
UNIVERSITI SAINS MALAYSIA

Second Semester Examination
2009/2010 Academic Session

April/May 2010

MGM 502 – Number Theory
[Teori Nombor]

Duration : 3 hours
[Masa : 3 jam]

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

[Sila pastikan bahawa kertas peperiksaan ini mengandungi LIMA 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) Use the Euclidean Algorithm to obtain integers x and y satisfying

$$\gcd(119, 272) = 119x + 272y$$

- (b) Consider the problem of purchasing RM510 postal orders using RM30 and RM50 postal orders. How many of each type of postal order should be used? Find all the possible combinations.
- (c) Define a multiplicative function. Show that the function $\frac{\sigma(n)}{n}$ is a multiplicative function.
- (d) Find $\sigma(650)$ and $\tau(650)$.
- (e) If $2^p - 1$ a prime, show that $2^{p-1} (2^p - 1)$ is a perfect number.

[100 marks]

2. (a) Define a Mersenne number. If p is an odd prime, then any divisor of the Mersenne number, $M_p = 2^p - 1$ is of the form $2kp + 1$, where k is a positive integer. Using this statement show that M_{29} is a composite number.
- (b) Using the Lucas-Lehmer Test, determine whether the Mersenne number M_{11} is a Mersenne prime.
- (c) Given the linear congruence $34x \equiv 60 \pmod{98}$, determine the number of solutions for this congruence. Give reasons. Next, find all solutions of the given linear congruence.
- (d) Solve the following simultaneous linear congruences,

$$x \equiv 5 \pmod{6}; \quad x \equiv 4 \pmod{11}; \quad x \equiv 3 \pmod{17}$$

- (e) Given $a \equiv b \pmod{n}$ and $c \equiv d \pmod{n}$.
Show that $a + c \equiv b + d \pmod{n}$ and $ac \equiv bd \pmod{n}$.

[100 marks]

1. (a) Dengan menggunakan algoritma Euclidean, dapatkan integer x dan y yang memenuhi

$$\gcd(119, 272) = 119x + 272y.$$

- (b) Pertimbangkan satu situasi yang memerlukan pembelian RM510 kiriman wang menggunakan kiriman wang RM30 dan RM50. Berapakah jumlah setiap kiriman wang yang digunakan. Cari semua kombinasi
- (c) Takrifkan fungsi multiplikatif. Tunjukkan bahawa fungsi $\frac{\sigma(n)}{n}$ adalah satu fungsi yang multiplikatif.
- (d) Cari $\sigma(650)$ dan $\tau(650)$.
- (e) Jika $2^p - 1$ nombor perdana, tunjukkan bahawa $2^{p-1} \mid 2^p - 1$ adalah nombor sempurna.

[100 marks]

2. (a) Takrifkan nombor Mersenne. Jika p adalah satu nombor perdana, maka sebarang pembahagi bagi nombor mersenne, $M_p = 2^p - 1$ adalah dalam bentuk $2kp + 1$, di mana k adalah satu nombor integer positif. Dengan menggunakan kenyataan ini, tunjukkan bahawa M_{29} adalah satu nombor komposit.

- (b) Menggunakan ujian Lucas-Lehmer. Tentukan sama ada nombor Mersenne M_{11} adalah nombor perdana Mersenne.
- (c) Diberikan kongruen $34x \equiv 60 \pmod{98}$, tentukan bilangan penyelesaian bagi kongruen ini. Berikan alasan anda. Seterusnya dapatkan semua penyelesaian bagi kongruen linear ini.
- (d) Selesaikan kongruen linear serentak berikut,

$$x \equiv 5 \pmod{6}; \quad x \equiv 4 \pmod{11}; \quad x \equiv 3 \pmod{17}$$

- (e) Diberikan $a \equiv b \pmod{n}$ dan $c \equiv d \pmod{n}$.
Tunjukkan bahawa $a + c \equiv b + d \pmod{n}$ dan $ac \equiv bd \pmod{n}$.

[100 marks]

3. (a) Solve the following quadratic congruence.

$$5x^2 + 6x + 1 \equiv 0 \pmod{23}$$

- (b) Define a Legendre symbol. If $a \equiv b \pmod{p}$ then show that $\left(\frac{a}{p}\right) = \left(\frac{b}{p}\right)$, where a, b are integers that are relatively prime to the odd prime p .
- (c) Using the concept of Legendre symbol, determine whether or not the congruence $x^2 \equiv -46 \pmod{17}$ is solvable.
- (d) Encrypt the message DO NOT STOP using the affine transformation $C \equiv P + 5 \pmod{26}$.
- (e) What is the ciphertext that is produced when RSA encryption with key $(e, n) = (7, 2627)$ is used to encrypt the message LIFE IS A DREAM.

[100 marks]

3. (a) *Selesaikan kongruen kuadratik berikut*
$$5x^2 + 6x + 1 \equiv 0 \pmod{23}$$
- (b) *Takrifkan simbol Legendre. Jika $a \equiv b \pmod{p}$ maka tunjukkan bahawa*
$$\left(\frac{a}{p}\right) = \left(\frac{b}{p}\right),$$
di mana a, b adalah integer yang secara relatif adalah perdana terhadap nombor perdana p yang ganjil.
- (c) *Dengan menggunakan konsep simbol Legendre, tentukan sama ada kongruen*
$$x^2 \equiv -46 \pmod{17}$$
mempunyai penyelesaian.
- (d) *Enkripkan pesanan DO NOT STOP menggunakan transformasi afin*
$$C \equiv P + 5 \pmod{26}.$$
- (e) *Apakah teks saifer yang dihasilkan apabila enkripsi RSA dengan kekunci*
 $(e, n) = (7, 2627)$ *digunakan untuk mengenkripsi pesanan LIFE IS A F DREAM.*

[100 markah]