Algoritmo di Euclide esteso

$$1876 = 365 * 5 + 51$$

$$365 = 51 * 7 + 8$$

$$51 = 8 * 6 + 3$$

$$8 = 3 * 2 + 2$$

$$3 = 2 * 1 + 1$$

$$2 = 1 * 2 + 0$$

a	b	q	r	x	y
			1876	1	0
			365	0	1
1876	365	5	51	1	-5
365	51	7	8	-7	36
51	8	6	3	43	-221
8	3	2	2	-93	478
3	2	1	1	136	-699
2	1	2	0		

$$a = bq + r \qquad r = 1876x + 365y$$

$$(x_i, y_i) = (x_{i-2} - x_{i-1} \cdot q_i, \qquad y_{i-2} - y_{i-1} \cdot q_i)$$

$$51 = 1876 - 365 * 5 =$$

$$= 1876 * (1) + 365 * (-5)$$

$$8 = 365 - 51 * 7 =$$

$$= [1876 * (0) + 365 * (1)] - [1876 * (1) + 365 * (-5)] * 7 =$$

$$= 1876 * [(0) - (1) * 7] + 365 * [(1) - (-5) * 7] =$$

$$= 1876 * (-7) + 365 * (36)$$

$$3 = 51 - 8 * 6 =$$

$$= [1876 * (1) + 365 * (-5)] - [1876 * (-7) + 365 * (36)] * 6 =$$

$$= 1876 * [(1) - (-7) * 6] + 365 * [(-5) - (36) * 6] =$$

$$= 1876 * (43) + 365 * (-221)$$

$$2 = 8 - 3 * 2 =$$

$$= [1876 * (-7) + 365 * (36)] - [1876 * (43) + 365 * (-221)] * 2 =$$

$$= 1876 * [(-7) - (43) * 2] + 365 * [(36) - (-221) * 2] =$$

$$= 1876 * (-93) + 365 * (478)$$

$$1 = 3 - 2 * 1 =$$

$$= [1876 * (43) + 365 * (-221)] - [1876 * (-93) + 365 * (478)] * 1 =$$

$$= 1876 * [(43) - (-93) * 1] + 365 * [(-221) - (478) * 1] =$$

$$= 1876 * (136) + 365 * (-699)$$

Equazioni diofantee

$$ax + by = c$$

Primo metodo (sostituzione)

1. calcola $MCD(a, b)$ (eventualmente con l'algoritmo di Euclide)
2. $MCD(a, b) \mid c$?
   - NO: non ci sono soluzioni
   - SÌ: vai avanti
3. dividi tutto per $MCD(a, b)$

$$a' = \frac{a}{MCD(a,b)}, \qquad b' = \frac{b}{MCD(a,b)}, \qquad c' = \frac{c}{MCD(a,b)}$$

$$\boldsymbol{a'x + b'y = c'}$$

4. risolvi l'omogenea associata

$$a'x + b'y = 0$$

   - chiamiamo α e β le soluzioni, allora

$$\boldsymbol{\alpha = -b't} \qquad \boldsymbol{\beta = a't,} \qquad t \in \mathbb{Z}$$

5. trova una coppia di soluzioni dell'equazione originaria [quella azzurra]
   - applica l'identità di Bézout

$$1 = a'\boldsymbol{r} + b'\boldsymbol{s}$$

   - trova i coefficienti r e s con l'algoritmo di Euclide esteso
   - chiamiamo (x_0, y_0) una coppia di soluzioni dell'equazione originaria dove

$$\boldsymbol{x_0} = c'r \qquad \text{e} \qquad \boldsymbol{y_0} = c's$$

6. tutte le soluzioni dell'equazione di partenza sono del tipo

$$(\boldsymbol{x_0 + \alpha},\ \boldsymbol{y_0 + \beta})$$ in funzione del parametro $\boldsymbol{t}$

Secondo metodo (congruenze)

1. risolvi la congruenza

$$ax \equiv c\ \ (b)$$

$$\boldsymbol{x} = q + kb$$

2. sostituisci x nella diofantea e trova y

$$\boldsymbol{y} = \frac{c - ax}{b}$$

3. le soluzioni sono del tipo

$$(\boldsymbol{x},\ \boldsymbol{y})$$ in funzione del parametro $\boldsymbol{k}$

NOTA: puoi scambiare i ruoli di x e y e risolvere $by \equiv c\ (a)$

in generale conviene scegliere in modo da avere moduli piccoli

Congruenze I grado

$$Ax \equiv B\ (m)$$

1. sostituisci A e B con il rispettivo resto modulo m

$$A \equiv a\ (m) \quad \wedge \quad B \equiv b\ (m), \qquad 0 \leq a, b < m$$

$$\boldsymbol{ax \equiv b}\ (m)$$

2. calcola $MCD(a, m)$ (eventualmente con l'algoritmo di Euclide)
3. $MCD(a, m) \mid b$?
   - NO: non ci sono soluzioni
   - SÌ: vai avanti
4. dividi tutto per $MCD(a, m)$

