

Phân kiểm tra kiến thức

Chương 1.

1. Độ phức tạp của thuật toán được đo bằng:

- a) Dung lượng bộ nhớ của máy tính cần thiết để thực hiện thuật toán.
- b) Thời gian làm việc của máy tính khi thực hiện thuật toán.
- c) Số phép tính bit cần thiết để thực hiện thuật toán.
- d) Số phép tính bit cần thiết, xét như một hàm của độ lớn đầu vào.

<u>Điểm:</u>	a	b	c	d
	3	5	7	10

2. Một thuật toán được gọi là có độ phức tạp đa thức nếu đầu vào có độ lớn n thì thời gian thực hiện thuật toán không vượt quá:

- a) $O(n^d)$ với d là một số nguyên dương nào đó.
- b) $O(\log^d n)$ với d là một số nguyên dương nào đó.
- c) $O(1)$.
- d) $O(f(n))$ với $f(n)$ là một đa thức của n .

<u>Điểm:</u>	a	b	c	d
	0	10	0	0

3. Thuật toán khai triển số nguyên ra thừa số nguyên tố có độ phức tạp:

- a) mũ
- b) đa thức
- c) dưới mũ
- d) chưa đánh giá được

<u>Điểm:</u>	a	b	c	d
	0	0	10	0

Chương 2.

1. Giả sử b là số nguyên lớn hơn 1 và n là số được biểu diễn dưới dạng:

$$n = a_k b^k + a_{k-1} b^{k-1} + \dots + a_1 b + a_0,$$

trong đó a_j nguyên, $0 \leq a_j \leq b-1$, $j=0, 1, \dots, k$; $a_k \neq 0$. Khi đó số chữ số của n trong cơ sở b là

- a) n/b
- b) $\log_2 n$
- c) $\lceil \log_b n \rceil + 1$
- d) $\lceil \log_b n \rceil$

<u>Điểm:</u>	a	b	c	d
	0	0	10	8

2. a) Để cộng trừ hai số nguyên k -bit, ta cần $O(k^2)$ phép tính bit.

b) Để cộng trừ hai số nguyên k -bit, ta cần $O(k)$ phép tính bit.

c) Giả sử n, m là các số trong cơ sở 2, có k chữ số. Để nhân m với n (theo quy tắc thông thường) ta cần $O(k)$ phép tính bit.

d) Như câu c), cần $O(k^2)$ phép tính bit.

<u>Điểm:</u>	a	b	c	d
	0	10	0	10

3. a) Mọi ước nguyên tố của hợp số n đều nhỏ hơn \sqrt{n} .

b) Để kiểm tra xem n có phải là số nguyên tố hay không, cần làm n phép chia.

c) Để kiểm tra xem n có phải là số nguyên tố hay không, cần làm ít nhất là n phép tính bit.

d) Để kiểm tra xem n có phải là số nguyên tố hay không, cần làm $O(\sqrt{n})$ phép tính bit.

<u>Điểm:</u>	a	b	c	d
	0	0	3	10

4. Cho 2 số nguyên dương a, b . Khi đó số phép tính bit cần thiết để thực hiện thuật toán Euclid tìm ƯCLN của a và b là:

- a) $O(ab)$
- b) $O(\log_2 a \cdot \log_2 b)$
- c) $O((\log_2 a)^2)$ nếu $a < b$
- d) $O((\log_2 a)^3)$ nếu $a < b$

<u>Điểm;</u>	a	b	c	d
	0	2	4	10

5. a) Nếu p là số nguyên tố thì $(p-1)! \equiv 1 \pmod{p}$

b) Nếu p là số nguyên tố và a là số nguyên dương thì $a^{p-1} \equiv 1 \pmod{p}$

c) p là số nguyên tố khi và chỉ khi $(p-1)! \equiv -1 \pmod{p}$

d) Nếu p là số nguyên tố và a là số nguyên dương thì a^{p-2} là nghịch đảo modulo p

<u>Điểm;</u>	a	b	c	d
	0	5	10	5

6. a) Nếu với mọi số a nguyên dương, $a^p \equiv a \pmod{p}$ thì p là số nguyên tố.

b) Nếu với một số a nguyên dương nào đó, $a^p \equiv a \pmod{p}$ thì p là số nguyên tố.

c) Có vô hạn hợp số p sao cho với mọi số a nguyên tố cùng nhau với p , ta có $a^{p-1} \equiv 1 \pmod{p}$.

d) Tồn tại hữu hạn số có tính chất nói trong câu c).

