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: $n = 33,\ 45,\ 12$.
2. Un *numero di Carmichael* è un numero naturale che non è primo, ma che 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.
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 $n - 1$.
4. Dimostrare che un numero di Carmichael ha almeno tre fattori primi (Sugg. usare il fatto che per ogni primo p esiste $g \in \mathbf{Z}_p^*$ di ordine $p - 1$).
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 determinare sui seguenti numeri:
$$n = 91,\ 101,\ 113,\ 221,\ 1729,\ 2465,\ 8911$$
(usare ad esempio $a = 2$).
7. Fare il test di primalità di Miller-Rabin sul numero: $n = 1009$. (usare ad esempio $a = 2$). Cosa possiamo concludere?
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 $M^{ED} \equiv M \bmod n$.
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 ??

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. 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
11	12	13	14	15	16	17	18	19	20	21	22	23	24	25	26	27	28	29	30	31	00

Decifrare il messaggio

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

inviato all'utente

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