

Assignatura:

Estudiant/a:

Data:

Two Men OTeHenta

1878

Agafarem com a  $p$  el nombre  $10^9 + 7$ ,  
que és un primer segur (no mostro dubte, és  
que els primers de la forma  $2K+1$  amb  $K$  primer s'anomenen  
segurs), molt conegut en l'àmbit de la informàtica, i  
com a  $q$  agafarem  $37$ , que també és primer.

No tenim una bona definició de "primer gran",  
però considerarem que  $p$  i  $q$  ho són, el primer  
perquè l'he hagut d'escriure en notació científica  
per a no equivocar-me amb el nombre de zeros,  
i el segon basant-me en el fet que quan  
feia primària, el professor va decidir no baixar  
nota a aquells que no havien simplificat la fracció  
generant triu següent (cosa que em va indignar prou per  
recordar-ho gairebé 20 anys després):

$$1' \overline{629} = \frac{1629 - 1}{999} = \frac{1628}{999} = \frac{44 \cdot 37}{27 \cdot 37} = \frac{44}{27}$$

$$5 < \frac{1}{4} \sqrt{(10^9 + 7) \cdot 37} \text{ trivialment}$$

Com a  $a$  agafarem ~~36~~, i com a  $b$  agafarem l'únic <sup>primer</sup>  
nombre entre 1:  $\varphi(n) = 36 \cdot (10^9 + 6) = 2^2 \cdot 3^2 \cdot 2 \cdot (5 \cdot 10^8 + 3)$   
tal que  $\frac{b}{5} \equiv 1 \pmod{\varphi(n)}$ . Mirant la factorització, ha d'existir,



Assignatura: \_\_\_\_\_

Estudiant/a: \_\_\_\_\_

Data: \_\_\_\_\_

i ni de conya el calcularem. En lloc d'això,  
definirem una successió  $(y_n)$  així:

$$y_0 = 1, \quad y_1 = 0$$

$$y_{n+1} = q_n y_n + y_{n-1}$$

Fixem-nos que

$$a_1 = -x_0 b + y_0 n \quad (=n)$$

$$a_2 = x_1 b + y_1 n \quad (=b)$$

Això no és casualitat:

$$a_{2k+1} = -x_{2k} b + y_{2k} n$$

$$a_{2k+2} = x_{2k+1} b + y_{2k+1} n$$

((

$$a_{2k+1} - q_{2k+1} a_{2k+2} = (-x_{2k} - q_{2k+1} x_{2k+1}) b + (y_{2k} + q_{2k+1} y_{2k+1}) n$$

$$= a_{2k+3} = -x_{2k+2} b + y_{2k+2} n$$

Semblantment,

$$a_{2k+4} = x_{2k+3} b + y_{2k+3} n,$$

completant la inducció



Assinatura: \_\_\_\_\_

Estudiant/a: \_\_\_\_\_

Data: \_\_\_\_\_

Pensant-ho millor, b és molt fàcil de calcular, ja que  $\varphi(n) = 36 \cdot (10^9 - 16)$  acaba en 6:

$$56 \equiv 1 \quad | \quad 36\,000\,000\,216$$

$$5b \equiv -36\,000\,000\,215 \pmod{36\,000\,000\,216}$$

$$b_2 = -7200\,000\,043 \quad (36\,000\,000\,216)$$

$$b \equiv 28800000173 \pmod{36000000216}$$

$$a_4 = 37\,000\,000\,259$$

$$b_1 = a_2 = 28\,800\,000\,173$$

$$r_1 = b_2 = a_3 = 8\,200\,000\,086$$

$$r_2 = b_3 = a_4 = 419999915$$

$$q_1 = 1$$

$$q_2 = 2$$

$$q_3 = 1$$

$$X_0 = 0, \quad \cancel{X_1 = 1}, \quad \cancel{X_2 = 2}, \quad \cancel{X_3 = 3}, \quad \cancel{X_4 = 4},$$

$$X_1 = 1$$

$$X_2 = 1 \cdot 1 + 0 = 1$$

$$x_3 = 2 \cdot 1 + 1 = 3$$

$$x_4 = 1 \cdot 3 + 1 = 4$$

$$X_9 = ? \cdot 4 + 3 > 5$$

Não temos calculado que:

per tant no sabem  $X_5$ ,

però  $q_4 \geq 1$ , ja que els quocients sempre ho són al fer Euclides. Això

implica  $X_5 > 5$  i

$X_n > 5 \quad \forall n$ , ja que la successió és creixent.

Per tant, mai no arriba a  $a=5$