Nome:_____.

Data:_____.

N.B. I riferimenti sono agli *Appunti di Matematica Discreta, Esculapio, 2015*

1. Dare la definizione di Massimo Comun Divisore di due interi a e b, non entrambi nulli. Calcolare poi MCD(1234567,6543) e la corrispondente identità di Bézout. **Soluzione.** Per la definizione vedere Definizione 1.2.3 degli *Appunti*. Per il calcolo usiamo l'algoritmo delle divisioni successive.

$$\begin{gathered}1234567 = 188(6543) + 4483\\ 6543 = 1(4483) + 2060\\ 4483 = 2(2060) + 363\\ 2060 = 5(363) + 245\\ 363 = 1(245) + 118\\ 245 = 2(118) + 9\\ 118 = 13(9) + 1\\ 9 = 9(1) + 0\end{gathered}$$

   Dunque $1 = MCD(1234567, 6543)$. Per ottenere la sua espressione mediante l'identità di Bézout, risaliamo a ritroso.

$$\begin{gathered}1 = 118 - 13 \times 9 = 118 - 13 \times (245 - 2 \times 118)\\ = 27 \times 118 - 13 \times 245 = 27(363 - 245) - 13 \times 245\\ = 27 \times 363 - 40 \times 245 = 27 \times 363 - 40(2060 - 5 \times 363)\\ = 227 \times 363 - 40 \times 2060 = 227(4483 - 2 \times 2060) - 40 \times 2060\\ = 227 \times 4483 - 494 \times 2060 = 227 \times 4483 - 494(6543 - 4483)\\ = 721 \times 4483 - 494 \times 6543 = 721(1234567 - 188 \times 6543) - 494 \times 6543\\ = 721(1234567) - 136042(6543)\end{gathered}$$

2. Dimostrare che il Teorema di Lagrange per i gruppi implica il Piccolo Teorema di Fermat e, più in generale, il Teorema di Eulero. **Soluzione.**Vedere Corollari 2.2.14 e 2.2.15.

3. Enunciare e dimostrare il Teorema Cinese dei resti. **Soluzione.** Vedere Teorema 1.8.4.

4. Indichiamo con $p(n)$ il numero delle partizioni dell'intero n e con $f(n)$ il numero delle partizioni dello stesso intero in parti diverse da 1. Dimostrare che $f(n) = p(n) - p(n-1)$. (È possibile dare una dimostrazione usando le funzioni generatrici oppure stabilendo una corrispondenza biunivoca. Punti in più saranno dati per chi risolve l'esercizio in entrambe le maniere). **Soluzione mediante le funzioni generatrici.** Sia $\mathcal{E}(x) = \sum_{n=0}^{\infty} p(n)x^n$ la funzione generatrice di $p(n)$ e sia $\mathcal{F}(x) = \sum_{n=0}^{\infty} f(n)x^n$ la funzione generatrice di $f(n)$. Il Teorema 6.1.4 ci dà una formula per $\mathcal{E}(x)$ e fornisce

anche un metodo per costruire la funzione generatrice $\mathcal{F}(x)$. Si ha infatti

$$\mathcal{E}(x) = \prod_{n=1}^{\infty} \frac{1}{1-x^n}$$

mentre

$$\mathcal{F}(x) = \prod_{n=2}^{\infty} \frac{1}{1-x^n} = (1-x)\mathcal{E}(x)$$

Se prendiamo il coefficiente di x^n di $\mathcal{F}(x)$ abbiamo $f(n)$ per definizione. La relazione appena dimostrata ci fa vedere che tale coefficiente deve essere uguale al coefficiente di x^n in $(1-x)\mathcal{E}(x)$ e questo è $p(n) - p(n-1)$ come desiderato. **Soluzione mediante una corrispondenza biunivoca.** Fissato un intero positivo n, sia $\mathcal{P}_n$ l'insieme di tutte le partizioni di n e sia $\mathcal{F}_n$ l'insieme di quelle partizioni che non hanno parti uguali a 1. Una partizione di n è di due tipi: o contiene parti uguali a 1 oppure non le contiene. Quelle che non contengono 1 sono, per definizione, in numero di $f(n)$. Dobbiamo solo dimostrare che le partizioni di n in cui almeno una parte è uguale a 1 sono in corrispondenza biunivoca con le partizioni di $n-1$. La corrispondenza è la seguente: se una partizione di n ha almeno una parte uguale a 1, cancello quella parte e ottengo una partizione di $n-1$. Viceversa, se ho una qualunque partizione di $n-1$ e aggiungo una parte uguale a 1 ottengo una partizione di n con almeno una parte uguale a 1.

