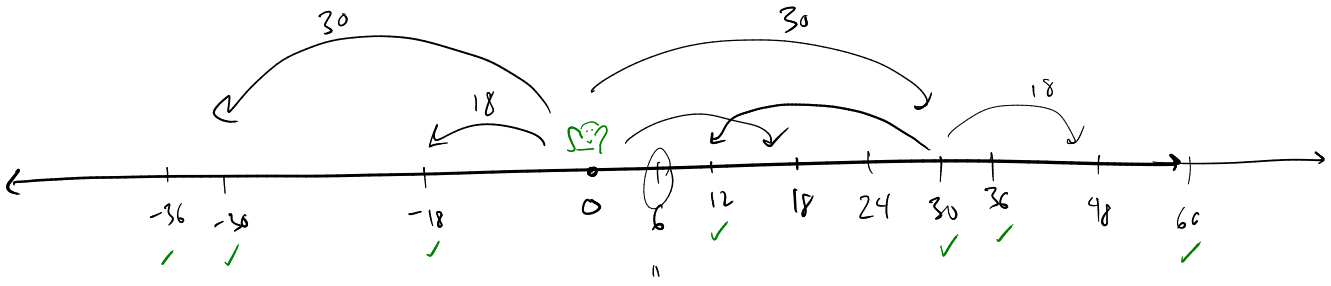

$6 = +18 - 30 + 18$

Where can frog reach?

- 1 ✗ — odd, can only reach even.
- Can reach every multiple of 6, + only multiples of 6.

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

$$sa + tb = \gcd(a, b).$$

Proof

Let $S = \{ja + kb \mid j, k \in \mathbb{Z}\}$. Note that S must have a smallest positive element, call it d. We will show that $d = \gcd(a,b)$. By definition, this means we must show ① $d \mid a$ and $d \mid b$, ② any other common divisor $g \mid a$, $g \mid b$ must divide d: $g \mid d$.

② Suppose $g \mid a$ and $g \mid b$. But $d = ja + kb$ for some j, k. And $g \mid ja$ and $g \mid kb$ and $g \mid (ja + kb = d)$.

① By the Division Alg., $a = qd + r$, where $0 \le r < d$.

$$r = a - qd = a - q(ja + kb) = a - qja - qkb$$
$$= (1 - qj)a + (-qk)b$$

So $r \in S$ by definition, since S contains all numbers made by adding copies of a and b. But $r < d$. Since d is smallest positive element of S, $r = 0$.

Hence $a = qd + r = qd + 0$, so $d \mid a$.

Likewise $d \mid b$. ∎

Hence, by definition, $d = \gcd(a,b)$; and hence

$\gcd(a,b) \in S$, ie. $\gcd(a,b) = s \cdot a + t \cdot b$ for some s, t.

But given a, b, can we compute s, t such that

$sa + tb = \gcd(a,b)$?

Yes, using the Extended Euclidean Algorithm.

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

	s	t	$60s + 18t$
	1	0	60
	0	1	18
$1 - 3 \cdot 0 \rightarrow$	1	−3	6
			0

each row should satisfy

] start w/ a, b.

$60 - 3 \cdot 18 = 6$

So subtract 3 copies of $(0, 1, 18)$ row from $(1, 0, 60)$ row.

Ex. $a = 39$, $b = 16$.

	s	t	$39s + 16t$	q
	1	0	39	
$-2\times$	0	1	16	39 div 16 = 2
$-2\times$	1	−2	7	16 div 7 = 2
$-3\times$	−2	5	2	7 div 2 = 3
	7	−17	1	
			0	

$\gcd(39, 16) = 1$

$39 \cdot 7 + 16(-17) = 1$.

$39x \equiv_{16} \ldots$

Solving modular equivalences.

$$3x \equiv_7 5.$$

Question: can we "cancel" the 3 by multiplying both sides by something?

ie. is there some s such that $3s \equiv_7 1$?

Yes — $3 \cdot 5 = 15 \equiv_7 1$.

So if we multiply both sides by 5:

→ $5 \cdot 3x \equiv_7 5 \cdot 5$

→ $\boxed{x \equiv_7 4}$ ✓

Theorem For all $a \in \mathbb{Z}$ and $m \in \mathbb{Z}^+$, if $\gcd(a, m) = 1$, then there exists some $b \in \mathbb{Z}$ such that

$$a \cdot b \equiv_m 1.$$

b is called the modular inverse of a modulo m.

Proof Let $a \in \mathbb{Z}$, $m \in \mathbb{Z}^+$ be arbitrary, and suppose $\gcd(a,m)=1$. Then by Bézout's Theorem, there exist $s, t \in \mathbb{Z}$ such that

$$s \cdot a + t \cdot m = 1.$$

But since $t \cdot m \equiv_m 0$, $\boxed{s \cdot a \equiv_m s \cdot a + tm = 1}$.

So s is an inverse of a modulo m, and we can compute it using the Extended Euclidean Algorithm.

Ex. Solve for x:

$$3x \equiv_9 5 - x$$

$$\rightarrow$$

$$4x \equiv_9 5$$

$$\rightarrow$$

$$-8x \equiv_9 -10$$

$$\rightarrow \quad x \equiv_9 -1 \equiv_9 8$$

	s	t	$4s + 9t$	q
	0	1	9	
$-2\times$	1	0	4	2
	-2	1	1	

-2: inverse of 4 modulo 9.

1: gcd(4,9)

Ex.

$$523x \equiv_{17405} 77.$$

$$\rightarrow$$

$$7987 \cdot 523x \equiv_{17405} 77 \cdot 7987$$

$$\rightarrow \quad \boxed{x \equiv_{17405} 5824}$$

s	t	$523s + 17405t$	q
0	1	17405	
1	0	523	33
-33	1	146	3
100	-3	85	1
-133	4	61	1
233	-7	24	2
-599	18	13	1
832	-25	11	1
-1431	43	2	5
7987	-240	1	

7987: inverse of 523 mod 17405