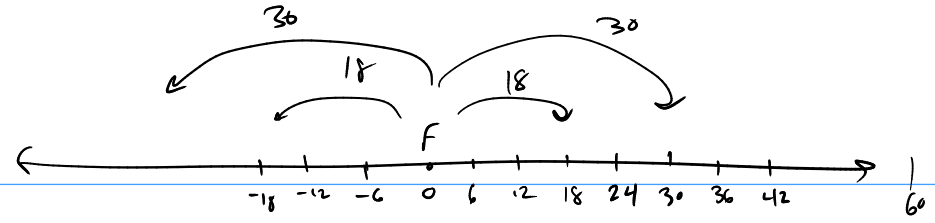
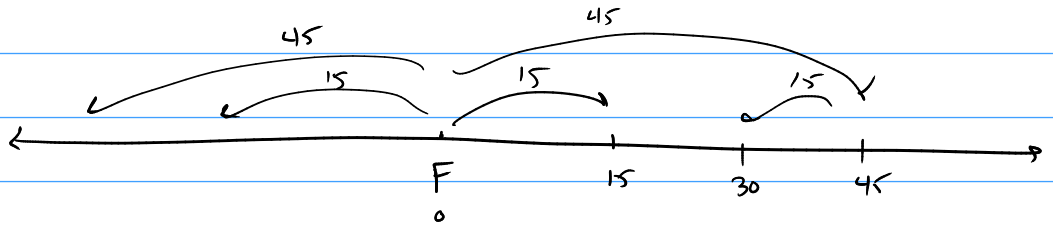


We can get to every multiple of 6!



Every multiple of 15.

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

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

Proof (sketch) Let $S = \{ja + kb \mid j, k \in \mathbb{Z}\}$. (set of all places the frog can reach)

Let d be the smallest positive element of S.

We will show that $d = \gcd(a,b)$.

- Show $d \mid a$: write $a = dq + r$. Show $r \in S$.
  But we know $0 \le r < d$, but d is smallest pos. elt of S. So $r = 0$.
- Likewise show $d \mid b$.
- Show if $c \mid a$ and $c \mid b$ then $c \mid d$.

– By def'n $d = \gcd(a,b)$.

Extended Euclidean Algorithm —— Compute s, t from a, b.

Ex. $a = 60$, $b = 18$.

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

keep track of s, t.

run Euclid. Alg. in this column

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

Ex. 39, 16.

s	t	$s\cdot 39 + t\cdot 16$	
1	0	39	
-2×0	-2×1	-2×16	$39/16$: $q=2$, $r=7$.
1	-2	7	$q=2$, $r=2$.
-2	5	2	$q=3$, $r=1$
7	-17	1	

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

Modular inverses.

Thm (Modular Inverses). Let $a \in \mathbb{Z}$ and $m \in \mathbb{Z}^+$. If $\gcd(a,m)=1$, then a has an inverse modulo m, that is, there exists $b \in \mathbb{Z}$ such that $a\cdot b \equiv_m 1$.

Proof: By Bézout's theorem, there exist s and t such that $s\cdot a + t\cdot m = 1$. But

$$1 = s\cdot a + t\cdot m \equiv_m s\cdot a + t\cdot 0 = s\cdot a.$$

Ex. Solve for x:

$$3x \equiv_7 5.$$

By the theorem, since $\gcd(3,7)=1$, 3 must have an inverse mod 7, which we can compute using Ext. Eucl. alg. It is 5. Hence

$$\rightsquigarrow \quad 5\cdot 3x \equiv_7 5\cdot 5$$

$$\rightsquigarrow \quad x \equiv_7 4.$$

Ex. Solve for x:

$$3x \equiv_9 5 - x.$$

$$4x \equiv_9 5.$$

$$-2 \cdot 4x \equiv_9 -2 \cdot 5$$

$$1x \equiv_9 -10$$

$$\boxed{x \equiv_9 8}$$

s	t	$9s + 4t$
1	0	9
0	1	4
1	-2	1

-2: inverse of 4 mod 9.

