Jorge Vitória, email: jorge.vitoria@unica.it
Sergio Pavon, email: sergio.pavon@math.unipd.it
Università di Studi di Cagliari, 2019/2020
Corso di Laurea in Informatica

Esercizi per il Corso di MATEMATICA DISCRETA

Foglio 6
8 novembre 2019

1. Si dimostrino i seguenti criteri di divisibilità.[1]

   (a) Un numero intero n è divisibile per 3 se e solo se la somma delle sue cifre (in base 10) è divisibile per 3.

   (b) Un numero intero n è divisibile per 9 se e solo se la somma delle sue cifre (in base 10) è divisibile per 9.

   (c) Un numero intero n è divisibile per 3 se e solo se la somma alternata delle sue cifre (in base 10) è zero.

2. Si determinino tutti gli elementi di $\mathbb{Z}_{10}$, $\mathbb{Z}_{11}$ e $\mathbb{Z}_{12}$ che hanno inversi moltiplicativi. Per ogni tale elemento si trovi il suo inverso.

3. Si determini quali delle seguenti equazioni modulari hanno soluzioni. In caso ci siano soluzioni, si trovino tutte le soluzioni.

   (a) $3x \equiv 1 \pmod 7$
   (b) $3x \equiv 1 \pmod{12}$
   (c) $3x \equiv 0 \pmod{12}$
   (d) $12x \equiv -4 \pmod{11}$
   (e) $90x \equiv 12 \pmod{42}$
   (f) $24x \equiv -2 \pmod{20}$
   (g) $40x \equiv -5 \pmod{25}$

4. Per ogni a, si determinino il resto r delle divisione per n.

   (a) $a = 20^{20}$, $n = 21$;
   (b) $a = 32^{300}$, $n = 21$;
   (c) $a = 7^{102}$, $n = 51$;
   (d) $a = 43^{22}$, $n = 17$;
   (e) $a = 2020^{2020}$, $n = 9$;
   (f) $a = 22^{76}$, $n = 13$;
   (g) $a = 14^{115}$, $n = 9$

5. Si consideri la il cifrario definito della seguente permutazione

   $$(AFZGU)(RPBC)(VZMO)(HEL).$$

   Si decripti il seguenti messaggio:

   $$REL\ \ BIFRLPL\ \ DLRPIBTFPL\ \ OLSSFUUI$$

[1] **Suggerimento:** Si scriva il un numero n come una somma di potenze di base 10 moltiplicate per le cifre di n. Si usino le proprietà additive e moltiplicative delle congruenze modulo 3, 9 o 11 per dimostrare le affermazioni.

6. Con l'uso del cifrario generalizzato di Cesare che ad ogni lettera associa la lettera 5 posizioni più avanti, si cripti il messaggio

$$IN\ \ BOCCA\ \ AL\ \ LUPO$$

7. Si consideri il cifrario affine definito da $x \mapsto 4x + 3 (\mathsf{mod}\ 21)$.

   (a) Si dimostri che, infatti, questa è una corrispondenza biettiva e si scriva la corrispondente permutazione dell'alfabeto.

   (b) Si trovi la regola di corrispondenza del cifrario inverso attraverso l'uso di congruenze.

   (c) Si decripti il messaggio: $EGNBEGNTQG\ \ UTHQDBNG$.

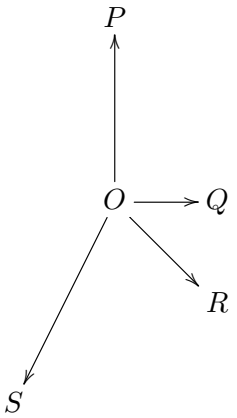
8. Il mittente M vuole inviare un codice numerico ad un destinatario D in modo criptato. La chiave pubblica RSA di D è $(N = 35, e = 5)$.

   (a) Si verifichi che la chiave pubblica di D è valida.

   (b) M vuole inviare in modo criptato il codice 14 a D. Si trovi il messaggio criptato che M deve inviare.

   (c) Se D riceve come messaggio criptato 7, quale è il corrispondente messaggio decriptato?

9. Si considerino i seguenti vettori.



   (a) Si sa che ognuna delle seguenti combinazioni lineari corrisponde ad un solo vettore fra questi quattro. Si trovi quale vettore è descritto in queste combinazioni lineari.

      i. $(-1) \cdot \vec{OS} + (-1) \cdot \vec{OQ}$
      ii. $\vec{OQ} - \frac{1}{2}\vec{OP}$
      iii. $2\vec{OQ} + \frac{1}{2}\vec{OS}$

   (b) Usando le espressioni trovate sopra, si scrivino le coordinate di tutti quattri vettori rispetto alle seguenti basi:

      i. $B_1 = \{\vec{OP}, \vec{OQ}\}$;
      ii. $B_2 = \{\vec{OQ}, \vec{OR}\}$;
      iii. $B_3 = \{\vec{OS}, \vec{OP}\}$.

Alcuni risultati del Foglio 4

3 (a) 248831; (b) 7776; (c) 77760; (d) 32768.

4 (a) $45 + 10^3 + 10^4 + 10^5 = 111045$; (b) $720 + 5040 + 10^5 + 10^6 = 1105760$.