

Teoria dei numeri e Crittografia

Christian Ferrari

Esercizi

Esercizio 1 Costruire le tavole di addizione e di moltiplicazione di: \mathbb{Z}_2 , \mathbb{Z}_3 , \mathbb{Z}_6 , \mathbb{Z}_7 e \mathbb{Z}_9 .

Esercizio 2 Determinare il massimo comun divisore delle seguenti coppie di numeri, utilizzando l'*algoritmo di Euclide*, e dire se i numeri sono coprimi.

1. (15; 6) [3]
2. (345; 75) [15]
3. (987; 610) [1;coprimi]
4. (1233; 9999) [9]
5. (2345; 350) [35]
6. (37; 6576) [1;coprimi]

Esercizio 3 Determinare le seguenti potenze negli anelli \mathbb{Z}_n dati, utilizzando l'*algoritmo di Legendre*.

1. 2^8 in \mathbb{Z}_5 [1]
2. 3^{21} in \mathbb{Z}_{10} [3]
3. 89^{66} in \mathbb{Z}_{91} [64]
4. 58^{37} in \mathbb{Z}_{77} [9]
5. 9^{34} in \mathbb{Z}_{35} [16]
6. 14^7 in \mathbb{Z}_{33} [20]

Esercizio 4 Determinare, se possibile, gli inversi dei seguenti elementi degli anelli \mathbb{Z}_n dati, utilizzando l'*algoritmo di Euclide esteso*.

1. 2 in \mathbb{Z}_5 [3]
2. 18 in \mathbb{Z}_{35} [2]
3. 6 in \mathbb{Z}_{112} [non esiste]
4. 7 in \mathbb{Z}_{67} [48]
5. 4 in \mathbb{Z}_{17} [13]
6. 5 in \mathbb{Z}_{34} [7]

Esercizio 5 Determinare la funzione $\varphi(n)$ di Euler per i seguenti numeri.

1. $\varphi(4)$ [2]
2. $\varphi(5)$ [4]
3. $\varphi(9)$ [6]
4. $\varphi(10)$ [4]
5. $\varphi(17)$ [16]
6. $\varphi(27)$ [18]

Esercizio 6 Determinare (quando esiste) l'inverso dei numeri dell'esercizio 3 con il piccolo teorema di Fermat e il teorema di Euler.

Esercizio 7

1. Sono dati i seguenti numeri in base b , determinare il numero decimale corrispondente.

- | | |
|--------------------------|------------------|
| (a) $(1011001)_2$ | $[(89)_{10}]$ |
| (b) $(3\ 9\ 1\ 15)_{26}$ | $[(58853)_{10}]$ |
| (c) $(171)_8$ | $[(121)_{10}]$ |
| (d) $(441)_5$ | $[(121)_{10}]$ |
| (e) $(567)_{10}$ | $[(567)_{10}]$ |
| (f) $(3\ 9\ 1\ 15)_{27}$ | $[(65652)_{10}]$ |

2. Determinare le cifre dei seguenti numeri decimali nella base data.

- | | |
|-------------------------------|------------------------|
| (a) $(89)_{10}$ in base 2 | $[(1011001)_2]$ |
| (b) $(89)_{10}$ in base 3 | $[(10022)_3]$ |
| (c) $(35)_{10}$ in base 17 | $[(2\ 1)_{17}]$ |
| (d) $(24)_{10}$ in base 24 | $[(1\ 0)_{24}]$ |
| (e) $(58853)_{10}$ in base 26 | $[(3\ 9\ 1\ 15)_{26}]$ |
| (f) $(65652)_{10}$ in base 27 | $[(3\ 9\ 1\ 15)_{27}]$ |

3. Verificare che

$$(75)_{10} = (300)_5 = (203)_6.$$

Attenzione: Se la base $b > 10$ le cifre $0 \leq \beta_i \leq b - 1$ possono essere composte da due numeri (decimali), esse sono quindi indicate separate da degli spazi.

