Teorema cinese del resto

Leonardo Bizzoni

October 10, 2023

Siano $n_1, n_2, \dots, n_r \in \mathbb{Z} \geq 0$, a due a due coprimi ovvero che presi a caso n_i, n_j essi sono coprimi tra di loro, e siano $b_1, b_2, \dots, b_r \in \mathbb{Z}$. Il sistema di congruenze lineari $\begin{cases} x \equiv b_1 \bmod n_1 \\ x \equiv b_2 \bmod n_2 \\ \vdots \\ x \equiv b_r \bmod n_r \end{cases}$ ammette soluzione. Date 2 soluzioni c, c', allora $c \equiv c' (\text{mod } \prod_{i=1}^{r} n_i)$.

1 Osservazione

Questo teorema da solo una condizione **sufficiente** e non necessaria affinchè il sistema ammetta soluzione. Può quindi esistere un sistema di congruenze dove $\forall i, j | i \neq j$ non è vero che n_i, n_j siano coprimi ma abbia comunque soluzione.

2 Esercizi

Algoritmo generico

$$\begin{cases} x \equiv b_1 \bmod n_1 \\ x \equiv b_2 \bmod n_2 \\ x \equiv b_3 \bmod n_3 \\ \vdots \\ x \equiv b_r \bmod n_r \end{cases}$$

① $\forall i,j \ (n_i, n_j) = 1$ con $i \neq j$

② $N = \prod_{i=1}^{r} n_i$, $N_i = \prod_{x=1, x \neq i}^{r} n_x$

③ $N_i \cdot y_i \equiv 1 \bmod n_i$

④ $X = \sum_{i=1}^{r} N_i \, b_i \, y_i + NK$, $K \in \mathbb{Z}$

$$\begin{cases} x \equiv 4 \bmod 11 \\ x \equiv 3 \bmod 12 \\ x \equiv 5 \bmod 17 \end{cases}$$

$(11,12) = 1$, $(12,17) = 1$, $(17,11) = 1$

$N = 11 \cdot 12 \cdot 17 = 2244$

$N_1 = 12 \cdot 17 = 204$

$N_2 = 11 \cdot 17 = 187$

$N_3 = 11 \cdot 12 = 132$

$204 y_1 \equiv 1 \bmod 11 \Rightarrow 6y_1 \equiv 1 \bmod 11 \Rightarrow y_1 = 2$

$204 \mid 11$, $99 \mid 18$, 6

$11 \mid 6y_1 - 1$

$187 y_2 \equiv 1 \bmod 12 \Rightarrow 7y_2 \equiv 1 \bmod 12 \Rightarrow y_2 = 7$

$187 \mid 12$, $67 \mid 15$, 7

$7x + 12y = 1$

$12 = 7 \cdot 1 + 5$ $\quad 5 = a \cdot b$

$7 = 5 \cdot 1 + 2$ $\quad 2 = 2b - a$

$5 = 2 \cdot 2 + 1$ $\quad 1 = 3a - 5b$

$2 = 2 \cdot 1 + 0$ $\quad c = -5$

$c' = -5 + 12K = 7 \ (K = 1)$

(è meglio avere $y_2 > 0$ per questo prendo c' invece di c)

$132 y_3 \equiv 1 \bmod 17 \Rightarrow 13 y_3 \equiv 1 \bmod 17 \Rightarrow y_3 = 4$

$132 \mid 17$, $13 \mid 7$

$17 \cdot 7 = 119$, $132 - 119 = 13$

$13x + 17y = 1$

$17 = 13 + 4$ $\quad 4 = a \cdot b$

$13 = 4 \cdot 3 + 1$ $\quad 1 = 4b - 3a$

$4 = 1 \cdot 4 + 0$ $\quad c = 4$

$$x = 204\left(4\left(-2\right)\right) + 187\left(3\left(-7\right)\right) + 132\left(5\left(-4\right)\right)$$

$204 \cdot 8 = 1632$

$187 \cdot 21 = 187 + 3740 = 3927$

$132 \cdot 20 = 2640$

$$= 1632 + 3927 + 2640 = 8199 + 2244K,\ K \in \mathbb{Z}$$

$1632 + 3927 = 5559 + 2640 = 8199$

La più piccola soluzione >0 è $8199 - 2244 \cdot 3 = 8199 - 6732 = 1467$

$$\begin{cases} x \equiv 2 \bmod 22 \\ x \equiv 3 \bmod 13 \\ x \equiv 4 \bmod 7 \end{cases}$$

$N = 22 \cdot 13 \cdot 7 = 2002$

$22 \cdot 13 = 66 + 220 = 286$, $286 \cdot 7 = 2002$

$N_1 = 13 \cdot 7 = 91$

$N_2 = 22 \cdot 7 = 154$

$N_3 = 22 \cdot 13 = 286$

$N_1 y_1 \equiv 1 \bmod n_1 \rightarrow 91 y_1 \equiv 1 \bmod 22 \rightarrow 3 y_1 \equiv 1 \bmod 22 \longrightarrow y_1 = 15$

$91 = 4 \cdot 22 + 3$

$3x + 22y = 1$

$22 = 3 \cdot 7 + 1 \quad 1 = a - 7b$

$3 = 1 \cdot 3 + 0 \quad c = -7$

$c' = -7 + \frac{22}{1} k = 15$

$7 \cdot 22 = 154$, $154 + 1 = 155$, $155 - 140 = 15$

$N_2 y_2 \equiv 1 \bmod n_2 \rightarrow 154 y_2 \equiv 1 \bmod 13 \longrightarrow 11 y_2 \equiv 1 \bmod 13 \rightarrow y_2 = 6$

$154 = 11 \cdot 13 + 11$

$11x + 13y = 1$

$13 = 11 + 2 \quad 2 = a - b$

$11 = 2 \cdot 5 + 1 \quad 1 = b - 5(a - b) = 6b - 5a$

$2 = 1 \cdot 2 + 0 \quad c = 6$

$N_3 y_3 \equiv 1 \bmod 7 \rightarrow 286 y_3 \equiv 1 \bmod 7 \rightarrow 6 y_3 \equiv 1 \bmod 7 \rightarrow y_3 = 6$

$286 = 6 \cdot 7 + 4$

$6x + 7y = 1$

$7 = 6 + 1 \quad 1 = a - b$

$6 = 1 \cdot 6 + 0 \quad x = -1$

$x' = -1 + \frac{7}{1} K = 6$

$x = N_1 b_1 y_1 + N_2 b_2 y_2 + N_3 b_3 y_3 + NK, K \in \mathbb{Z}$

$= 91(2(15)) + 154(3(6)) + 286(4(6)) + 2002K$

$91 \cdot 30 = 2730$

$154 \cdot 18 = 1232 + 1540 = 2772$

$286 \cdot 24 = 1144 + 5720 = 6864$

$= 2730 + 2772 + 6864 + 2002K$

$2730 + 2772 = 5502$

$5502 + 6864 = 12366$

$= 12366 + 2002K, K \in \mathbb{Z}$

$2002 \cdot 6 = 12012$

$12366 - 12012 = 354$

con $K = -6$ si ha la minima soluzione > 0 $x = 354$