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

1. Sia $n \in \mathbf{N}$. L'ordine $\mathrm{ord}_n(x)$ di $x \in \mathbf{Z}_n^*$ è il più piccolo $r > 0$ tale che $x^r \equiv 1 \pmod{n}$.
   (a) Sia $n = 7$. Calcolare $\mathrm{ord}_n(x)$ per ogni $x \in \mathbf{Z}_n^*$.
   (b) Sia n primo. Dimostrare che $\mathrm{ord}_n(x)$ divide $n-1$ per ogni $x \in \mathbf{Z}_n^*$.
   (c) Sia $n \in \mathbf{N}$. Calcolare l'ordine di $-1 \pmod{n}$.

2. (a) Sia $p > 2$ un primo. Dimostrare che $\{x \in \mathbf{Z}_p : x^2 = 1\} = \{\pm 1\}$.
   (b) Determinare tutti gli $x \in \mathbf{Z}_{15}^*$ per cui $x^2 = 1$. Stessa domanda per $\mathbf{Z}_{21}^*$.
   (c) Sia n prodotto di due primi dispari. Quanti sono gli elementi $x \in \mathbf{Z}_n^*$ con $x^2 = 1$?
   (d) Determinare tutti gli $x \in \mathbf{Z}_9^*$ per cui $x^2 = 1$. Stessa domanda per $\mathbf{Z}_{25}^*$.
   (e) Sia n quadrato di un numero primo $p > 2$. Quanti sono gli elementi $x \in \mathbf{Z}_n^*$ con $x^2 = 1$?

3. La *funzione φ di Eulero* è definita da $\varphi(n) = \#\mathbf{Z}_n^*$ (per $n \in \mathbf{N}$).
   (a) Dimostrare: $\varphi(n) = \#\{a \in \mathbf{N} : 0 \le a < n \text{ e } \mathrm{mcd}(a, n) = 1\}$.
   (b) Calcolare $\varphi(n)$ per ogni $n \le 10$.
   (c) Dimostrare che $\varphi(n) = n - 1$ quando n è primo.
   (d) Sia $n = pq$ per due primi p e q. Dimostrare che $\varphi(n) = (p-1)(q-1)$.
   (e) Sia p un primo. Calcolare $\varphi(p^2)$. Calcolare $\varphi(p^k)$ per ogni $k \ge 1$.

4. Un *numero di Carmichael* è un numero naturale che non è primo, ma per cui $x^{n-1} \equiv 1 \pmod{n}$ per ogni $x \in \mathbf{Z}_n^*$.
   (a) Dimostrare che $561 = 3 \cdot 17 \cdot 31$ è un numero di Carmichael.
   (b) Dimostrare che $8911 = 7 \cdot 19 \cdot 67$ è un numero di Carmichael.
   (c) 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. (mini-RSA) Sia $p = 7$ e $q = 13$ e sia $n = pq = 7 \cdot 13 = 91$ il modulo di questo sistema RSA. L'esponente pubblico è $E = 11$. Il messaggio è $m = 10$.
   (a) Cifrare il messaggio, cioè calcolare il resto $\tilde{m}$ della divisione di m^E per n.
   (b) Determinare l'esponente segreto D, cioè calcolare D tale che $DE \equiv 1 \pmod{(p-1)(q-1)}$.
   (c) Decifrare $\tilde{m}$, cioè controllare che il resto della divisione di $\tilde{m}^D$ per n è uguale al messaggio originale m.

6. (mini-RSA) Sia $n = 77$ il modulo di un sistema crittografico RSA. Sia $E = 13$ l'esponente che si usa per cifrare i messaggi. Determinare un esponente $D \in \mathbf{N}$ tale che $(x^E)^D \equiv x \pmod{n}$ per il messaggio $x = 4$.

7. Collegarsi al sito `http://modular.fas.harvard.edu/calc/` per usare il programma di manipolazione simbolica PARIGP: dopo aver scritto il comando nella parte superiore della finestra, fare click sulla scritta PARI e nella parte inferiore della finestra appariranno la risposta e il tempo impiegato per ottenerla. Ecco alcuni comandi da provare:

• *binary*(n) calcola l'espressione binaria di n; ad esempio

```
binary(259)

[1, 0, 0, 0, 0, 0, 0, 1, 1]
Errors (if any) and Timing Info:
Timing:
real 0m0.056s
user 0m0.040s
sys 0m0.020s
```

• $gcd(n, m)$ calcola il massimo comun divisore tra n ed m; ad esempio

```
gcd(12, 234)
6
Errors (if any) and Timing Info:
Timing:
real 0m0.057s
user 0m0.030s
sys 0m0.020s
```

• $Bezout(n, m)$ restituisce degli interi N ed M tali che $Nn + Mm = mcd(n, m)$ e il massimo comun divisore fra n ed m; ad esempio

```
bezout(12,234)
[-19, 1, 6]
Errors (if any) and Timing Info:
Timing:
real 0m0.064s
user 0m0.040s
sys 0m0.020s
```

• $Mod(x, n)$ calcola il numero x modulo n; ad esempio

```
Mod(34^1265,333)
Mod(238, 333)
Errors (if any) and Timing Info:
Timing:
real 0m0.055s
user 0m0.030s
sys 0m0.020s
```

• $factor(n)$ determina i fattori primi di n e la loro molteplicità; ad esempio

```
factor(89110666666667777777777700)
[2 2]
[5 2]
[107 1]
[7103 1]
[13297 1]
[881760077127421 1]
Errors (if any) and Timing Info:
Timing:
real 0m0.076s
user 0m0.070s
sys 0m0.010s
```

• $isprime(n)$ determina se n è un numero primo o no, rispondendo rispettivamente 0 o 1; ad esempio

```
isprime(89110666666667777777777700)
0
Errors (if any) and Timing Info:
Timing:
real 0m0.058s
```

```
user 0m0.030s
sys 0m0.030s
```

- *nextprime*(n) determina il più piccolo numero primo maggiore di n; ad esempio

```
nextprime(89110666666667777777777777700)
89110666666667777777777777761
Errors (if any) and Timing Info:
Timing:
real 0m0.061s
user 0m0.030s
sys 0m0.020s
```

Altri comandi sono:
prime(n) restituisce l'ennesimo numero primo;
$factorial(n)$ calcola n fattoriale;
eulerphi(n) calcola la funzione di Eulero di n.

Per svolgere i prossimi esercizi, aiutarsi con PARIGP.

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

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

9. 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 "1409141413000201190413".

   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 "1409141413000201190413" 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 $DE \equiv 1 \pmod{(p-1)(q-1)}$. Il messaggio originale è allora uguale a $\tilde{m}^D \pmod{n}$.)

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

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

11. Decifrare il messaggio

$M1 = 475394238194858892901219990750844 35, \ M2 = 401957449702894899560393214873280330$

inviato all'utente

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

12. Usando il test di primalità basato sulla versione "raffinata" del Piccolo Teorema di Fermat, determinare se i seguenti numeri sono primi o meno:

$$91, \quad 113, \quad 221, \quad 1729, \quad 2465.$$