **semua tiga** [3] soalan.]*

In the event of any discrepancies, the English version shall be used.

[Sekiranya terdapat sebarang percanggahan pada soalan peperiksaan, versi Bahasa Inggeris hendaklah diguna pakai].

1. (a) Given the linear Diophantine equation, $172x + 20y = 1000$. Use the Euclidean Algorithm to obtain the general form of the integer solutions of x and y. Next, find the solution in the positive integers.

   (b) Find the integer solution in a general form of the following linear Diophantine equation,

$$7x + 21y + 35z = 14\,.$$

   Next, give the first 3 integer solutions for this equation.

   (c) Show $\sqrt{p}$ is irrational for p primes.

   (d) Show that there are infinitely many primes.

[100 marks]

1. (a) Di berikan persamaan Diophantine linear $172x + 20y = 1000$. *Dengan menggunakan algoritma Euclidean, dapatkan penyelesaian bentuk am x dan y. Seterusnya, dapatkan penyelesaian dalam integer positif.*

   (b) Dapatkan penyelesaian bentuk am bagi persamaan Diophantine linear berikut:

$$7x + 21y + 35z = 14\,.$$

   Seterusnya, berikan 3 penyelesaian pertama bagi persamaan di atas.

   (c) Tunjukkan bahawa $\sqrt{p}$ *adalah suatu nombor tak nisbah, dengan p adalah nombor perdana.*

   (d) Tunjukkan bahawa terdapat tak terhingga banyaknya nombor perdana.

[100 markah]

2. (a) Define a perfect number. List the first four perfect numbers using the Euclid formula.

(a) Define a multiplicative function. Show that the arithmetic functions τ and σ are multiplicative.

(b) Find $\sigma(650)$ and $\tau(650)$.

(c) Define a Mersenne number. Next, using the Lucas- Lehmer Test, determine whether the Mersenne number M_{13} is a Mersenne prime.

(d) Solve the following simultaneous linear congruences,

$$x \equiv 5 (\bmod 11); \quad x \equiv 14 (\bmod 29); \quad x \equiv 15 (\bmod 31).$$

(e) Show using the congruence theory that 41 divides $2^{20} - 1$.

[100 marks]

2. (a) Takrifkan nombor sempurna. Senaraikan 4 nombor sempurna yang pertama menggunakan rumus Euclid.

(b) Takrifkan fungsi multiplikatif. Tunjukkan bahawa fungsi-fungsi τ dan σ adalah suatu fungsi multiplikatif.

(c) Dapatkan $\sigma(650)$ dan $\tau(650)$.

(d) Takrifkan nombor Mersenne. Dengan menggunakan cara Lucas-Lehmer, tentukan sama ada M_{13} merupakan nombor perdana Mersenne.

(e) Dapatkan penyelesaian bagi kongruen linear serentak berikut,

$$x \equiv 5 (\bmod 11); \quad x \equiv 14 (\bmod 29); \quad x \equiv 15 (\bmod 31).$$

(f) Tunjukkan dengan menggunakan teori kongruen, 41 membahagi $2^{20} - 1$.

[100 markah]

3. (a) Using the Fermat's Little Theorem, find the least positive residue modulo 11 (remainder when divided by 11) of 3^{201}

(b) If p is a prime and a is an integer such that p does not divide a, show that a^{p-2} is an inverse of a modulo p.

(c) State the Wilson's Theorem. Verify the Wilson's Theorem for $p = 7$.

(d) Solve the quadratic congruence $5x^2 + 6x + 1 \equiv 0 (\bmod 23)$.

(e) Define primitive root of an integer n. Next show that 3 is a primitive root of the integer 7.

(f) Encrypt the message DO NOT OPEN using the affine transformation $C \equiv 11P + 18 \mod 26$.

[100 marks]

3. (a) Menggunakan Teorem Little Fermat, dapatkan residu positif terkecil modulo 11 bagi 3^{201}.

(b) Jika p suatu nombor perdana dan a adalah suatu integer yang mana p tidak membahagi a. Tunjukkan bahawa a^{p-2} *adalah songsangan kepada a modulo p.*

(c) Berikan/sebutkan Teorem Wilson. Tentusahkan Teorem ini untuk p = 7.

(d) Dapatkan penyelesaian bagi kongruen kuadratik berikut:

$$5x^2 + 6x + 1 \equiv 0 (\bmod 23) .$$

(e) Takrifkan punca kuasa primitif (primitive root) untuk suatu integer n. Seterusnya, tunjukkan 3 adalah punca kuasa primitif (primitive root) bagi n = 7.

(f) Apakah teks sifer yang diperolehi apabila enkripsi transformasi afin $C \equiv 11P + 18 \mod 26$ *digunakan untuk mengenkripsi mesej* DO NOT OPEN.

[100 markah]

ooo O ooo -