Esercizi su nozioni matematiche, sottoinsiemi, bit manipulation

Andrea Ciprietti

29 novembre 2021

Gli esercizi indicati con una $\star$ sono da considerarsi più difficili degli altri.

Esercizio 1. (Molto teorico)

Dati interi a, b e $m \geq 1$, diciamo che $a \equiv b \pmod{m}$ (letto: "a congruo a b modulo m") se $m \mid a-b$.

(a) Dimostrare che, se $a \equiv b \pmod{m}$ e $a' \equiv b' \pmod{m}$, allora

$$a + a' \equiv b + b' \pmod{m}, \quad a - a' \equiv b - b' \pmod{m}, \quad a \cdot a' \equiv b \cdot b' \pmod{m}.$$

(b) Il resto della divisione intera tra a ed m è definito come l'unico intero r tale che $0 \leq r < m$ e si può scrivere $a = mk + r$ per un qualche intero k. Provare che il resto esiste ed è unico.

(c) Dimostrare che, se r è il resto della divisione tra a ed m, $a \equiv r \pmod{m}$. Inoltre, se a e b hanno lo stesso resto nella divisione per m, allora $a \equiv b \pmod{m}$.

(d) Se r ed r' sono i resti di a e a' nella divisione per m, è sempre vero che il resto di $a + a'$ diviso m è $r + r'$? E che il resto di $a \cdot a'$ è $r \cdot r'$?

Esercizio 2. Dati due interi a e b, non entrambi uguali a 0, definiamo il loro massimo comun divisore (gcd, dall'inglese *greatest common divisor*) come il più piccolo intero **positivo** che divide sia a sia b.

(a) Dimostrare che $\gcd(a, b) = \gcd(a, a + b) = \gcd(a, a - b)$. In generale, è vero che $\gcd(a, b) = \gcd(a + b, a - b)$?

(b) Supponiamo ora $a, b \geq 0$ e che non siano entrambi nulli. Cosa produce in output il seguente programma, e che complessità ha?

```
while (a != 0 and b != 0) {
    if (a <= b) b -= a;
    else a -= b;
}

cout << max(a, b) << endl;
```

(c) Come si può modificare il codice di cui sopra in modo che abbia complessità logaritmica in $a + b$?

Esercizio 3. (Molto teorico)

Nel seguito, p è un numero primo. Ricordiamo che un numero primo p ha la proprietà che, se x, y sono numeri interi, allora $p \mid xy$ se e solo se $p \mid x$ o $p \mid y$. Indichiamo inoltre con $r_p(a)$ il resto della divisione di a per p.

(a) Dimostrare che, dato un intero a non divisibile per p, gli interi $r_p(a)$, $r_p(2a)$, $\ldots$, $r_p((p-1)a)$ sono tutti distinti. In particolare, essi coincidono con gli interi $1, 2, \ldots, p-1$, a meno dell'ordine.

(b) Dedurne che, dato a come sopra, esiste ed è unico un intero $1 \leq b < p$ tale che $ab \equiv 1 \pmod{p}$. L'intero b si chiama *inverso moltiplicativo* di a modulo p, ed è spesso denotato con a^{-1}.

(c) ($\star$) Dimostrare che $a^{p-1} \equiv 1 \pmod{p}$ se $p \nmid a$. Questo risultato è noto come Piccolo Teorema di Fermat.
(*Hint:* considerare il prodotto $a \cdot (2a) \cdot (3a) \cdots ((p-1)a)$.)

(d) Concludere che $a^{p-2} \equiv a^{-1} \pmod{p}$.

Esercizio 4. Se n, k sono interi nonnegativi e $n \geq k$, il *coefficiente binomiale* "n su k" è definito come $\binom{n}{k} = \dfrac{n!}{k!(n-k)!} = \dfrac{n(n-1)\cdots(n-k+1)}{k!}$.

(a) Dimostrare che $\binom{n}{k}$ è intero.
(*Hint:* contare in due modi diversi il numero di modi di estrarre k numeri dall'insieme $\{1, 2, \ldots, n\}$, tenendo conto dell'ordine in cui vengono estratti.)

(b) È immediato osservare che $\binom{n}{k} = \binom{n}{n-k}$. Esprimere $\binom{n}{k+1}$ e $\binom{n+1}{k+1}$ in termini di $\binom{n}{k}$, e mostrare poi che vale l'identità

$$\binom{n}{k} + \binom{n}{k+1} = \binom{n+1}{k+1}.$$

(c) Provare che

$$\binom{n}{0} + \binom{n}{1} + \cdots + \binom{n}{n} = 2^n.$$

(*Hint:* 2^n è il numero di sottoinsiemi di $\{1, 2, \ldots, n\}$...)

Esercizio 5. ($\star$) Dato n intero positivo, quanto vale la seguente somma?

$$\sum_{A \subseteq \{1, \ldots, n\}} \sum_{B \subseteq A} |B|.$$

(Dove $|B|$ è la *cardinalità* dell'insieme B, ovvero il numero dei suoi elementi.)

Esercizio 6. Cosa fanno gli operatori tra interi del `C++` `&` (bitwise AND), `|` (bitwise OR), `^` (bitwise XOR), `<<` (shift sinistro), `>>` (shift destro)? Qual è la differenza tra `&` e `&&`, e tra `|` e `||`?

Scrivere un programma che stampa tutti i sottoinsiemi di $\{0, \ldots, n-1\}$ (in un ordine qualsiasi), senza l'uso di funzioni ricorsive.

Esercizio 7. ($\star$) Scrivere un programma che stampi il valore di `k & (-k)` (dove k è un intero positivo rappresentato in un `int`) per diversi valori di k (non troppo grandi). Cosa notate? Sapete spiegare perché succede?

Esercizio 8. ($\star$) Sia n una potenza di 2. Determinare l'output dei seguenti programmi:

```
int ans = 0;

for (int i = 0; i < n; i++) {
    for (int j = 0; j < n; j++) {
        ans += (i ^ j);
    }
}

cout << ans << endl;
```

```
int ans = 0;

for (int i = 0; i < n; i++) {
    for (int j = 0; j < n; j++) {
        ans += (i & j);
    }
}

cout << ans << endl;
```