não pode ter numeros pares

$C = m^e \bmod P$

$m = c^d \bmod P$

$ed \equiv 1 \bmod (p-1)$

Easy

$a^{p-1} \equiv 1 \bmod p$

$a^{1+k(p-1)} \equiv a \bmod p$

$a^{1+k\,\mathrm{lcm}(p-1,q-1)} \equiv a \bmod (p\,q)$

$c \equiv m^e \bmod \underbrace{n}_{pq}$

$m \equiv c^d \bmod n$ 2040 bits

$ed \equiv 1 \bmod \mathrm{lcm}(p-1, q-1)$

nada
rational

$e = 2^{16}+1$

$(a_1 x + a_0) \bmod P$; $x^2 + x + 1$

$x^2 = -x - 1$

não pode ser

$\ldots = (x+1)^2$

$\ldots = (x+1)(x-1)$

---

2 → How To enc or Sign

4 → Resto chines

10 → $23P = P + 2P + 4P + 16P$

$23 = 2^0 + 2^1 + 2^2 + 2^4$

DH

com mais users

no final se for 3 tem de ter

$r^{\alpha B}$ }

RSA

} → nº de nº coprimos

publico (pq) e e

$$M^e \pmod{pq} = C$$

$$C^d \pmod{pq} = M$$

normal a saber

$$ed \equiv 1 \mod (\text{mmc}(p-1, q-1))$$

$$ed \equiv 1 \pmod{\varphi(pq)}$$

Atach

$$A \rightarrow \leftarrow B$$

$$A = r^a \mod p$$

$$B = r^b \mod p$$

$$A = B^a \mod p = r^{ba}$$

$C = r^c \bmod p$

$AB = r^{ab}$ $\qquad$ $A = BC^a$

$AC = r^{ac}$ $\qquad$ $B = AC^b$

$BC = r^{bc}$ $\qquad$ $C = AB^c$

$B\cancel{A} = r^{ba}$

$C\cancel{A} = r^{ca}$

$C\cancel{B} = r^{cb}$

1°

$A = r^a \bmod p$

$B = r^b \bmod p$

$C = r^c \bmod p$

2°

$AB = B^a \bmod p = r^{ba} \bmod p$

$AC = C^a \bmod p = r^{ca} \bmod p$

$BA = A^b$ ....

$BC = C^b$ ....

$CA = A^c$ ...

$CB = B^c$ ...