<u>Điểm;</u>	a	b	c	d
	0	0	10	5

7. Cho n là số nguyên dương lẻ, $n=2^s t+1$, trong đó t lẻ, $s \geq 0$. Giả sử với 5 số ngẫu nhiên $a_1, a_2, a_3, a_4, a_5 < n$ ta có $a_i^t \equiv 1 \pmod{n}$. Có thể kết luận

a) n là hợp số

b) n là số nguyên tố

c) n là số nguyên tố với xác suất lớn hơn $1-1/2^5$

d) n là số nguyên tố với xác suất lớn hơn $1-1/4^5$

<u>Điểm;</u>	a	b	c	d
	0	2	5	10

Chương 3

1. Trong các hàm số học sau đây những hàm nào là hàm nhân tính mạnh

a) $f(n)$ =tích các ước nguyên tố của n

b) $f(n)$ = tổng các ước nguyên tố của n

c) $f(n)$ = tích các ước của n

d) $f(n) = n^2$

<u>Điểm:</u>	a	b	c	d
	3	0	3	10

(Nếu đánh dấu nhiều hơn 1 khả năng thì điểm bằng minimum của điểm các khả năng đó)

2. Kí hiệu φ là Phi-hàm Euler.

a) m, a nguyên dương thì $a^{\varphi(m)} \equiv 1 \pmod{m}$

b) m, a nguyên dương thì $a^{\varphi(m)} \equiv a \pmod{m}$

c) m, a nguyên dương, nguyên tố cùng nhau thì $a^{\varphi(m)} \equiv 1 \pmod{m}$

d) m, a nguyên dương, nguyên tố cùng nhau thì $a^{\varphi(m)} \equiv a \pmod{m}$

<u>Điểm:</u>	a	b	c	d
	3	0	10	0

3. Trong các hệ sau đây, những hệ nào thặng dư thu gọn modulo 24

a) 1, 3, 5, 7, 9, 11, 13, 15, 17, 19

b) 1, 2, 3, 5, 7, 9, 11, 13, 15, 17, 19

c) 1, 2, 4, 6, 8, 10, 12, 14, 16, 18, 20, 22

d) 5, 25, 35, 55, 65, 85, 95, 115

<u>Điểm:</u>	a	b	c	d
	0	0	0	10

(Nếu đánh dấu nhiều hơn 1 khả năng thì điểm bằng minimum của điểm các khả năng đó)

4. Giả sử m là số nguyên dương và $M_m = 2^m - 1$ là số Mersenne thứ m . Khi đó

a) M_m là hợp số

b) M_m là số nguyên tố

c) Các ước nguyên tố của M_m có dạng $2kp+1$ với p nguyên tố lẻ

d) Có vô hạn m để M_m nguyên tố

<u>Điểm:</u>	a	b	c	d
	0	0	10	5

5. Trong các số sau đây số nào có căn nguyên thủy

a) 1996 b) 1997 c) 1998 d) 1999

<u>Điểm:</u>	a	b	c	d
	-5	5	-5	5

(Nếu đánh dấu nhiều khả năng thì điểm bằng tổng của điểm các khả năng đó)

6. Hỏi cũng như câu 5.

a) 1250 b) 1251 c) 2401 d) 3993

<u>Điểm:</u>	a	b	c	d
	5	-5	5	-5

(Nếu đánh dấu nhiều khả năng thì điểm bằng tổng của điểm các khả năng đó)

Chương 4

1. Trong các số 1, 2, ..., 1996 số các số là thặng dư bình phương của 1997 là

a) 998 b) 0 c) 1995 d) 999

<u>Điểm:</u>	a	b	c	d
	10	0	0	0

2. $F_m = 2^{2^m} + 1$ là số Fermat thứ m

a) F_m là số nguyên tố với mọi m

b) F_m là hợp số với mọi m

c) F_m là số nguyên tố nếu $3^{(F_m-1)/2} \equiv -1 \pmod{F_m}$

d) F_m là số nguyên tố thì $3^{(F_m-1)/2} \equiv -1 \pmod{F_m}$

<u>Điểm:</u>	a	b	c	d
	-5	-5	5	5

(Nếu đánh dấu nhiều khả năng thì điểm bằng tổng của điểm các khả năng đó)

3. Đánh dấu những câu đúng:

