TEN 2014. Esercizi 4. Metodo Pollard $p-1$.

Notazione: Indichiamo con $\log n$ il logaritmo di n in base 2 e con $\ln n$ il logaritmo naturale di n, in base e.
Attenzione: i links ai file vanno ribattuti completamente (col copia-incolla non funzionano).

1. (*Pollard* $p-1$). Sia $M = 2^3 \cdot 3^2 \cdot 5 \cdot 7$.
   (a) Sia $n = 95431706263$. Scegliere $\overline{a} \in \mathbb{Z}_n^*$ a caso. Calcolare $\overline{b} = \overline{a}^M \bmod n$. Calcolare il divisore $d = \mathrm{mcd}(b-1, n)$ di n ed il cofattore n/d.
   (b) Sia $n = 57841557763361$. Scegliere $\overline{a} \in \mathbb{Z}_n^*$ a caso. Calcolare $\overline{b} = \overline{a}^M \bmod n$. Calcolare il divisore $d = \mathrm{mcd}(b-1, n)$ di n ed il cofattore n/d.
   (c) Come mai l'algoritmo trova queste due fattorizzazioni?

2. 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 (aumentare progressivamente il valore di B). Usare ad esempio:
   `http://www.mat.uniroma2.it/~geo2/pminus.txt`

$n = 648094404671778064954604256557085019633635801783629254997370651459604545391$

$n = 870085944154182961097983310733553997642948638641712158092697230355367338367$

$n = 390802951911189150181349589384151083467496228819995634385579417637773837879970068136035919305517302338111572218251 71$

   (b) Controllare la primalità dei fattori trovati al punto (a) ed eventualmente fattorizzarli.
   (c) Verificare che nei casi in cui ha successo, l'algoritmo 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.