TEN 2019. Esercizi1. (RSA, gcd, φ di Eulero, gruppi)

Notazione: Indichiamo con $\log n$ il logaritmo di n in base 2 e con $\ln n$ il logaritmo naturale di n, in base e.

1. Determinare le soluzioni dell'equazione $\bar{x}^2 = \bar{1}$ in $\mathbb{Z}_{11}$ e in $\mathbb{Z}_{15}$.
2. A partire dalla relazione $151262756 \cdot 48587659769876 - 596987687 \cdot 12310979747865 = 1$, calcolare:

   $\gcd(151262756, 596987687)$, $\gcd(48587659769876, 12310979747865)$; $\overline{596987687}^{-1} \in \mathbb{Z}^*_{48587659769876}$.

   Quali altri inversi possiamo ottenere dalla stessa relazione?
3. Sia $n = 2020$. Esibire qualche elemento di $\mathbb{Z}^*_{2020}$. Calcolare 11^{-1} in $\mathbb{Z}^*_{2020}$.
4. Siano E_1 ed E_2 numeri naturali con $gcd(E_1, E_2) = 1$. Determinare m, conoscendo

   $$m^{E_1} \mod N \qquad \text{ed} \qquad m^{E_2} \mod N.$$

5. Sia $(G, \cdot)$ un gruppo.
   (a) Verificare che l'elemento neutro e di G è unico.
   (b) Verificare che per ogni $x \in G$, l'inverso x^{-1} di x in G è unico.
6. (*prodotto diretto di gruppi*) Siano $(G_1, e_1, \circ)$ e $(G_2, e_2, *)$ due gruppi.
   (a) Verificare che il prodotto cartesiano $G_1 \times G_2$, col prodotto definito da $(x_1, x_2) \cdot (y_1, y_2) := (x_1 \circ x_2, y_1 * y_2)$, è un gruppo.
   (b) Determinare l'elemento neutro di $G_1 \times G_2$ rispetto al prodotto così definito.
   (c) Determinare l'inverso di $(x_1, x_2) \in G_1 \times G_2$ rispetto al prodotto così definito.
   (d) Verificare che se G_1 e G_2 sono abeliani, anche $G_1 \times G_2$ è abeliano.
   (e) Siano $(G_1, e_1, \circ) = (\mathbb{Z}_2, \bar{0}, +)$ e $(G_2, e_2,) = (\mathbb{Z}_3, \bar{0}, +)$. Scrivere la tabella moltiplicativa del gruppo $(\mathbb{Z}_2 \times \mathbb{Z}_3, +)$.
7. Sia G un gruppo tale che $g^2 = e$, per ogni $g \in G$. Dimostrare che G è abeliano.
8. Sia $p = 7$. Determinare l'inverso moltiplicativo di ogni elemento $\bar{a} \in \mathbb{Z}^*_7$.
9. Considerare i seguenti gruppi di ordine 4 e scrivere le rispettive tabelle moltiplicative.
   (a) $A = \{1, -1, i, -i\}$ con l'operazione data dalla moltiplicazione fra numeri complessi.
   (b) $\mathbb{Z}_4$ con la somma fra classi resto.
   (c) $\mathbb{Z}_2 \times \mathbb{Z}_2$ con la somma definita da $(\bar{x}, \bar{y}) + (\bar{u}, \bar{v}) = (\overline{x+u}, \overline{y+v})$.
   (d) $\mathbb{Z}^*_5$ col prodotto fra classi resto.
   (e) $\mathbb{Z}^*_{12}$ col prodotto fra classi resto.
   (f) $\mathbb{Z}^*_8$ col prodotto fra classi resto.
10. Sia $p \in \mathbb{N}$ un numero primo. Verificare che in $\mathbb{Z}_p$ vale l'uguaglianza $(\bar{x} + \bar{y})^p = \bar{x}^p + \bar{y}^p$, per ogni $\bar{x}, \bar{y} \in \mathbb{Z}_p$ (suggerimento: usare la formula di Newton).
    Verificare che per $n = 4$, tale uguaglianza non vale.
11. Dimostrare che $\sum_{\bar{x} \in \mathbb{Z}_n} \bar{x} = \bar{0}$ in $\mathbb{Z}_n$, per ogni n dispari.
12. Calcolare $(p-1)!$ in $\mathbb{Z}_p$, per p primo.
13. Sia $F\colon \mathbb{Z}_{15} \to \mathbb{Z}_3 \times \mathbb{Z}_5$, $\bar{x} \mapsto (\bar{x} \bmod 3, \bar{x} \bmod 5)$.
    (a) Determinare esplicitamente $F(\bar{x})$, per ogni $\bar{x} \in \mathbb{Z}_{15}$.
    (b) Verificare che $F(\mathbb{Z}^*_{15}) = \mathbb{Z}^*_3 \times \mathbb{Z}^*_5$.
14. Calcolare $\varphi(15^3 \cdot 33 \cdot 2^4 \cdot 27)$.
15. Sia n un intero positivo e sia p un divisore primo di n. Verificare che:
    (a) $\varphi(p) \mid \varphi(n)$;
    (b) se $p^2 \nmid n$, allora $\varphi(n) = \varphi(p)\varphi(\frac{n}{p})$

(c) se $p \mid \frac{n}{p}$, allora $\varphi(\frac{n}{p}) = \frac{n}{p}\prod_d(1-\frac{1}{d})$, dove d varia fra i divisori primi di n.

Esercizi che richiedono PARI/GP:

? presenta la lista dei comandi divisi per argomento
?5 presenta la lista dei comandi utili in Teoria ei Numeri "NUMBER THEORETICAL functions"
?comando spiega l'uso del comando.

Esempi:
gcd(986987987,69797987)
43
bezout(986987987,69797987)
[-216252, 3057941, 43]

gcd(7538415671,3674509)
1
bezout(7538415671,3674509)
[609569, -1250557422, 1]

Mod(3674509, 7538415671)$^{-}$1
Mod(6287858249, 7538415671)

Mod(-1250557422,7538415671)
Mod(6287858249, 7538415671)

isprime(76876876)
0

factor(76876876)
[2 2]
[19219219 1]

1. Sia $n = 486587657577$. Decidere se le classi di congruenza modulo n dei seguenti numeri appartengono o meno a $\mathbb{Z}_n^*$: 58765987, 76577, 5969876 ed eventualmente calcolarne l'inverso.
6. Siano dati due primi p, q primi dell'ordine di grandezza di 10^{250}. Costruire un KIT di chiavi $\{N = p \cdot q,\ E, D\}$ per un utente del sistema crittografico RSA. Spedire all'utente il messaggio

$$m = 11111$$

dopo averlo criptato. Provare poi a decriptarlo con la chiave segreta.
Qual è la complessità totale di tutta l'operazione? E scegliendo p, q dell'ordine di grandezza di 10^{400}?

1. *Due utenti RSA* **non devono** *avere chiavi pubbliche N_1 ed N_2 con un fattore comune.* Creare due interi di 600 cifre $N_1 = p * q$ ed $N_2 = p * r$, dove p, q, r sono primi di circa 300 cifre. Verificare che il comando $\gcd(N_1, N_2)$ calcola il fattore comune, anche se i numeri non sono fattorizzabili con gli algoritmi a disposizione.

1. Calcolare $\varphi(765765786)$.