PRÁCTICO 0

1. EL ALGORITMO (EXTENDIDO) DE EUCLIDES

TEO: SEAN $a, b \in \mathbb{Z} \setminus \{0\}$. EXISTEN $u, v \in \mathbb{Z}$ /

$$au + bv = \gcd(a,b) =: (a,b)$$

EJEMPLO: SABEMOS QUE $(23,11) = 1$. EL TEO SE VERIFICA:

$$1 \cdot 23 + (-2) \cdot 11 = 1$$

SI MIRAMOS MÓD 23,

$$-2 \cdot 11 \equiv 1 \ (23) \iff 21 \cdot 11 \equiv 1 \ (23)$$

$\rightsquigarrow$ 21 ES EL INVERSO DE 11 EN $\mathbb{Z}/23\mathbb{Z}$. VEMOS ASÍ QUE HALLAR u Y v NOS AYUDA A CALCULAR INVERSOS.

¿CÓMO HALLARLOS?

ALGORITMO (EUCLIDES):

$$a = q_0 b + r_0, \quad 0 \le r_0 < b \quad (\text{SUPONEMOS } b \in \mathbb{N})$$
$$b = q_1 r_0 + r_1, \quad 0 \le r_1 < r_0$$
$$\vdots$$
$$r_{m-1} = q_m r_m + r_{m+1} \quad \text{CON } r_{m+1} \neq 0$$
$$r_m = q_{m+1} r_{m+1} + 0$$

ENTONCES, $r_{m+1} = (a,b)$.

UN POSIBLE PSEUDOCÓDIGO:

```
1: x ← a, y ← b, r ← RESTO DE DIVIDIR A x POR y.
2: WHILE r > 0:
3:     x ← y, y ← r, r ← RESTO DE DIVIDIR A x POR y
4: RETURN y
```

NOTAR: $r_0 = a - q_0 b$ ES COMB. DE a y b

$r_1 = b - q_1 r_0 = b - q_1(a - q_0 b)$ TAMBIÉN LO ES

$\vdots$

$r_{m+1} = (a,b)$ TAMBIÉN LO ES. //

TEO (FERMAT): SEAN p UN PRIMO, $a \in \mathbb{Z}$.

SI $p \nmid a$, ENTONCES $a^{p-1} \equiv 1 \ (p)$

PUEDE SER ÚTIL PARA CALCULAR POTENCIAS, COSA QUE NOS VA A INTERESAR MÁS ADELANTE.

EJEMPLO: CALCULAR 3^{324} módulo 13.

SABEMOS QUE $3^{12} \equiv 1 \ (13)$; SI ESCRIBIMOS $324 = 12 \cdot 27 + 5$,

$3^{324} \equiv 3^{12 \cdot 27 + 5} \equiv (3^{12})^{27} \cdot 3^5 \equiv 3^5 \ (13)$;

$3^5 = 27 \cdot 9 \equiv 1 \cdot 9 \equiv 9 \ (13)$

OBS: LA ECUACIÓN $3^{12} \equiv 1 \ (13)$ NOS DICE QUE EL INV. DE 3 EN $\mathbb{Z}/13$ ES 3^{11}...

$\rightsquigarrow$ CUALQUIER POTENCIA MÓD 13 INVOLUCRA A LO SUMO 12 MULTIPLICACIONES

OBS: FERMAT DICE QUE $3^{12} \equiv 1 \ (13)$. PERO PUEDE PASAR ALGO MEJOR: QUE PARA ALGÚN DIVISOR d DE 12, VALGA $3^d \equiv 1 \ (13)$

DE HECHO, VALE PARA $d = 3$

$\rightsquigarrow$ DIVIDO POR 3 EN LUGAR DE 12:

$324 = 3 \cdot 4 \cdot 27 + 3 \cdot 1 + 2 = 3 \cdot * + 2$, Y ASÍ

$3^{324} = (3^3)^* \cdot 3^2 \equiv 1 \cdot 3^2 \equiv 9 \ (13)$

OJO: SI p NO ES PRIMO, NO VALE FERMAT. POR EJEMPLO:

TOMO $m = 6$, $a = 5$. ENTONCES NO ES CIERTO QUE $a^{m-1} \equiv 1 \ (m)$:

$5^5 \equiv (5^2)^2 \cdot 5 \equiv 1 \cdot 5 \equiv 5 \ (6)$

COMENTARIO: SÍ VALE, PARA $(a,m)=1$, QUE $a^{\varphi(m)} \equiv 1 \ (m)$, DONDE $\varphi = \varphi$ DE EULER...

VALE $\varphi(6)=4$

TEO. CHINO DEL RESTO

EJEMPLO: QUEREMOS HALLAR $x \in \mathbb{Z}$ TAL QUE

$$(*) \begin{cases} x \equiv 2 \ (6) \\ x \equiv 3 \ (7) \end{cases}$$

COMO $(6,7)=1$, EL TEO CHINO NOS ASEGURA QUE EXISTE UNA ÚNICA SOL EN $\mathbb{Z}/6\cdot7\mathbb{Z}$ ¿CÓMO HALLARLA?

SI $x \equiv 2 \ (6)$, ENTONCES $x = 6\cdot q + 2$, PARA ALGÚN $q \in \mathbb{Z}$.

AHORA, $6\cdot q + 2 \equiv 3 \ (7) \iff 6q \equiv 1 \ (7) \iff$

$q \equiv 6 \ (7) \iff q = 7\cdot k + 6$, CON $k \in \mathbb{Z}$.

EL INV. DE 6 ES 6

ASÍ, $x = 6(7\cdot k + 6) + 2 = 42k + 38$ CON $k \in \mathbb{Z}$ ES SOL. DE $(*)$, EL ÚNICO EN $\mathbb{Z}/42\mathbb{Z}$ SE OBTIENE TOMANDO $k=0$.

FINALMENTE, UN EJEMPLO DE CÓMO SE PUEDE USAR LA ARITMÉTICA MODULAR PARA RESOLVER UN PROBLEMA SOBRE NÚMEROS ENTEROS (LLAMADOS ECUACIONES DIOFÁNTICAS)

EJEMPLO: SEA $m \in \mathbb{Z}$ IMPAR, PROBAR QUE LA ECUACIÓN

$$2m + a^2 = b^2 \qquad (a, b \in \mathbb{Z})$$

NO TIENE SOLUCIÓN.

- MIRANDO MÓD 2, VEMOS QUE

$$a^2 \equiv b^2 \pmod 2$$

LUEGO, a ES PAR SII b ES PAR.

- SI a (Y ∴ b) ES PAR, MIRO MÓD 4:

$$2m + (2k)^2 \equiv (2l)^2 \pmod 4$$

$\iff 2m \equiv 0 \pmod 4 \iff 4 \mid 2m$ ABS.! m IMPAR

→ LUEGO, a Y b SON IMPARES.

- SI $a \equiv 1 \pmod 4$, $a^2 \equiv 1 \pmod 4$; SI $a \equiv 3 \pmod 4$, $a^2 = 9 \equiv 1 \pmod 4$

ASÍ, $a^2 \equiv b^2 \equiv 1 \pmod 4$ Y POR LO TANTO

$$2m + a^2 \equiv b^2 \pmod 4 \iff 2m \equiv 0 \pmod 4, \text{ ABS.!}$$

[illegible]

[illegible]