

## Zadání

Vyřešte

$$a_1x \equiv b_1 \pmod{c_1}$$

$$a_2x \equiv b_2 \pmod{c_2}$$

...

$$a_nx \equiv b_n \pmod{c_n}$$

## Pozorování

*Je-li  $x$  řešením, pak i  $x \pm \text{lcm}(c_1, \dots, c_n)$  je řešením, a tedy existuje řešení  $x \in \{0, 1, \dots, \text{lcm}(c_1, \dots, c_n) - 1\}$ .*

$$a_1x \equiv b_1 \pmod{c_1}$$

$$a_1x + c_1t = b_1$$

- Nemá řešení, pokud  $d = \gcd(a_1, c_1)$  nedělí  $b_1$ .
- Jinak z Euklidova algoritmu:

```
(r, r') = (0, 1); (s, s') = (1, 0);  
while (a1 != 0) {  
    q = c1 / a1;  
    (c1, a1) = (a1, a1 - q * c1);  
    (r, r') = (r', r - q * r');  
    (s, s') = (s', s - q * s');  
}  
d = c1;
```

$$a_1r + c_1s = d$$

$$a_1r(b_1/d) + c_1s(b_1/d) = b_1$$

$$x = r(b_1/d) + (c_1/d)m$$

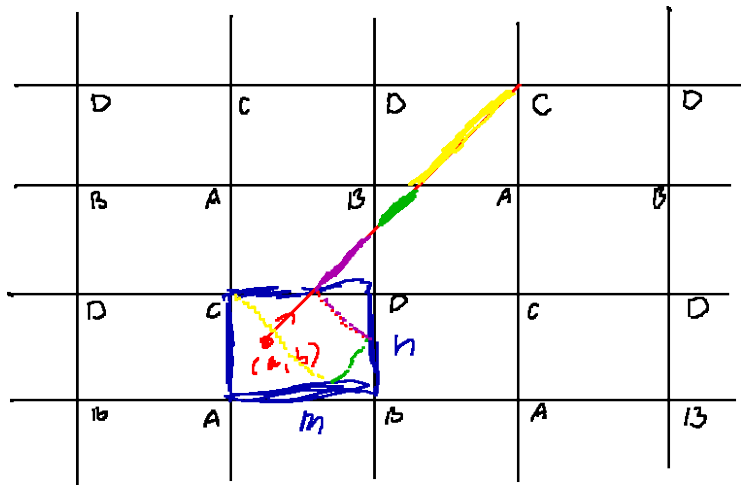
$$\begin{aligned}x &= \beta_1 + \gamma_1 m \\a_2 x &\equiv b_2 \pmod{c_2} \\&\dots \\a_n x &\equiv b_n \pmod{c_n}\end{aligned}$$

Redukce na

$$\begin{aligned}a_2 \gamma m &\equiv b_2 - a_2 \beta \pmod{c_2} \\&\dots \\a_n \gamma m &\equiv b_n - a_n \beta \pmod{c_n}\end{aligned}$$

## Zadání

*Na kulečnickovém stole o rozměrech  $n \times m$  pošleme kouli z bodu  $(a, b)$  ve směru  $(1, 1)$ , kde  $n, m, a, b$  jsou celá čísla. Který roh zasáhne jako první?*



$$a + x \equiv 0 \pmod{m}$$

$$b + x \equiv 0 \pmod{n}$$

Chceme: Nejmenší kladné řešení  $x$ .