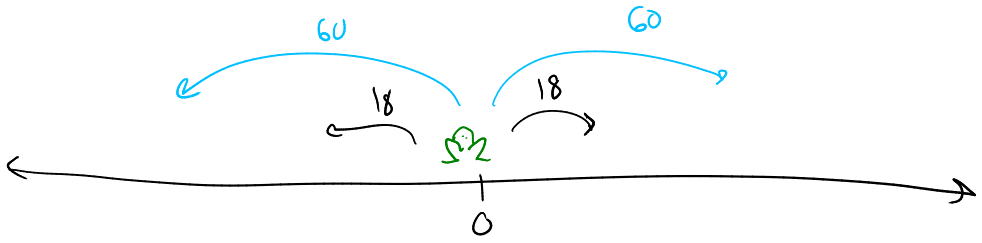

Frog can hop ± 18, jump ± 60. Where can it reach starting from 0?

12? $-60 + 18 + 18 + 18 + 18 = 12$. ✓

6? $60 - 3 \cdot 18 = 6$ ✓

3? ✗

1? ✗

8? ✗ — not a multiple of 6.

42252? ✓

42254? ✗

Theorem. (Bézout's theorem) Let $a, b \in \mathbb{N}$. Then there exist $s, t \in \mathbb{Z}$ such that

$$s \cdot a + t \cdot b = \gcd(a, b).$$

Proof (idea): Define $S = \{ja + kb \mid j, k \in \mathbb{Z}\}$.

Let d = smallest positive element of S.

$a = dq + r$, show $r \in S$. Since $r < d$, d is smallest positive in S, $r = 0$. $\Rightarrow d \mid a$.

etc.

How to find s, t? Extended Euclidean Algorithm.

eg $a = 60,\ b = 18.$

s	t	$60s + 18t$
1	0	60
0	1	18
1	−3	6
		0

60 mod 18 $= 60 - 3 \cdot 18$

gcd(60, 18)

$= \gcd(18, 60 \bmod 18)$

gcd(60, 18)

$60 \cdot 1 + 18 \cdot (-3) = 6.$

eg. $a = 39,\ b = 16.$

	s	t	$39s + 16t$	q
	1	0	39	
	0	1	16	2
−2×	1	−2	7	2
−2×	−2	5	2	3
−3×	7	−17	1	
			0	

gcd(39, 7)

$7 \cdot 39 - 17 \cdot 16 = 1.$