

Università degli Studi Roma Tre  
Corso di Studi in Matematica  
CR410 – Crittografia a chiave pubblica  
Esercizi  
Foglio 1

1. Dimostrare che

- (a) se  $\lim_{n \rightarrow \infty} \frac{f(n)}{g(n)} = \infty$ , allora  $g \in \mathcal{O}(f)$ ;
- (b) se  $\lim_{n \rightarrow \infty} \frac{f(n)}{g(n)} = 0$ , allora  $f \in \mathcal{O}(g)$ ;
- (c) se  $\lim_{n \rightarrow \infty} \frac{f(n)}{g(n)} = l \neq 0$ , allora  $f \in \mathcal{O}(g)$  e  $g \in \mathcal{O}(f)$ .

2. Siano  $a \geq b > 0$  interi, e sia  $k$  la lunghezza di  $a$ . Dare una stima della complessità computazionale del calcolo di  $a - b$  e della divisione euclidea  $a = bq + r$ .

**SOL:** sottrazione in  $\mathcal{O}(k)$ , divisione euclidea in  $\mathcal{O}(k^2)$  Si veda il testo Baldoni et al, Aritmetica crittografia e codici, p. 94.

3. (a) Siano:  $a = (10101101)_2$ ,  $b = (110110)_2$ ,  $c = (11111)_2$ .

(b) Svolgere le operazioni indicate senza convertire i numeri in altra base e annotando il numero di operazioni bit utilizzate:

$$a + b, \quad a - b + c, \quad a/b, \quad (a * b)/c, \quad (a + b) * c/(a + c).$$

(c) Convertire  $a, b, c$  in base 10 e in base 16.

(d) Qual è una stima della complessità computazionale del passaggio dalla scrittura binaria a quella decimale (o più in generale in base  $b$ ) per un intero  $n$  di lunghezza  $k$ ?

**SOL:**  $\mathcal{O}(k^2)$  Si veda il testo Baldoni et al, Aritmetica crittografia e codici, p. 99.

4. (a) Consideriamo la sequenza supercrescente 1, 4, 7, 13, 28, 54. Ci sono soluzioni al problema dello zaino per  $b = 75$ ? E per  $b = 76$ ?

**SOL:** sì per 75, no per 76

(b) In un crittosistema di Merkle e Hellman, sia 1, 4, 7, 13, 28, 54 la sequenza supercrescente,  $n = 111$  e  $u = 25$ . Qual è la chiave pubblica per farci mandare messaggi cifrati? Qual è l'inverso di 25 (mod 111)?

**SOL:**  $PK = \{25, 100, 64, 103, 34, 18\}$ ,  $25^{-1} = 40$

(c) Cifrare il messaggio **forse** usando la tabella di conversione fra lettere e stringhe binarie presentata a lezione.

**SOL:** (98, 223, 167, 59, 100)

5. Dimostrare il Piccolo Teorema di Fermat: Se  $p$  è un numero primo, allora  $a^p \equiv a \pmod{p}$ .

**SOL:** Si può vedere per esempio il testo Baldoni et al, Aritmetica crittografia e codici, esercizio A4.11.

6. Calcolare  $2^{258} \pmod{259}$ . Cosa si può dedurre da questo conto sul numero 259?

**SOL:**  $2^{258} \equiv 64 \pmod{259}$ . 259 non è primo.

7. Dopo avere semplificato il conto, usando il teorema di Eulero-Fermat, calcolare

$$7^{73} \pmod{60}; \quad 4^{312} \pmod{75}.$$

**SOL:** 7, 16

8. Utilizzando il Teorema di Eulero-Fermat calcolare senza svolgere la potenza l'ultima cifra decimale di  $9^{201}$ ,  $7^{222}$  e le ultime due cifre di  $3^{923}$ .

**SOL:** 9, 9, 27 rispettivamente.

9. Calcolare le seguenti potenze:

(a)  $21^{149} \pmod{361}$

(b)  $25^{289} \pmod{1840}$

**SOL:** 355, 905