NOTA: Per fattorizzare i numeri, andare sul sito
`http://wims.unice.fr/wims/wims.cgi?cmd=new&module=tool/algebra/factor.en`
oppure su `http://www.alpertron.com.ar/ECMC.HTM`.
Per gli esercizi 10–12 è necessario usare PARI/GP.

Sia $\mathbf{Z}_n$ l'anello delle classi di congruenza modulo n e sia $\mathbf{Z}_n^*$ l'insieme degli elementi di $\mathbf{Z}_n$ che hanno un inverso moltiplicativo.

1. Usando il Piccolo Teorema di Fermat verificare che i seguenti numeri non sono primi: $n = 33,\ 45,\ 12$.

Sol. $\bar{2} \in \mathbf{Z}_{33}^*$, ma $\bar{2}^{32} \equiv 4 \not\equiv 1 \bmod 33$;
$\bar{2} \in \mathbf{Z}_{45}^*$, ma $\bar{2}^{44} \equiv 31 \not\equiv 1 \bmod 45$;
$\bar{5} \in \mathbf{Z}_{12}^*$, ma $\bar{5}^{11} \equiv 5 \not\equiv 1 \bmod 12$.

2. Un *numero di Carmichael* è un numero naturale che non è primo, ma soddisfa $x^{n-1} \equiv 1 \pmod{n}$ per ogni $x \in \mathbf{Z}_n^*$.
   (a) Dimostrare che $561 = 3 \cdot 11 \cdot 17$ 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.

Sol. (a) Verifichiamo che per ogni $x \in \mathbf{Z}_{561}^*$ vale $x^{560} \equiv 1 \bmod 561$. Per il Teorema Cinese del Resto, ciò equivale al sistema di congruenze

$$\begin{cases} x^{560} \equiv 1 \bmod 3 \\ x^{560} \equiv 1 \bmod 11 \\ x^{560} \equiv 1 \bmod 17. \end{cases}$$

Osserviamo che se $mcd(x, 561) = 1$, allora anche $mcd(x, 3) = mcd(x, 11) = mcd(x, 17) = 1$, per cui x appartiene a $\mathbf{Z}_3^*$, $\mathbf{Z}_{11}^*$ e $\mathbf{Z}_{17}^*$. Poiché $\varphi(3) = 2$, $\varphi(11) = 10$ e $\varphi(17) = 16$ dividono 560, le tre congruenze sistema sono soddisfatte. Dunque $561 = 3 \cdot 11 \cdot 17$ è un numero di Carmichael, come richiesto.
(b) e (c) si svolgono in modo analogo.

3. *Criterio di Korselt:* Un intero positivo n è un numero di Carmichael se e solo se ha le seguenti proprietà:
   (i) n è privo di fattori quadratici;
   (ii) se un numero primo p divide n, allora $p - 1$ divide $n - 1$.

(Sugg.: usare il fatto che per ogni primo p esiste $g \in \mathbf{Z}_p^*$ di ordine $(p - 1)$).

Sol. Sia n un numero di Carmichael. Per definizione,

$$\text{per ogni } a \in \mathbf{Z}_n^*, \qquad a^{n-1} \equiv 1 \bmod n.$$

(i) Sia p un divisore primo di n. Supponiamo per assurdo che $p^2 \mid n$. Per ottenere una contraddizione costruiamo una classe $a \in \mathbf{Z}_n^*$ per cui *non vale* $a^{n-1} \equiv 1 \bmod n$. Prendiamo per esempio $a = \frac{n}{p} + 1$. Si vede facilmente che $a \in \mathbf{Z}_n^*$ e che $a,\ a^{-1} \not\equiv 1 \bmod n$.
Calcoliamo a^p modulo n con la formula di Newton:

$$a^p = (\frac{n}{p} + 1)^p = \sum_{i=0}^{p} \binom{p}{i} \left(\frac{n}{p}\right)^i \equiv \left(\frac{n}{p}\right)^p + 1 \bmod p$$

(vedi Esercizio 18, Foglio 4); poiché $p \geq 2$, ne segue che $n \mid \left(\frac{n}{p}\right)^p$ e

$$a^p \equiv 1 \bmod n;$$

poiché $n - 1 = p\frac{n}{p} - 1$, otteniamo

$$a^{n-1} = a^{p\frac{n}{p}-1} \equiv a^{-1} \not\equiv 1 \bmod n,$$

come richiesto.

Ripetendo questo ragionamento per divisori primi distinti di n, possiamo concludere che n è privo di fattori quadratici.