3º

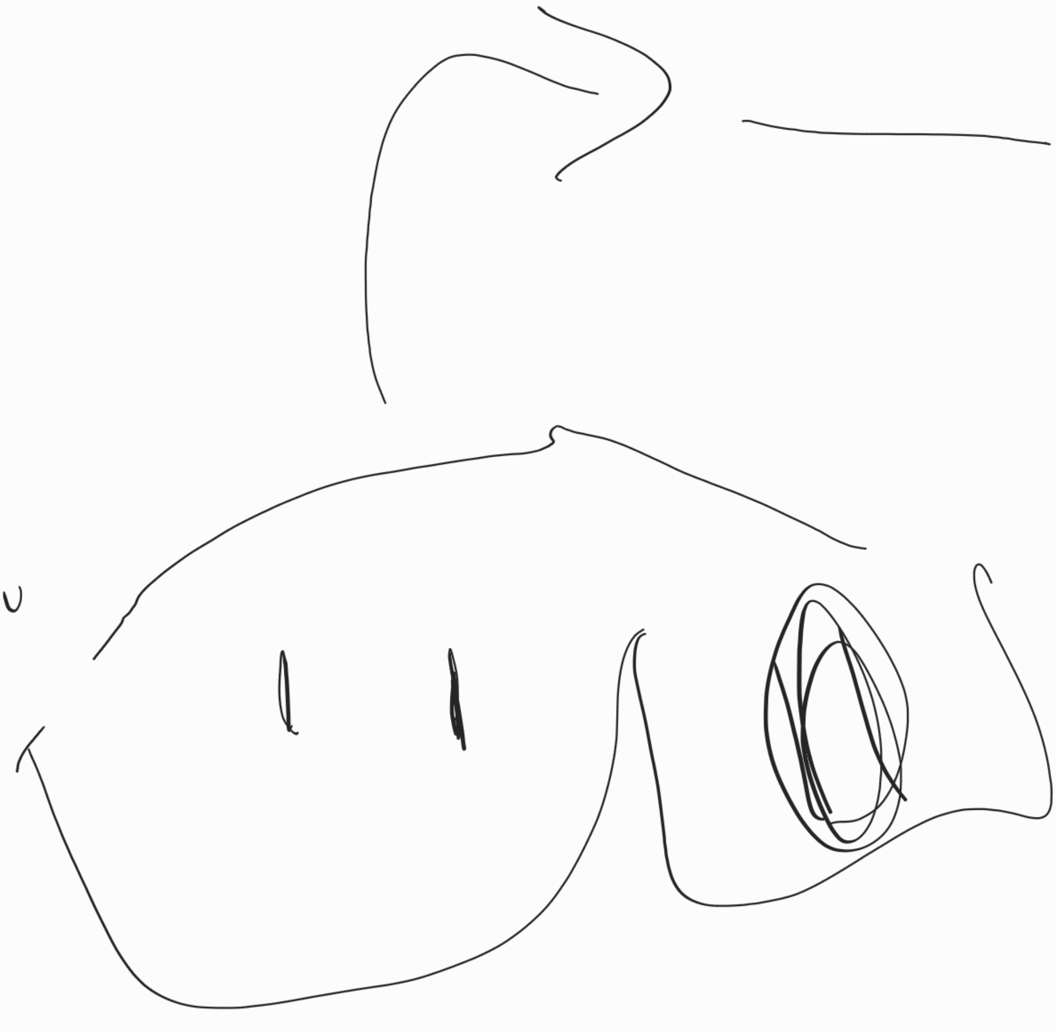
$ABC = BC^a \bmod p$ ou $CB^a \bmod p$

$= r^{abc} \bmod p$

Faz-se o mesmo para o outro