If we keep multiplying by 4, will we get back to 1 (mod 9)?

$$4^1 = 4$$

$$4^2 = 16 \equiv_9 7$$

$$4^3 \equiv_9 4 \cdot 7 \equiv_9 28 \equiv_9 1$$

$$5^1 = 5$$

$$5^2 \equiv_9 25 \equiv_9 -2$$

$$5^3 \equiv_9 5 \cdot (-2) \equiv_9 -10 \equiv_9 -1$$

$$5^4 \equiv_9 5 \cdot (-1) \equiv_9 -5 \equiv_9 4$$

$$5^5 \equiv_9 5 \cdot 4 \equiv_9 20 \equiv_9 2$$

$$5^6 \equiv_9 5 \cdot 2 \equiv_9 10 \equiv_9 1.$$

Thm Fermat's Little Theorem Let p be a prime and a be any integer such that p does not divide a. Then:

$$a^{p-1} \equiv_p 1.$$

Corollary: Suppose $\gcd(a, n) = 1$. If $a^{n-1} \not\equiv_n 1$, then n is not prime. On the other hand, if $a^{n-1} \equiv_n 1$, then... we don't know.

Proof. Let p be prime and let a be an integer such that $p \nmid a$. Consider

$$(1a) \cdot (2a) \cdot (3a) \cdots \cdot (p-1)a \pmod{p}.$$

Examples: $p = 3$, $a = 7$.

$(1a)$ $(2a)$ (mod p)

$\equiv_3 1$ $= 14 \equiv_3 2$

$p = 5$ $a = 11$

$(1a)$ $(2a)$ $(3a)$ $(4a)$ (mod 5)

$\equiv_5 1$ $\equiv_5 2$ $\equiv_5 3$ $\equiv_5 4$.

$p = 5$ $a = 8$

$(1a)$ $(2a)$ $(3a)$ $(4a)$

$\equiv_5 3$ $\equiv_5 1$ $\equiv_5 4$ $\equiv_5 2$.

$p = 7$ $a = 2$

$(1a)$ $(2a)$ $(3a)$ $(4a)$ $(5a)$ $(6a)$

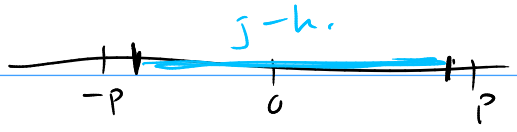
$\equiv_7 2$ $\equiv_7 4$ $\equiv_7 6$ $\equiv_7 1$ $\equiv_7 3$ $\equiv_7 5$.

Claim: $1a, 2a, \ldots, (p-1)a$ give us each of the numbers $1, 2, 3, \ldots, p-1$ exactly once (mod p).

By contradiction: Suppose $ja \equiv_p ka$. Then by definition $p \mid (ja - ka)$, so $p \mid a(j-k)$. Since we assumed $p \nmid a$, we must have $p \mid (j-k)$.

But both j, k are between 1 and $p-1$.

So the smallest possible value of $j-k$ is $1-(p-1) = -p+2$
And the largest possible value is $(p-1)-1 = p-2$.



But $p \mid (j-k)$, so the only possible thing it could be is $j-k=0$, so $j=k$.

Therefore, if $j \neq k$, then $ja \not\equiv_p ka$.

So $1a, 2a, 3a, \ldots, (p-1)a$ gives us $p-1$ different values so they must in fact be $1, 2, 3, \ldots, p-1$ in some order.

So:

$$(1a)\cdot(2a)\cdot(3a)\cdots(p-1)a$$
$$\equiv_p 1\cdot 2\cdot 3\cdots\cdot(p-1) = (p-1)!$$

But also,

$$(1a)\cdot(2a)\cdots(p-1)a = a^{p-1}\cdot(p-1)!.$$

So

$$(p-1)! \equiv_p a^{p-1}\cdot(p-1)!$$

But $p \nmid (p-1)!$, so $(p-1)!$ has a modular inverse mod p. So we can cancel it from both sides, giving

$$1 \equiv_p a^{p-1}.$$