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. Esercizio col metodo $p-1$ di Pollard (Usare PARI/GP e l'applet per la fattorizzazione on-line di Alpertron).
   (a) Fattorizzare i seguenti 3 numeri col metodo $p-1$ di Pollard. Usare ad esempio:
   `http://www.mat.uniroma2.it/~geo2/pminus.txt`

$n = 39080295191118915018134958938415108346749622881999563438557941763777 38$
$37879970068136035919305517302338111572218251 71$

$n = 54776770731927734524510635129304900304647682454932386722232624524088 99$
$11619631465164124733005068230074356253946038850399554060231365982075 03$

$n = 10000000000000000003847900345723000001348582330307531700000000466235469063$

   (b) Controllare la primalità dei fattori trovati al punto (a) ed eventualmente fattorizzarli.
   (c) Ripetere l'algoritmo $p-1$ di Pollard e verificare che nei casi in cui ha successo, generalmente spezza il numero come $n = m * q$ dove m è il prodotto di tutti i fattori primi p, per cui $p-1$ è B-smooth (in questo caso provare con $B = 1500$).
   (d) Sperimentare con l'algoritmo $p-1$ di Pollard, scegliendo diversi valori di B.

2. Sia E la curva ellittica di equazione $Y^2 = X^3 + 5X$.
   (a) Determinare $\#E(\mathbb{Z}_p)$ per $p = 11$ e formulare il corrispondente Teorema di Lagrange per il gruppo abeliano finito $E(\mathbb{Z}_p)$.
   (b) Ripetere quanto fatto al punto (a) per $p = 13$.

3. Sia $n = p \cdot q$, con p e q primi. Sia E una curva ellittica su $\mathbb{Z}_n$

$$Y^2 = X^3 + AX + B, \qquad \Delta = 4A^3 + 27B^2 \in \mathbb{Z}_n^*.$$

   (a) Verificare che E definisce una curva ellittica sia su $\mathbb{Z}_p$ che su $\mathbb{Z}_q$.
   (b) Sia $P = (X_0, Y_0) \in E(\mathbb{Z}_n)$. Verificare che $P = (\bar{X}_0, \bar{Y}_0) \bmod p$ appartiene a $E(\mathbb{Z}_p)$ e che $P = (\bar{X}_0, \bar{Y}_0) \bmod q$ appartiene a $E(\mathbb{Z}_q)$.
   (c) $P + Q$ è un punto all'infinito in $E(\mathbb{Z}_n)$ se e solo se $P + Q$ è il punto all'infinito in $E(\mathbb{Z}_p)$ oppure $P + Q$ è il punto all'infinito in $E(\mathbb{Z}_q)$.

4. Sperimentare col programma in PARI/GP
   `http://www.mat.uniroma2.it/~geo2/maxfactor.txt`