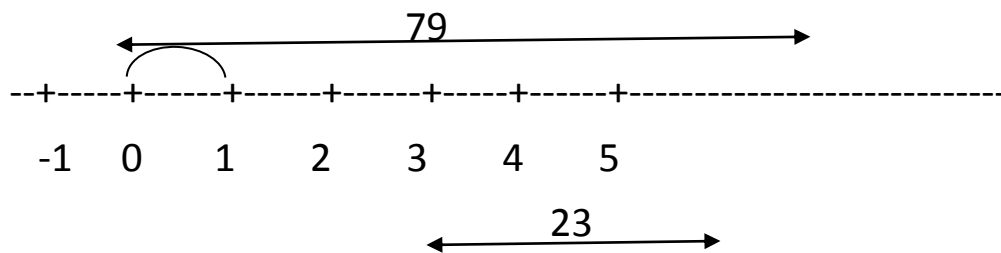


Chinese Equations: Systems of Linear Algebra

- Chinese remainder theorem
- How to compute square roots
- Pascal's triangle: polynomial theorem $(a + b)^4 = a^4 + 4a^3b + 6a^2b^2 + 4ab^3 + b^4$
- Euclidean Algorithm
- Linear Algebra {solutions with integers}

Example : Linear line with steps {79, 23}



Can we go from zero to one using steps of size 79 and 23 only?

Linear equation that finds integer solution: $79m + 23n = 1$

Euclidean Algorithm

$$79 = 3 * 23 + 10$$

$$23 = 2 * 10 + 3$$

$$10 = 3 * 3 + 1$$

$$3 = 3 * 1 \text{ {no remainder}}$$

$$\Rightarrow \text{GCD}(23, 79) = 1$$

Now:

$$1 = 10 - 3 * 3$$

$$= 10 - 3 * (23 - 2 * 10)$$

$$= 7 * 10 - 3 * 23 \text{ {for all 10's and 23's groups}}$$

$$1 = 7 * (79 - 3 * 23) - 3 * 23$$

$$1 = 7 * 79 - 24 * 23$$

Chinese Remainder Theorem (CRT)

Example: Find an integer n satisfying:

$$n \equiv 2 \pmod{3}$$

$$n \equiv 3 \pmod{5}$$

$$n \equiv 2 \pmod{7}$$

Solution: using the mod notation :

$$n \equiv 2 \pmod{3} \rightarrow n = 3K + 2$$

$$n \equiv 3 \pmod{5} \rightarrow n = 5L + 3$$

$$\therefore 3K + 2 = 5L + 3$$

$$\therefore 3K - 5L = 1 \quad \{\text{Euclidean Algorithm}\}$$

$$\therefore K = 2 \text{ \& } L = 1$$

$$\rightarrow n = 8$$

Other solutions for n :

multiple of 5 and 3 {mod notation}

General solution for n :

$$n = 8 + 15m$$

To satisfy the 3rd mod equation;

$$n :: 8 + 15m = 7t + 2$$

$$15m - 7t = -6$$

$$\therefore m = 1 \text{ \& } t = 3$$

$$\rightarrow n = 23 \quad \{\text{satisfies the three linear equations}\}$$

CPT General Formula

if P_1, P_2, P_3 are relatively prime {no common factor}

then

$$n = r_1 \pmod{P_1}$$

$$n = r_2 \pmod{P_2}$$

$$n = r_3 \pmod{P_3}$$

The problem always has solution n . {Euler and Gauss applications}