VNU-HUS MAT3500: Toán rời rạc

Bài tập Lý thuyết số cơ bản I

Hoàng Anh Đức

Bộ môn Tin học, Đại học KHTN, ĐHQG Hà Nội
hoanganhduc@hus.edu.vn

Bài tập 1. Biểu diễn các số nguyên sau dưới dạng nhị phân

(a) 231

(b) 4532

(c) 97644

Bài tập 2. Tính tổng và tích các số nhị phân sau

(a) $(1000111)_2$ và $(1110111)_2$

(b) $(11101111)_2$ và $(10111101)_2$

Bài tập 3. Sử dụng thuật toán tính $b^n \bmod m$ thông qua biểu diễn nhị phân của n để tính $7^{644} \bmod 645$.

Bài tập 4. Tính các biểu thức sau

(a) $(-133 \bmod 23 + 261 \bmod 23) \bmod 23$

(b) $((457 \bmod 23) \cdot (182 \bmod 23)) \bmod 23$

(c) $(99^2 \bmod 32)^3 \bmod 15$

(d) $(3^4 \bmod 17)^2 \bmod 11$

Bài tập 5. Chứng minh rằng nếu $a \equiv b \pmod{m}$ và $c \equiv d \pmod{m}$, trong đó a, b, c, d và m là các số nguyên thỏa mãn $m \geq 2$, thì $a - c \equiv b - d \pmod{m}$.

Bài tập 6. Giá trị của hàm Euler ϕ tại số nguyên dương n được định nghĩa là số các số nguyên dương nhỏ hơn hoặc bằng n và nguyên tố cùng nhau với n. Ví dụ, $\phi(6) = 2$ vì trong các số nguyên dương nhỏ hơn hoặc bằng 6, chỉ có 1 và 5 là nguyên tố cùng nhau với 6.

(a) Tính $\phi(4)$, $\phi(10)$, và $\phi(13)$.

(b) Chứng minh rằng n là số nguyên tố khi và chỉ khi $\phi(n) = n - 1$

Bài tập 7. Chứng minh rằng với mọi số nguyên dương n, tồn tại một dãy n hợp số liên tiếp. (**Gợi ý:** Xét dãy số nguyên liên tiếp bắt đầu từ $(n + 1)! + 2$.)

Bài tập 8. Tìm $\gcd(92928, 123552)$ and $\operatorname{lcm}(92928, 123552)$, và kiểm tra lại rằng $\gcd(92928, 123552) \cdot \operatorname{lcm}(92928, 123552) = 92928 \cdot 123552$. (**Gợi ý:** Phân tích 92928 và 123552 thành tích các thừa số nguyên tố.)

Bài tập 9. Sử dụng thuật toán Euclid để tìm

(a) $\gcd(12, 18)$

(b) $\gcd(111, 201)$

(c) $\gcd(1001, 1331)$

Bài tập 10. Biểu diễn ước chung lớn nhất của các cặp số sau dưới dạng tổ hợp tuyến tính của chúng

(a) $10, 11$

(b) $21, 44$

(c) $36, 48$

(d) $34, 55$

(e) $117, 213$

Bài tập 11. Chứng minh rằng tích của ba số nguyên liên tiếp bất kỳ chia hết cho 6

Bài tập 12. Chứng minh rằng nếu a, b, m là các số nguyên với $m \geq 2$ và $a \equiv b \pmod{m}$ thì $\gcd(a, m) = \gcd(b, m)$. (**Gợi ý:** Chứng minh tập các ước chung của a và m bằng với tập các ước chung của b và m.)

Bài tập 13 ($\star$)**.** Chứng minh rằng nếu a và b đều là các số nguyên dương thì

$$(2^a - 1) \bmod (2^b - 1) = 2^{a \bmod b} - 1$$

(**Gợi ý:** $2^a - 1 = 2^{a-b}(2^b - 1) + 2^{a-b} - 1$.)