UNIVERSITI SAINS MALAYSIA

First Semester Examination
2017/2018 Academic Year

January 2018

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 **FOUR** (4) questions.

*[**Arahan**: Jawab semua **EMPAT** (4) 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 mathematical induction to verify that

$$2 \cdot 6 \cdot 10 \cdot 14 \cdots (4n-2) = \frac{(2n)!}{n!}$$

for all $n \geq 1$.

(b) Prove that $k^2 - k + 3$ is odd for all integers k.

(c) For positive integers a and b, prove that $\gcd(a,b)$ divides both

(i) $a+b$

(ii) $\text{lcm}(a,b)$.

[100 marks]

1. (a) Guna aruhan matematik untuk menentusahkan

$$2 \cdot 6 \cdot 10 \cdot 14 \cdots (4n-2) = \frac{(2n)!}{n!}$$

untuk semua $n \geq 1$.

(b) Buktikan bahawa $k^2 - k + 3$ *adalah ganjil untuk semua integer k.*

(c) Untuk integer positif a dan b, buktikan bahawa $\gcd(a,b)$ *membahagi kedua-dua*

(i) $a+b$

(ii) $\text{lcm}(a,b)$.

[100 markah]

2. (a) Ali wants to buy two types of chocolates. The milk chocolate costs 57 cents each while the strawberry chocolate costs 22 cents each.

(i) How many milk chocolates and strawberry chocolates can he buy for exactly RM4.00?

(ii) Assume that there is a discount for milk chocolate and the price changed from 57 cents to 55 cents. Can Ali still buy milk chocolates and strawberry chocolates for exactly RM4.00?

(b) Show that the only prime of the form $n^2 - 4$ is 5.

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

[100 marks]

2. *(a)* *Ali mahu membeli dua jenis coklat. Coklat susu berharga 57 sen manakala coklat strawberi berharga 22 sen setiap satu.*

(i) *Berapakah bilangan coklat susu dan coklat strawberi yang boleh dibeli oleh Ali dengan tepat RM4.00?*

(ii) *Anggap terdapat diskaun untuk coklat susu dan harganya berubah dari 57 sen ke 55 sen. Adakah Ali masih boleh membeli coklat susu dan coklat strawberi dengan tepat RM4.00?*

(b) *Tunjukkan bahawa hanya 5 merupakan nombor perdana yang berbentuk* $n^2 - 4$.

(c) *Tunjukkan bahawa 41 membahagi* $2^{20} - 1$ *dengan menggunakan teori kongruen.*

[100 markah]

3. (a) Given $ax \equiv b \pmod{n}$ and $d = \gcd(a, n)$, show that this congruence does not have any solution if d does not divide b.

(b) State the Chinese Remainder Theorem (CRT). Solve the following simultaneous linear congruences using CRT:

$$x \equiv 6 \pmod{5}; \qquad x \equiv 4 \pmod{11}; \qquad x \equiv 3 \pmod{7}$$

(c) State the Wilson's Theorem. Using the Wilson's Theorem, give an example to determine whether or not a given number is a prime.

(d) Solve the quadratic congruence $5x^2 + 6x + 1 \equiv 0 \pmod{17}$.

(e) Define a primitive root of an integer. Is 2 a primitive root of 11? Give justification to your answer.

[100 marks]

3. *(a)* *Diberikan* $ax \equiv b \pmod{n}$ *dan* $d = \gcd(a,n)$*, tunjukkan bahawa kongruen ini tidak mempunyai penyelesaian apabila d tidak membahagi b.*

(b) *Nyatakan Teorem Baki Cina (CRT). Selesaikan persamaan linear kongruen berikut mengunakan (CRT):*

$$x \equiv 6 \pmod{5}; \qquad x \equiv 4 \pmod{11}; \qquad x \equiv 3 \pmod{7}$$

(c) *Nyatakan Teorem Wilson. Dengan menggunakan Teorem Wilson, berikan saru contoh untuk menentukan sesuatu nombor itu adalah nombor perdana.*

(d) *Selesaikan kongruen kuadratik* $5x^2 + 6x + 1 \equiv 0 \pmod{17}$.

(e) *Takrifkan punca primitif bagi suatu integer. Adakah* 2 *suatu punca primitif bagi* 11*? Berikan justifikasi kepada jawapan anda.*

[100 markah]

4. (a) Define the Legendre symbol. Next, given $a \equiv b \pmod{p}$, show

$$\left(\frac{a}{p}\right) = \left(\frac{b}{p}\right),$$

where a, b are integers and they are relatively prime to an odd prime p.

(b) Encrypt the message DO NOT EAT using the affine transformation $C \equiv 5P + 11 \pmod{26}$.

(c) What is the underlying mathematical hard problem for RSA cryptography?

(d) What is the ciphertext that is produced when RSA encryption with key $(e,n) = (13, 2627)$ is used to encrypt the message ALL THE BEST?

[100 marks]

4. *(a)* *Takrifkan simbol Legendre. Seterusnya, diberi* $a \equiv b \pmod{p}$*, tunjukkan bahawa*

$$\left(\frac{a}{p}\right) = \left(\frac{b}{p}\right),$$

untuk a, b adalah integer dan perdana secara relatif kepada p.

(b) *Enkrip mesej DO NOT EAT dengan menggunakan penjelmaan afin,* $C \equiv 5P + 11 \pmod{26}$.

(c) *Apakah pemasaalah matematik yang sukar untuk kriptografi RSA?*

(d) *Apakah teks sifer yang diperoleh apabila enkripsi RSA dengan kekunci* $(e,n) = (13, 2627)$ *digunakan untuk mengenkrip mesej ALL THE BEST?*

[100 markah]

- ooo OOO ooo -