Matematica Discreta. Esercizi 6. Funzione φ di Eulero, test di primalità, RSA. Roma, 11 aprile 2008.

NOTA: Per fattorizzare i numeri, andare sul sito `http://www.alpertron.com.ar/ECMC.HTM`.

1. La *funzione φ di Eulero* è definita da $\varphi(n) = \#\mathbf{Z}_n^*$ (per $n \in \mathbf{N}$).
   (a) Calcolare $\varphi(n)$ per ogni $n \leq 10$.
   (b) Calcolare $\varphi(n)$ nei seguenti casi: $n = 1729,\ 1100,\ 1313,\ 2^3 \cdot 5^3 \cdot 7^2$.
   (c) In ognuno di tali casi enunciare il corrispondente Teorema di Lagrange per $\mathbf{Z}_n^*$.
2. Calcolare $\bar{2}^{300}$ in $\mathbf{Z}_6$. Possiamo usare il Teorema di Lagrange?
3. Calcolare
$$5^{95} \bmod 100, \qquad 2^{1000} \bmod 200.$$
4. Calcolare il resto della divisione per 385 di 3^{302}.
5. (a) Sia $p > 2$ un primo. Dimostrare che $\{x \in \mathbf{Z}_p : x^2 = 1\} = \{\pm 1\}$.
   (b) Determinare tutte le soluzioni dell'equazione $\bar{x}^2 = \bar{1}$ in $\mathbf{Z}_{pq}$, per p, q primi dispari.
   (c) Determinare tutti gli $x \in \mathbf{Z}_{15}^*$ per cui $x^2 = 1$. Stessa domanda per $\mathbf{Z}_{21}^*$.
   (d) Sia n quadrato di un numero primo $p > 2$. Quanti sono gli elementi $x \in \mathbf{Z}_n^*$ con $x^2 = 1$?
   (e) Determinare tutti gli $x \in \mathbf{Z}_9^*$ per cui $x^2 = 1$. Stessa domanda per $\mathbf{Z}_{25}^*$.
6. Usando il Piccolo Teorema di Fermat verificare che i seguenti numeri non sono primi: $n = 33,\ 45,\ 12$.
7. *Criterio di Korselt:* Un intero $n \in \mathbf{N}$ è un numero di Carmichael se e solo se è prodotto di almeno tre primi distinti ed ha la proprietà che se un primo p divide n, allora anche $p - 1$ divide $n - 1$.
   (a) Dimostrare che $561 = 3 \cdot 17 \cdot 31$ è un numero di Carmichael.
   (b) Dimostrare che $1729 = 7 \cdot 13 \cdot 19$ è un numero di Carmichael.
   (b) Dimostrare che $8911 = 7 \cdot 19 \cdot 67$ è un numero di Carmichael.
   (c) Verificare che un numero di Carmichael soddisfa il Piccolo Teorema di Fermat, ossia per ogni $a \in \mathbf{Z}_n^*$, vale $a^{n-1} \equiv 1 \bmod n$.
8. Fare il test di primalità di Miller-Rabin sui numeri $n = 91,\ 101,\ 113,\ 221,\ 2465,\ 8911$, con $a = 2$.
9. Sfruttando l'espressione binaria dell'esponente, calcolare
$$3^{200} \bmod 48, \quad 45^{54} \bmod 91, \quad 12^{256} \bmod 561.$$
10. Siano p e q numeri primi e sia $n = pq$. Siano E, D interi tali che $E \cdot D \equiv 1 \bmod (p-1)(q-1)$. Sia $M \in \mathbf{Z}_n^*$.
    (a) Verificare che $M^{ED} \equiv M \bmod n$.
    (b) Siano $p = 7$, $q = 11$ ed $n = 77$. Determinare una coppia E, D come sopra.
    (c) Sia $M = 15$. Per gli E, D determinati al punto precedente, calcolare $M^E \bmod n$ e verificare che $M^{ED} \equiv M \bmod n$.
11. Il signor Rossi è un utente con chiavi pubbliche $N = 77$ e $E = 17$.
    (a) Spedirgli il messaggio $m = 13$ dopo averlo encriptato.
    (b) Un pirata informatico è riuscito a fattorizzare N ed ha scoperto la chiave segreta D del signor Rossi. Qual è ??

12. Per trasformare un testo in una serie di numeri, usiamo questa tabella.

A	B	C	D	E	F	G	H	I	L	M	N	O	P	Q	R	S	T	U	V	Z	spazio
01	02	03	04	05	06	07	08	09	10	11	12	13	14	15	16	17	18	19	20	21	00

(a) Verificare che il testo "PIPPO BAUDO" viene trasformato in "14091414130000201190413".

Il modulo del sistema RSA usato in questo esercizio è uguale a $n = 2000000002864822776563$. L'esponente pubblico è uguale a $E = 25042003$.

(b) Far vedere che il messaggio "14091414130000201190413" della parte (a), cifrato tramite questo sistema RSA, è uguale a 474795864046624770221.

(c) Supponiamo di intercettare il messaggio cifrato $\tilde{m} = 605233533198702885420$. Cercare di rompere questo sistema e di decifrare e leggere il messaggio. (Suggerimento: trovare la fattorizzazione $n = pq$ e calcolare l'esponente segreto, cioè determinare D tale che $DE \equiv 1 \bmod (p-1)(q-1)$. Il messaggio originale è allora uguale a $\tilde{m}^D \bmod n$.)

13. Usando la tabella di conversione dell'esercizio 9, convertire il messaggio "CIAO" in un numero. Poi cifrarlo per inviarlo all'utente

$$N = 406888839617379160907451419196545509, \quad E = 493127.$$

14. Decifrare il messaggio

$$M1 = 475394238194858892901219990750844 35, \ M2 = 401957449702894899560393214873280330$$

inviato all'utente

$$N = 406888839617379160907451419196545509, \quad E = 493127.$$