Università degli Studi Roma Tre
Corso di laurea in Matematica A.A 2011-2012
Crittografia - Esercitazione n.1
12 Marzo 2012
Antonio Cigliola

Sistemi di numerazione e cambiamenti di base

Esercizio 1. Stabilire se esiste una base di numerazione per i sistemi numerici usati nell'Antica Grecia e nell'Antica Roma.

Esercizio 2. Dati i seguenti numeri, rappresentarli nelle basi b accanto indicate[†]:

(i) $(12)_{10}$, $b = 2; 3; 5; 16$;

(ii) $(358)_{10}$, $b = 2; 5; 7; 13$;

(iii) $(100)_{10}$, $b = 2; 4; 8; 16$;

(iv) $(10001)_2$, $b = 3; 5; 10$;

(v) $(10001110010)_2$, $b = 4; 6; 7; 10$;

(vi) $(1201)_3$, $b = 2; 5; 10; 16$;

(vii) $(2304)_5$, $b = 2; 10; 16$;

(viii) $(1AF3C)_{16}$, $b = 2; 5; 10$;

(ix) $(7^5 - 1)_{10}$, $b = 2; 3; 7$;

(x) $(5^3 + 5^2 + 3)_{10}$, $b = 2; 3; 5$.

Esercizio 3. Siano dati un intero naturale $n \geqslant 2$ e $b = n^2 + 1$. Si esprimano in base b i numeri seguenti:

(i) n;

(ii) $n^2 - n$;

(iii) $n^2 + 1$;

(iv) $n^2 + 2$;

(v) $n^2 + 2n$;

(vi) $n^4 + 2n^2 + 1$;

(vii) $(n^2 + 2)^2$;

(viii) n^4;

[†]Si ricordi che nel sistema esadecimale le cifre sono $0, 1, \ldots, 9, A, B, \ldots, F$.

(ix) $n^4 - 1$;

(x) $(n^2 + 1)(n^3 + n)$;

(xi) n^5;

(xii) $n^2(n^2 + 2)^2$;

(xiii) $n^3 - n$;

(xiv) $n^5 - n$;

(xv) $n^8 - 1$.

Complessità computazionale

Esercizio 4. Siano f e g due successioni di numeri reali positivi. Dimostrare le asserzioni seguenti.

(i) Se esiste finito il $\lim_{n\to\infty} \dfrac{f(n)}{g(n)} = l \neq 0$ allora $f \asymp g$, ovvero f e g sono dello stesso ordine.

(ii) Se $\lim_{n\to\infty} \dfrac{f(n)}{g(n)} = \infty$ allora $g \in \mathcal{O}(f)$, ovvero f domina g.

(iii) Se esiste finito il $\lim_{n\to\infty} \dfrac{f(n)}{g(n)} = 0$ allora $f \in \mathcal{O}(g)$, overo g domina f.

(iv) Se non esiste il $\lim_{n\to\infty} \dfrac{f(n)}{g(n)}$ allora non si può dedurre nulla, né che $f \in \mathcal{O}(g)$ né che $f \notin \mathcal{O}(g)$.

Esercizio 5. Confrontare, se possibile, le coppie di successioni di numeri reali sotto indicate:

(i) $f(n) = n^2 + 1 + (-1)^n n^2$ e $g(n) = n^2 + 1 - (-1)^n n^2$;

(ii) $f(n) = n^3 - n^2 + sin(2\pi n)$ e $g(n) = n^4 + (-1)^n$;

(iii) $f(n) = \log n + 3n^2 + \sqrt{5}$ e $g(n) = 2n^2 + \arctan n$;

(iv) $f(n) = n^2$ e $g(n) = (2 + (-1)^n)n^2$;

(v) $f(n) = 3n^4 - \arcsin\left(\frac{1-n}{n^3}\right)$ e $g(n) = \sqrt{n^2 - 2n + 3}$;

(vi) $f(n) = e^{3-n}$ e $g(n) = e^{-n}[2 + \cos(n\pi)]$.

Esercizio 6. Sia n un numero naturale e sia k_n il numero delle sue cifre. Provare che k_{n^3} può assumere i valori $3k_n$, $3k_n - 1$ o $3k_n - 2$. Si produca un esempio esplicito per ciascuno dei tre casi possibili.

Esercizio 7. Dati n ed $s \geqslant 2$ interi naturali, provare che

$$sk_n - s + 1 \leqslant k_{n^s} \leqslant sk_n.$$

Esercizio 8. Dopo aver ricordato il test di primalità di Wilson, se ne indichi la complessità computazionale.

Esercizio 9. Stimare la complessità computazionale del crivello di Eratostene per decidere della primalità di un numero $n \in \mathbb{N}$.

Esercizio 10. Sia $n \in \mathbb{N}$ un intero naturale. Stimare la complessità computazionale per il calcolo delle somme $s_1 = 1 + 2 + \cdots + n$, $s_2 = 1 + 4 + 9 + \cdots + n^2$ ed $s_3 = 1 + 8 + 27 + \cdots + n^3$. Esistono delle stime migliori?

Esercizio 11. Siano $f(x) \in \mathbb{Z}[x]$ un polinomio a coefficienti interi ed $a \in \mathbb{Z}$ un intero. Stimare la complessità computazionale della valutazione di $f(x)$ in a. Esiste una procedura che comporta una complessità minore?

Esercizio 12. Siano $A \in \mathcal{M}_{r,n}(\mathbb{Z})$ e $B \in \mathcal{M}_{n,s}(\mathbb{Z})$, con $|a_{ij}| \leqslant m$ e $|b_{ij}| \leqslant k$. Stimare la complessità computazionale per calcolare il prodotto AB in funzione di r, n, s, m, k.

Esercizio 13. Dimostrare che

$$\lim_{n\to\infty} \frac{\log(n!)}{n \log n} = 1.$$

Dedurne che $k_{n!} \asymp k_{n \log n}$.

Il teorema dei numeri primi

Esercizio 14. Si indichi con p_n l'n-simo numero primo. Provare che il teorema dei numeri primi, secondo cui $\pi(n) \sim \frac{n}{\log n}$, equivale a dire che $p_n \sim n \log n$.

Esercizio 15. Si indichi con p_n l'n-simo numero primo. Provare che p_n ed n hanno asintoticamente lo stesso numero di cifre.

Esercizio 16. Si indichi con p_n l'n-simo numero primo. Provare che

$$\lim_{n\to\infty} \frac{p_n}{n \log(p_n)} = 1.$$

Esercizio 17. Sia $n \in \mathbb{N}$, $n \geqslant 2$. Si supponga di avere la lista $\{p_1, p_2, \ldots, p_{s_n}\}$ dei numeri primi minori di n. Sia $P = \prod_{i=1}^{s_n} p_i$.

(a) Stimare in funzione di n il numero di cifre di P.

(b) Stimare in funzione di n il tempo di calcolo di P.

(c) Provare che $\varphi(P^2) = P\varphi(P)$.

Esercizio 18. Provare che

$$\prod_{p \text{ primo}} \frac{1}{1 - \frac{1}{p}} = \infty.$$

Esercizio 19. Dimostrare che

$$\sum_{p \text{ primo}} \frac{1}{p} = \infty.$$

Esercizio 20. Esibire due successioni divergenti di numeri naturali $\{a_n\}_{n\in\mathbb{N}}$ e $\{b_n\}_{n\in\mathbb{N}}$ tali che $\lim_{n\to\infty} \frac{\varphi(a_n)}{a_n} = 1$ mentre $\lim_{n\to\infty} \frac{\varphi(b_n)}{b_n} = 0$.