.... a a

aab



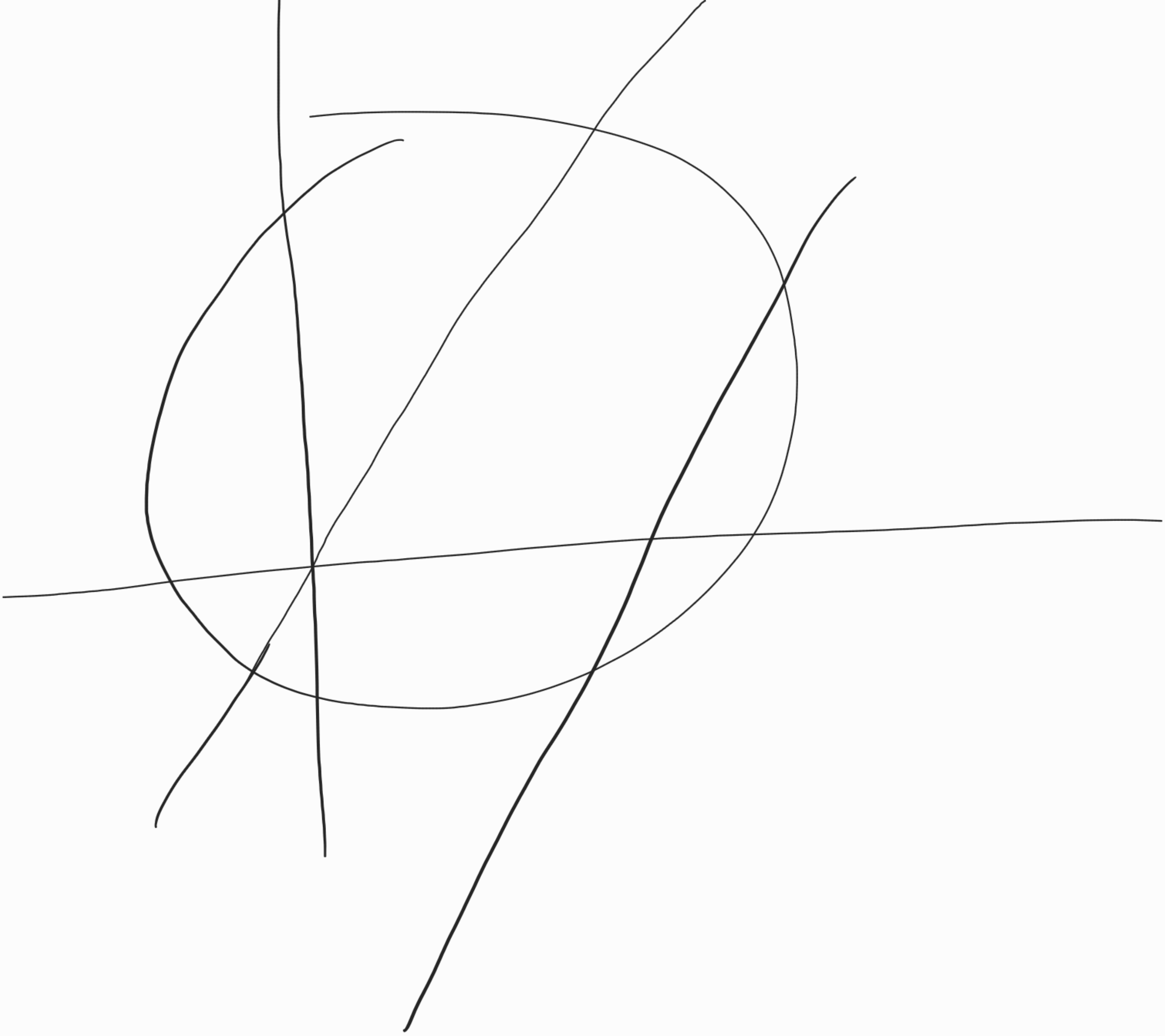
$$\frac{\sqrt{2}}{(\sqrt{5}-2\sqrt{3})(\sqrt{5}+2\sqrt{5})}$$