$$a' = \frac{a}{MCD(a,m)}, \qquad b' = \frac{b}{MCD(a,m)}, \qquad m' = \frac{m}{MCD(a,m)}$$

$$\boldsymbol{a'x \equiv b'}\ (\boldsymbol{m'})$$

5. trova l'inverso di a'
   - applica l'identità di Bézout

$$1 = a'\boldsymbol{r} + m'\boldsymbol{s}$$

   - trova il coefficiente r con l'algoritmo di Euclide esteso
   - ora abbiamo che

$$a'\boldsymbol{r} \equiv 1\ (m')$$

6. moltiplica per l'inverso

$$\boldsymbol{x} \equiv b'r\ (m')$$

NOTA: ci sono $MCD(a, m)$ soluzioni modulo m del tipo

$$x = x_0 + m't, \qquad 0 \leq t < MCD(a, m)$$

dove x_0 è l'unica soluzione modulo m'.

Sistemi di congruenze lineari

$$\begin{cases} A_1 x \equiv B_1 \ \ (m_1) \\ A_2 x \equiv B_2 \ \ (m_2) \end{cases}$$

Primo metodo (sostituzione)

1. risolvere le singole equazioni e ricondursi a

$$\begin{cases} x \equiv c_1 \ \ (m_1) \\ x \equiv c_2 \ \ (m_2) \end{cases}$$

2. calcola $MCD(m_1, m_2)$ (eventualmente con l'algoritmo di Euclide)
3. $MCD(m_1, m_2) \mid c_2 - c_1$?
   - NO: non ci sono soluzioni
   - SÌ: vai avanti
4. trova una soluzione del sistema
   - ricava x da una delle due equazioni [supponiamo la prima]

$$x = c_1 + km_1$$

   - sostituisci nell'altra

$$km_1 \equiv c_2 - c_1 \ \ (m_2)$$

   - risolvi per k

$$\boldsymbol{k} \equiv q \ \ (m_2)$$

   - sostituisci il valore di k per ottenere la soluzione particolare

$$x_0 = c_1 + qm_1$$

5. tutte le altre soluzioni del sistema soddisfano

$$x \equiv x_0 \ \ (mcm(m_1, m_2))$$

Secondo metodo (metodo di interpolazione)

1. come sopra
2. idem
3. idem
4. risolvi i sistemi

$$\begin{cases} x_1 \equiv 1 \ \ (m_1) \\ x_1 \equiv 0 \ \ (m_2) \end{cases} \qquad \begin{cases} x_2 \equiv 0 \ \ (m_1) \\ x_2 \equiv 1 \ \ (m_2) \end{cases}$$

5. la soluzione del sistema di partenza è $x \equiv c_1 x_1 + c_2 x_2 \ \ (m_1 m_2)$

Teorema cinese del resto

Il sistema $\begin{cases} x \equiv c_1 \ \ (m_1) \\ \quad \vdots \\ x \equiv c_n \ \ (m_n) \end{cases}$ con $(m_i, m_j) = 1, \ \ \forall\, 1 \leq i, j \leq n$ è equivalente a

$$x \equiv c \ \ \left(\prod_{i=1}^{n} m_i \right)$$

Binomio ingenuo

$$(x + y)^p \equiv x^p + y^p \ \ (p) \qquad\qquad p \text{ primo}$$

Funzione φ di Eulero

$$\varphi(n) = \prod_{i=1}^{r} p_i^{e_i - 1} (p - 1), \qquad\qquad n = \prod_{i=1}^{r} p_i^{e_i}$$

Teorema di Eulero

$$x^{\varphi(m)} \equiv 1 \ \ (m)$$

Ordine moltiplicativo

$$ord_m(a) = \min \{\, k > 0 : a^k \equiv 1 \ \ (m) \,\}$$

NOTA: dato che $ord_m(a) \mid \varphi(m)$ puoi cercare $ord_m(a)$ tra i divisori di $\varphi(m)$

Congruenze esponenziali

$$A^x \equiv B\ (m)$$

1. sostituisci A e B con il rispettivo resto modulo m

$$A \equiv a\ \ (m) \quad \wedge \quad B \equiv b\ \ (m), \qquad 0 \leq a, b < m$$

$$\boldsymbol{a^x \equiv b\ (m)}$$

2. calcola $MCD(a, m)$ (eventualmente con l'algoritmo di Euclide)
3. $MCD(a, m) = 1$?
    - NO: non ci sono soluzioni
    - SÌ: vai avanti
4. cerca una soluzione x_0 "a tentativi"
    - calcola le potenze di a (ovviamente modulo m) finché non ne trovi una congrua a b
    - se non c'è, non ci sono soluzioni
5. la soluzione è

$$x \equiv x_0\ \ (ord_m(a))$$