- a) Số giả nguyên tố Euler cơ sở b là số giả nguyên tố cơ sở b
- b) Số giả nguyên tố cơ sở b là số giả nguyên tố Euler cơ sở b
- c) Số giả nguyên tố mạnh Euler cơ sở b là số giả nguyên tố Euler cơ sở b
- d) Số giả nguyên tố Euler cơ sở b là số giả nguyên tố mạnh cơ sở b

<u>Điểm:</u>	a	b	c	d
	5	-3	5	-3

(Nếu đánh dấu nhiều khả năng thì điểm bằng tổng của điểm các khả năng đó)

4. Giả sử k là số các số nguyên dương $b \leq 2000$, nguyên tố cùng nhau với 2001 sao cho 2001 là giả nguyên tố mạnh Euler cơ sở b . Khi đó

- a) $k \leq 650$
- b) $650 \leq k \leq 750$
- c) $750 < k \leq 850$
- d) $850 < k$

<u>Điểm:</u>	a	b	c	d
	10	0	0	0

5. Giả sử n là hợp số lẻ, b là số nguyên chọn ngẫu nhiên trong các số từ 1 đến $n-1$. Gọi p là xác suất để n giả nguyên tố Euler cơ sở b . Khi đó

- a) $1 \geq p \geq 3/4$
- b) $3/4 > p \geq 2/3$
- c) $2/3 > p \geq 1/2$
- d) $1/2 > p \geq 0$

<u>Điểm:</u>	a	b	c	d
	0	0	0	10

Chương 5

1. Trong những tập hợp số sau đây, những tập nào lập thành một trường (với các phép toán thông thường)

a) tập hợp các số dạng $\left\{\frac{a}{1007}\right\}$, trong đó a nguyên

b) tập hợp các số hữu tỷ

c) tập hợp các số thực

d) tập hợp các số dạng $\left\{\frac{a}{b}\right\}$ trong đó a chẵn, b lẻ

<u>Điểm:</u>	a	b	c	d
	-10	5	5	-8

(Nếu đánh dấu nhiều khả năng thì điểm bằng tổng của điểm các khả năng đó)

2. Tồn tại các trường có k phần tử, trong đó

a) $k=17$

b) $k=24$

c) $k=27$

d) $k=39$

<u>Điểm:</u>	a	b	c	d
	5	-5	5	-5

(Nếu đánh dấu nhiều khả năng thì điểm bằng tổng của điểm các khả năng đó)

3. Cho F_q là trường có q phần tử. Khi đó số phép tính bit cần thiết để nhân (hoặc chia) hai phần tử của trường F_q là:

a) $O(q)$

b) $O(\log q)$

c) $O(\log^2 q)$

d) $O(\log^3 q)$

<u>Điểm:</u>	a	b	c	d
	0	2	4	10

4. Cho $a(t)$, $b(t)$, $c(t)$ là các đa thức hệ số phức, nguyên tố cùng nhau từng cặp và $a(t)+b(t)=c(t)$. Khi đó

a) Bậc của $a(t)$ lớn hơn số các nghiệm phân biệt của đa thức abc .

b) Bậc của mỗi đa thức a , b , c đều nhỏ hơn số nghiệm phân biệt của đa thức abc

c) Nói chung không thể so sánh bậc của các đa thức a , b , c với số nghiệm phân biệt của đa thức tích abc

d) Nếu đa thức $a(t)$ có nghiệm bội đủ lớn thì bậc của nó lớn hơn số các nghiệm phân biệt của đa thức abc

<u>Điểm;</u>	a	b	c	d
	0	10	0	0

5. Cho phương trình $x^n + y^n = z^k$. Hãy đánh dấu những trường hợp mà phương trình trên có thể có nghiệm x, y, z là các đa thức hệ số phức, nguyên tố cùng nhau từng đôi một

- a) $n=1997, m=1998, k=1999$
- b) $n=1998, m=1999, k=2000$
- c) $n=1, m=1998, k=1999$
- d) $n=2, m=1997, k=1998$

<u>Điểm;</u>	a	b	c	d
	-3	-3	5	5

(Nếu đánh dấu nhiều khả năng thì điểm bằng tổng của điểm các khả năng đó)