$a^2 + 2ab$

$(a+b)(a+b)$

$a^2 + 2ab + b^2$

$$\frac{(a+b)(a-b)}{a^2 - b^2}$$

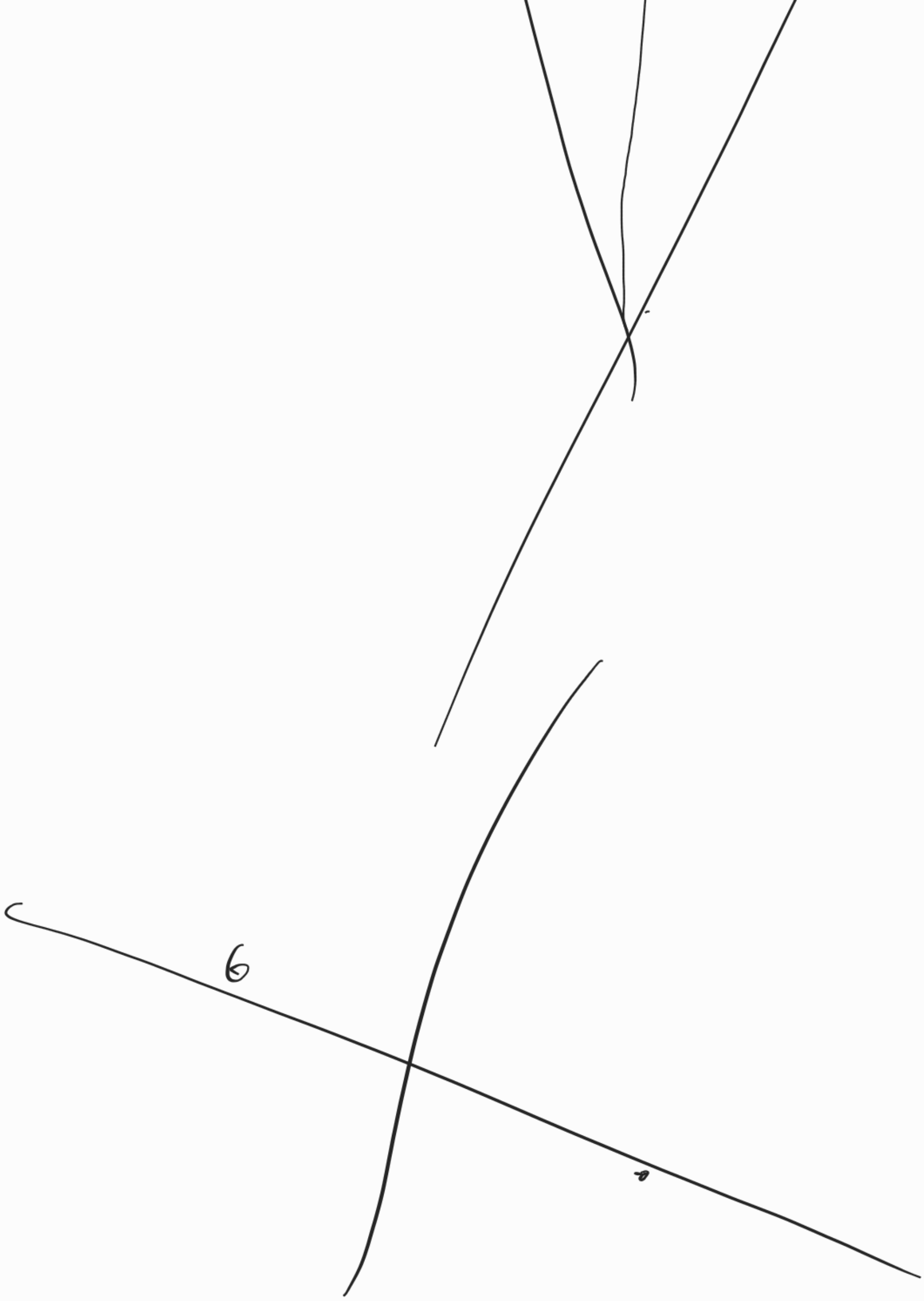


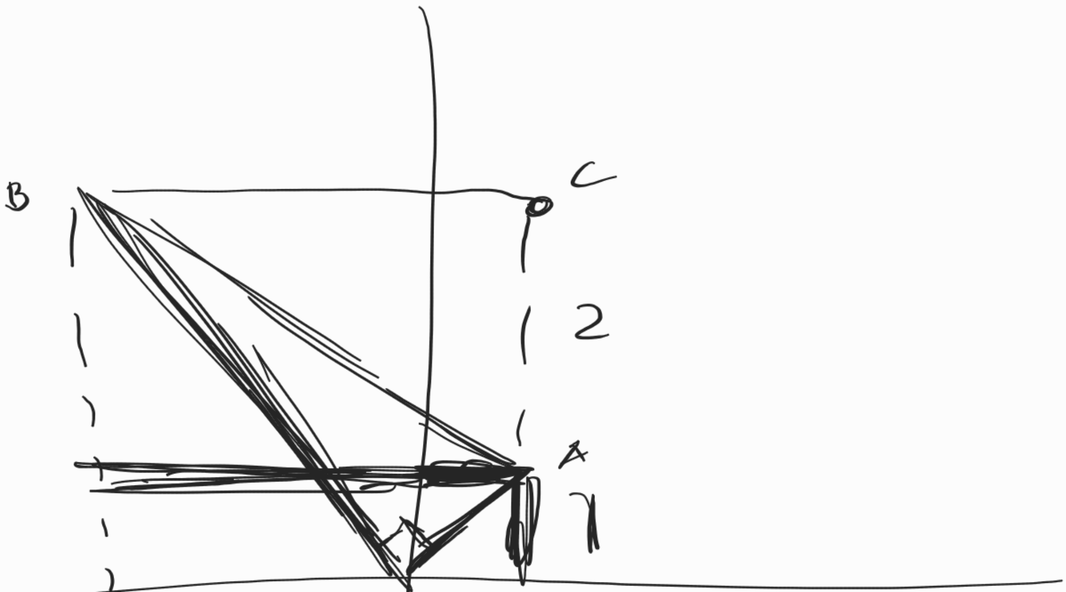
9

$r^2 = 9$

$r = \sqrt{5}$

$r - 3$


6


B
C
2
A
1

$2 \mid \underline{0}$

$$3 = \frac{b \times h}{2}$$

$$4 \times 12 = 48$$