# 1 RSA

- $p = 11$, $q = 7$, $d = 53$ $\Rightarrow$ $(77, 17)$
- $(119, 5)$, $E = 81$ $\Rightarrow$ $m = 30$
- $(65, 7)$, $E = 31$ $\Rightarrow$ $m = 21$
- $(299, 5)$ $\Rightarrow$ $p = 13$, $q = 23$, $d = 53$
- No se puede afirmar que calcular $d$ a partir de $(n, e)$ sea polinomial.

# 2 Curvas Elípticas

- Si tomamos una c.e. módulo $p$ dada en forma de Weierstrass $\Rightarrow$ El número de puntos de la c.e. está comprendido en el intervalo $[(\sqrt{p} - 1)^2, (\sqrt{p} + 1)^2]$.
- (V/F) Una c.e. sobre un cuerpo $K$ tiene siempre un punto proyectivo con coordenadas enteras.
- (V/F) Tres puntos alineados de una c.e. siempre suman cero.
- Si $E(\mathbb{F}_{p^k})$ es el grupo de una c.e. $\Rightarrow$ Si es cíclico, no puede tener más de un elemento de orden dos.

# 3 Primos de Fermat

- (V/F) Un pseudoprimo de Fermat, $n = psp(a)$, satisface $a^{n-1} \equiv 1 \pmod{n}$ y es compuesto.
- (V/F) Los pseudoprimos fuertes pueden certificar que un número es compuesto pero no que es primo.
- (V/F) Aunque sea fácil comprobar la primalidad de un número de Fermat puede ser dificil demostrar la primalidad de alguno de sus factores.
- (V/F) Un pseudoprimo de Euler respecto de la base $a$ es siempre pseudoprimo de Fermat respecto de la misma base.

# 4 FCS

- La FCS de $\sqrt{d}$ con $d$ libre de cuadrados es $[q_0, \dots, 2q_0]$ donde cada $q_i < q_0$.
- Si $\alpha = \frac{P+\sqrt{d}}{Q}$ es un irracional cuadrático ($d$ libre de cuadrados):
  - La FCS de $\alpha$ es periódica con periodo máximo $2d - 1$.
  - La FCS de $\alpha$ es puramente periódica sii $\alpha > 1$ y $1 < \overline{\alpha} < 0$ (su conjugado).
- (V/F) Una FCS finita coincide con su último convergente.
- Si $x^2 - dy^2 = N$ ($|N| < \sqrt{d}$) es una ecuación de Pell $\Rightarrow$ Cualquier solución positiva con $mcd(x, y) = 1$, son el numerador y el denominador de una convergente de la FCS de $\sqrt{d}$.
- $\alpha = \sqrt{2}$ $\Rightarrow$ $\alpha = [1, 2, 2, \dots]$
- $\alpha = \sqrt{3}$ $\Rightarrow$ No es puramente periódica.

- $\alpha = \frac{a+\sqrt{a^2+4}}{2} \qquad \Rightarrow \qquad \alpha = [a, a, a, \dots]$
- $\alpha = \frac{1+\sqrt{5}}{2} \qquad \Rightarrow \qquad \alpha = [1, 1, 1, \dots]$
- (V/F) $\sqrt{a^2-1} = [a-1, \overline{1, 2(a-1), \dots}]$