Chương 6

1. Trong các ma trận cấp 2 sau đây, ma trận nào có thể dùng làm khoá để lập mã khối hai chữ (với 24 chữ cái)

$$a) \begin{pmatrix} 19 & 12 \\ 2 & 9 \end{pmatrix}$$

$$b) \begin{pmatrix} 24 & 11 \\ 5 & 6 \end{pmatrix}$$

$$c) \begin{pmatrix} 19 & 5 \\ 22 & 10 \end{pmatrix}$$

$$d) \begin{pmatrix} 20 & 10 \\ 16 & 2 \end{pmatrix}$$

<u>Điểm;</u>	a	b	c	d
	5	5	-5	-5

(Nếu đánh dấu nhiều khả năng thì điểm bằng tổng của điểm các khả năng đó)

2. Đánh dấu những câu đúng

- a) Thuật toán lập mã mã có thời gian mũ
- b) Thuật toán giải mã mã có thời gian mũ
- c) Thuật toán giải mã mã có thời gian dưới mũ
- d) Thuật toán lập mã và giải mã mã đều có thời gian đa thức

<u>Điểm;</u>	a	b	c	d
--------------	---	---	---	---

-10 -5 10 -5

(Nếu đánh dấu nhiều khả năng thì điểm bằng tổng của điểm các khả năng đó)

3. Đánh dấu những câu đúng

a) Trong hệ mật mã khoá công khai, các khoá lập mã và giải mã đều được thông báo công khai

b) Chỉ có khoá lập mã được thông báo

c) Chỉ có khoá giải mã được thông báo

d) Thuật toán lập mã thường có thời gian đa thức, thuật toán giải mã thường có thời gian mũ hoặc dưới mũ

<u>Điểm:</u>	a	b	c	d
	-5	5	-10	5

(Nếu đánh dấu nhiều khả năng thì điểm bằng tổng của điểm các khả năng đó)

4. Trong các cặp số (e, n) sau đây, những cặp số nào có thể dùng làm khoá lập mã của hệ mã mũ

a) $e=8, n=1996$

b) $e=4, n=3992$

c) $e=9, n=1996$

d) $e=5, n=3992$

<u>Điểm:</u>	a	b	c	d
	-5	-5	5	5

(Nếu đánh dấu nhiều khả năng thì điểm bằng tổng của điểm các khả năng đó)

5. Trong cặp số (e, n) sau đây, những cặp số nào có thể dùng làm khoá lập mã của hệ RSA

a) (27, 1998)

b) (27, 1961)

c) 27, 2183)

d) (31, 3599)

<u>Điểm:</u>	a	b	c	d
	-3	-3	-3	10

(Nếu đánh dấu nhiều khả năng thì điểm bằng tổng của điểm các khả năng đó)

Chương 7

1. Trong các phương trình sau đây, phương trình nào xác định đường cong elliptic trên trường thực

- a) $y^2 - x^3 = 0$ b) $y^2 - x^3 + x = 0$
 c) $y^3 - x^3 + 1 = 0$ d) $y^2 - x^2 + 1 = 0$

<u>Điểm;</u>	a	b	c	d
	0	10	0	0

2. Trong các phương trình sau đây, phương trình nào xác định đường cong elliptic trên trường F_3

- a) $y^2 - x^3 = 0$ b) $y^2 - x^3 + 1 = 0$
 c) $y^2 - x^4 + 1 = 0$ d) $y^2 - x^3 + x + 1 = 0$

<u>Điểm;</u>	a	b	c	d
	0	0	0	10

3. Cho P là điểm trên đường cong elliptic E trên trường hữu hạn F_q . Khi đó

- a) Nếu k là một số nguyên dương thì thuật toán tìm $kP \in E$ có thời gian mũ
 b) Nếu k là một số nguyên dương thì thuật toán tìm điểm $kP \in E$ có thời gian đa thức
 c) Biết các điểm P và $Q = kP$, thuật toán tìm k có thời gian đa thức
 d) Biết các điểm P và $Q = kP$, thuật toán tìm k có thời gian mũ

<u>Điểm;</u>	a	b	c	d
	-5	5	-5	5

(Nếu đánh dấu nhiều khả năng thì điểm bằng tổng của điểm các khả năng đó)

4. Để xây dựng mật mã khoá công khai sử dụng đường cong elliptic, ta cần: đường cong elliptic E trên trường F_q , một điểm B dùng làm cơ sở, mỗi người chọn một số nguyên e_j làm khoá. Những phần tử sau đây sẽ được thông báo công khai (chỉ được chọn một khả năng khi làm bài)

- a) E b) E, B c) E, B, e_j d) $E, B, e_j B$

<u>Điểm;</u>	a	b	c	d
	2	3	0	10