(ii)

4. Dimostrare che un numero di Carmichael ha almeno tre fattori primi.

Sol. Sia n un numero di Carmichael (vedi Esercizio 2). Dall'Esercizio 3 segue che n soddisfa (i) e (ii). Supponiamo per assurdo che $n = p_1 \cdot p_2$ sia prodotto di due soli fattori primi $p_2 > p_1 > 1$. Dal fatto che $p_1 \mid n$ implica $p_1 - 1 \mid n - 1$, segue che possiamo scrivere

$$n - 1 = p_1 p_2 - 1 = k(p_1 - 1), \qquad k \in \mathbf{Z}. \tag{$*$}$$

Riducendo l'espressione (*) modulo $(p_1 - 1)$ e sfruttando il fatto che $p_1 \equiv 1 \bmod (p_1 - 1)$, troviamo

$$p_2 \equiv 1 \bmod (p_1 - 1) \quad \Leftrightarrow \quad (p_2 - 1) \mid (p_1 - 1).$$

Simmetricamente, partendo dal fatto che $p_2 \mid n$ implica $p_2 - 1 \mid n - 1$, troviamo che $(p_2 - 1) \mid (p_1 - 1)$. Ne segue che $p_1 - 1 = p_2 - 1$, ossia $p_1 = p_2$. Contraddizione.

5. Sfruttando l'espressione binaria dell'esponente, calcolare

$$3^{200} \bmod 48, \quad 45^{54} \bmod 91, \quad 12^{256} \bmod 561.$$

6. Fare il test di primalità di Miller-Rabin sui seguenti numeri:

$$n = 91,\ 101,\ 113,\ 221,\ 1729,\ 2465,\ 8911$$

(usare ad esempio $a = 2$ oppure un altro primo piccolo).

Sol. Sulla nota2 ci sono vari esempi svolti del test di Miller-Rabin, tra cui 8911.

7. Fare il test di primalità di Miller-Rabin sul numero: $n = 1009$. (usare ad esempio $a = 2$). Cosa possiamo concludere?

Sol. $n - 1 = 63 \cdot 2^4$. Dunque $m = 63$ e $k = 4$.

$$\bar{b} \equiv \bar{2}^{63} \equiv \overline{192} \bmod 1009, \qquad \bar{b}^2 \equiv \overline{540}, \quad \bar{b}^2 \equiv \bar{b} \cdot \bar{b} \equiv \overline{1008} \equiv \overline{-1}, \quad \bar{b}^{2^2} \equiv \bar{b}^2 \cdot \bar{b}^2 \equiv \bar{1} \quad \bmod 1009.$$

CONCLUSIONE: $n = 1009$ è 2-pseudoprimo. La probabilità che non sia primo è minore del 25%. Se vogliamo diminuire ancora tale probabilità possiamo ripetere il test di Miller-Rabin con altre basi. Inquestocaso comunque il numero è effettivamente primo.

8. 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 $M^{ED} \equiv M \bmod n$.

Sol. (a) $E \cdot D \equiv 1 \bmod (p-1)(q-1)$ se e solo se $E \cdot D = 1 + k(p-1)(q-1)$, con $k \in \mathbf{Z}$. Ne segue che

$$M^{ED} \equiv M^{1+k(p-1)(q-1)} \equiv M \cdot M^{k(p-1)(q-1)} \bmod n.$$

Facciamo vedere che $M^{k(p-1)(q-1)} \equiv 1 \bmod n$. Poiché $n = p \cdot q$ e gli interi p e q sono primi fra loro

$$M^{k(p-1)(q-1)} \equiv 1 \bmod n \quad \Leftrightarrow \quad \begin{cases} M^{k(p-1)(q-1)} \equiv 1 \bmod p \\ M^{k(p-1)(q-1)} \equiv 1 \bmod q. \end{cases}$$

La tesi adesso segue applicando il Piccolo Teorema di Fermat alle due congruenze del sistema.

(b) $(p-1)(q-1) = 60$. Se ad esempio $E = 17$, allora $D = 53$
(se ad esempio $E = 23$, allora $D = 47$).

(c) $M^E \equiv \overline{15}^{17} \equiv \overline{71} \bmod 77$, $\qquad \overline{71}^{53} \equiv \overline{15} \bmod 77$.
(nel secondo caso avremmo trovato: $M^E \equiv \overline{15}^{23} \equiv \overline{64} \bmod 77 \quad \overline{64}^{47} \equiv \overline{15} \bmod 77$).

9. Il signor Rossi è un utente con chiavi pubbliche $N = 77$ e $E = 17$.
   (a) Spedirgli il messaggio $m = 13$ dopo averlo criptato.
   (b) Un pirata informatico è riuscito a fattorizzare N ed ha scoperto la chiave segreta D del signor Rossi. Qual è ??

Sol. (a) $\bar{m}^{17} \equiv \overline{62} \bmod 77$.
(b) $77 = 7 \cdot 11$, da cui $(p-1)(q-1) = 60$, $D = E^{-1} \equiv \overline{53} \bmod 60$.

10. 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 "14091414130002011904 13".

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 "14091414130002011904 13" 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 $\tilde{m}^D \bmod n$.)

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

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

12. Decifrare il messaggio

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

inviato all'utente

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