TEN 2016. Esercizi 5. Interi B-smooth. 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.

1. Usare il programma

`http://www.mat.uniroma2.it/~geo2/TEN/Bsmooth.txt`

per confrontare il numero di primi e di interi B-smooth in un certo intervallo.

2. (*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?

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

$n1 = 64809440467177806495460425655708501963363580178362925499737065145960454539 1$

$n2 = 87008594415418296109798331073355399764294863864171215809269723035536733836 7$

$n3 = 39080295191118915018134958938415108346749622881999563438557941763777383787997006$
$81360359193055173023381157221825171$

$n4 = 57910112155118020986691000616209882696955852203304284420354228211689903$
$41093047692287240333682685742862801$

   (b) Nel caso in cui un fattore trovati al punto (a) è un primo p, confrontare B con la decomposizione in fattori primi di $p-1$.
   (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.