Esercizio 8 Determinare la lunghezza dei seguenti numeri utilizzando il logaritmo.

$$8 \quad 367 \quad 5654357 \quad 3.5 \cdot 10^3 \quad 6.4 \cdot 10^{32}$$

Esercizio 9 Utilizzare il criterio di primalità basato sul piccolo teorema di Fermat per dimostrare che 8, 15 e 22 *non* sono numeri primi.

Lo scopo degli esercizi seguenti è di applicare le competenze acquisite negli esercizi precedenti al protocollo di ***crittografia RSA***.

Esercizio 10 Per i seguenti valori dei numeri primi p e q determinare una possibile coppia di chiavi pubblica e privata.

1. $p = 5, q = 11$
2. $p = 7, q = 3$
3. $p = 13, q = 5$
4. $p = 19, q = 5$
5. $p = 23, q = 3$
6. $p = 17, q = 29$

Esercizio 11 Eseguire la conversione *testo* \leftrightarrow *numero decimale* per i seguenti messaggi/numeri utilizzando l'alfabeto seguente

$\{ , a, b, c, d, e, f, g, h, i, j, k, l, m, n, o, p, q, r, s, t, u, v, w, x, y, z \}$

in corrispondenza con i 27 numeri $\{0, 1, 2, 3, \dots, 24, 26\}$.

1. $M = 6568$ [i g]
2. **enigma** [79367311]
3. $M = 13636$ [rsa]
4. **segreto** [7436812407]
5. $M = 52802025$ [cripto]

Esercizio 12 Cifrare e decifrare i seguenti numeri con le chiavi date.

1. $M = 6$ con $(e = 13, n = 55)$ e $(d = 37, n = 55)$ [$C = 51$]
2. $M = 2$ con $(e = 17, n = 33)$ e $(d = 13, n = 33)$ [$C = 29$]
3. $M = 17$ con $(e = 11, n = 86)$ e $(d = 23, n = 86)$ [$C = 67$]
4. $M = 55$ con $(e = 29, n = 143)$ e $(d = 29, n = 143)$ [$C = 22$]
5. $M = 11$ con $(e = 73, n = 249)$ e $(d = 9, n = 249)$ [$C = 206$]
6. $M = 26$ con $(e = 25, n = 395)$ e $(d = 25, n = 395)$ [$C = 151$]

Esercizio 13 Con *Excel* costruire gli algoritmi seguenti.

1. Algoritmo di Euclide per l'MCD;
2. algoritmo di Euclide esteso per l'inverso in \mathbb{Z}_n ;
3. algoritmo di scomposizione di un numero decimale in base 27;
4. algoritmo semplice per le potenze in \mathbb{Z}_n .

Esercizio 14 Sono date le chiavi pubblica e privata

$$(e = 12575, n = 21949) \quad (d = 12715, n = 21949) .$$

Eseguire, con l'aiuto degli algoritmi dell'esercizio 13, il protocollo RSA con i seguenti messaggi.

1. `rsa` $[M = 13636, C = 9660]$

2. `mate` $[\text{ma+te: } M_1 = 352, C_1 = 17702; M_2 = 545, C_2 = 21218]$

Esercizio 15 Una spia scopre i seguenti messaggi cifrati C e le chiavi pubbliche (e, n) utilizzati per cifrarli.

1. $C = 373557$ con $(e = 275113, n = 414173)$ `[mate]`

2. $C = 132273$ con $(e = 85311, n = 191329)$

3. $C = 934$ con $(e = 58271, n = 86699)$

4. $C = 20958$ con $(e = 64309, n = 82063)$

Che informazione è necessario avere per decifrare i messaggi cifrati? Cosa è necessario “fare” per ottenere questa informazione?

Rompere poi il codice RSA e scoprire i messaggi originali. Utilizzare gli algoritmi dell'esercizio 13 e *Maple* per fattorizzare n (comando: `ifactor(numero);`).

Esercizio 16 Generare delle chiavi e scambiare messaggi con i compagni utilizzando il protocollo RSA e gli algoritmi *Excel*.