5. Costruire un campo finito con 8 elementi. Calcolarne la tabella moltiplicativa. **Soluzione.** Occorre partire dal campo $\mathbb{F}_2$ e trovare un polinomio di terzo grado irriducibile su questo campo. Vedere esempi dopo il Teorema 2.6.2.

6. Supponiamo che Beatrice abbia chiave pubblica $(1003, 3)$ e quindi chiave privata 619. Se Beatrice riceve il messaggio crittato $C = 722$ qual è l'equivalente numerico del testo in chiaro? **Soluzione.** Vedere esempio 3.5.1

7. Data la matrice a coefficienti nel campo con due elementi $\mathbb{F}_2$

$$H = \begin{pmatrix} 1 & 1 & 0 & 1 & 0 & 1 \\ 1 & 1 & 0 & 0 & 1 & 0 \\ 1 & 0 & 1 & 1 & 0 & 0 \end{pmatrix}$$

determinare tutte le parole del codice definito da $H\mathbf{x} = \mathbf{0}$. **Soluzione.** (Confronta Esercizio 5 della sezione 9.8). Si tratta di risolvere un sistema lineare omogeneo su $\mathbb{F}_2$. Si può applicare il metodo di Gauss alla matrice ed ottenere la matrice a gradini ridotta

$$H = \begin{pmatrix} 1 & 0 & 1 & 0 & 1 & 1 \\ 0 & 1 & 1 & 0 & 0 & 1 \\ 0 & 0 & 0 & 1 & 1 & 1 \end{pmatrix}$$

si trovano le tre soluzioni di base: $x = 111000, y = 100110, z = 110101$. Tutte le altre sono combinazioni lineari di queste a coefficienti in $\mathbb{F}_2$ e cioè

$$0, x, y, z, x + y, x + z, y + z, x + y + z$$

otto in tutto.

8. Scrivere la funzione generatrice della successione di Lucas definita da

$$L_0 = 2, L_1 = 2, L_{n+2} = L_{n+1} + L_n, n \geq 1$$

e determinare una formula chiusa per il termine L_n. **Soluzione.** (Confronta esercizio in sezione 5.2.1) Sappiamo (v.Teorema 5.4.1) che la funzione generatrice è del tipo

$$f(x) = \frac{a + bx}{1 - x - x^2}$$

dove il denominatore si ottiene a partire dal polinomio caratteristico che, per la successione di Lucas, è lo stesso di quella di Fibonacci. Imponendo che $f(0) = a = 2$ e che $f'(0) = a + b = 1$ si deduce che $a = -1$ e $b = 2$ la funzione desiderata è quindi

$$f(x) = \frac{2 - x}{1 - x - x^2}$$

Per la formula chiusa, ricordiamo il Teorema 5.3.4, essa sarà del tipo

$$a\phi^n + b\hat{\phi}^n$$

dove ϕ e $\hat{\phi}$ sono come negli *Appunti*. Ricordiamo anche che $\phi^2 = \phi + 1$ e $\hat{\phi}^2 = \hat{\phi} + 1$. Abbiamo quindi

$$a\phi + b\hat{\phi} = 2$$

$$a\phi^2 + b\hat{\phi}^2 = 1$$

da cui possiamo dedurre che $a = b = 1$. La formula desiderata è quindi $L_n = \phi^n + \hat{\phi}^n$.

9. Dimostrare che se n è un intero non negativo allora

$$\binom{2n}{n} = \sum_{k=0}^{n} \binom{n}{k}^2$$

Soluzione. Vedi esercizio nel paragrafo 7.3.3.

10. Dimostrare che in un grafo semplice non orientato, finito, la somma dei gradi di tutti i vertici è uguale a due volte il numero degli archi (o lati). (Handshaking lemma). **Soluzione.** Vedi Proposizione 8.1.14.