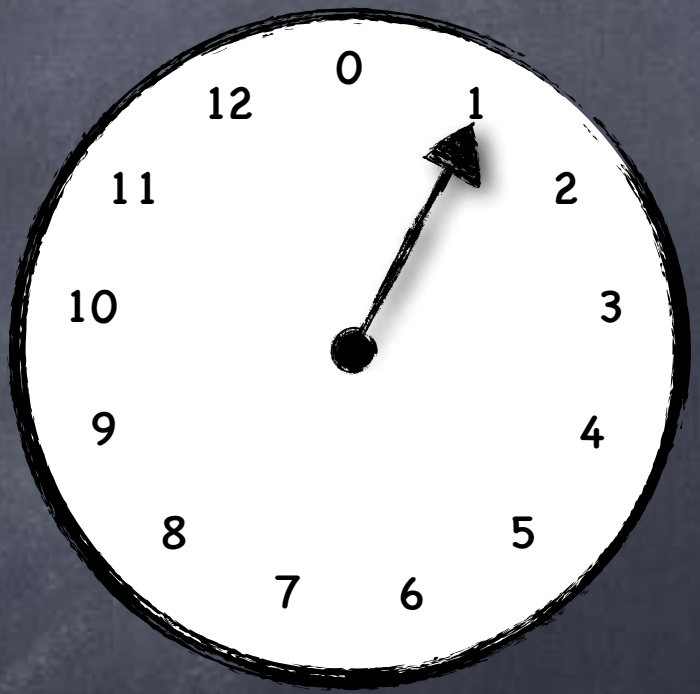
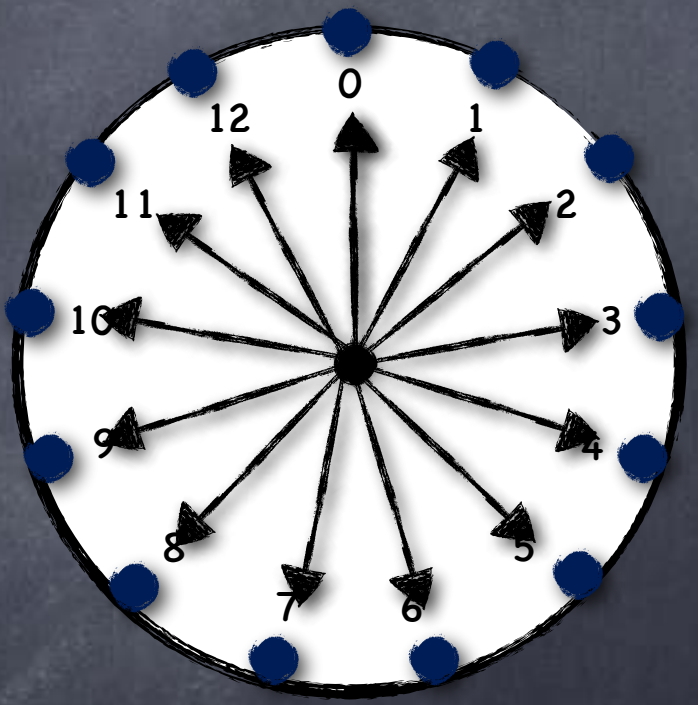
Numb3rs

GCD



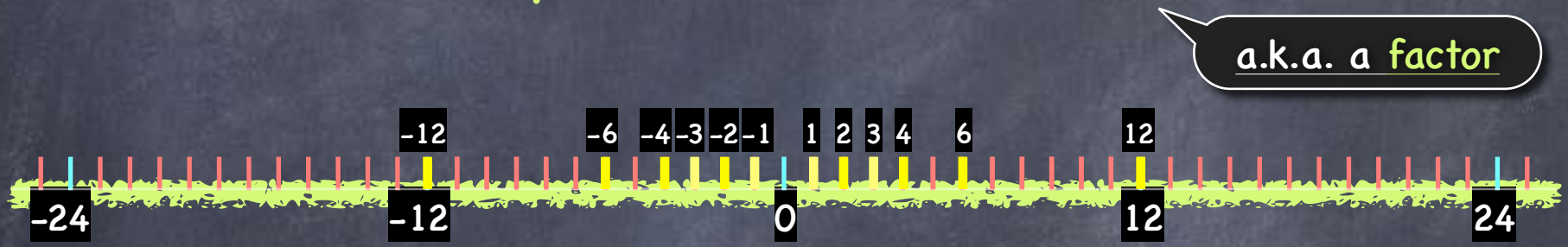
The Skippy Clock

- Has 13 hours on its dial!
- Needle moves two hours at a time
- Which all numbers will the needle reach?
  - Reaches all of them!



Divisibility

- Definition: For $n,d \in \mathbb{Z}$, $d|n$ (d divides n) if $\exists q \in \mathbb{Z}$ $n = qd$
  - $d|n$ ≡ n is a multiple of d ≡ d is a divisor of n



  - e.g. Multiples(12) = { …, -24, -12, 0, 12, 24, … }.
  - e.g. Divisors(12) = { ±1, ±2, ±3, ±4, ±6, ±12 }.
- Divisors(0) = $\mathbb{Z}$ [$\forall d \in \mathbb{Z}$ $d|0$]. Multiples(0) = {0} [$\forall n \in \mathbb{Z}$ $0|n \leftrightarrow n=0$]

Common Factors

- Common Divisor: m is a common divisor of integers a and b if m|a and m|b. [a.k.a. common factor]

- Greatest Common Divisor (for $(a,b)\neq(0,0)$)
  gcd(a,b) = largest among common divisors of a and b

  - Well-defined: 1 is always a common factor. And, no common factor is larger than min(|a|,|b|) (unless a=0 or b=0; see below). Then, gcd(a,b) is an integer in the range [1, min(|a|,|b|)].

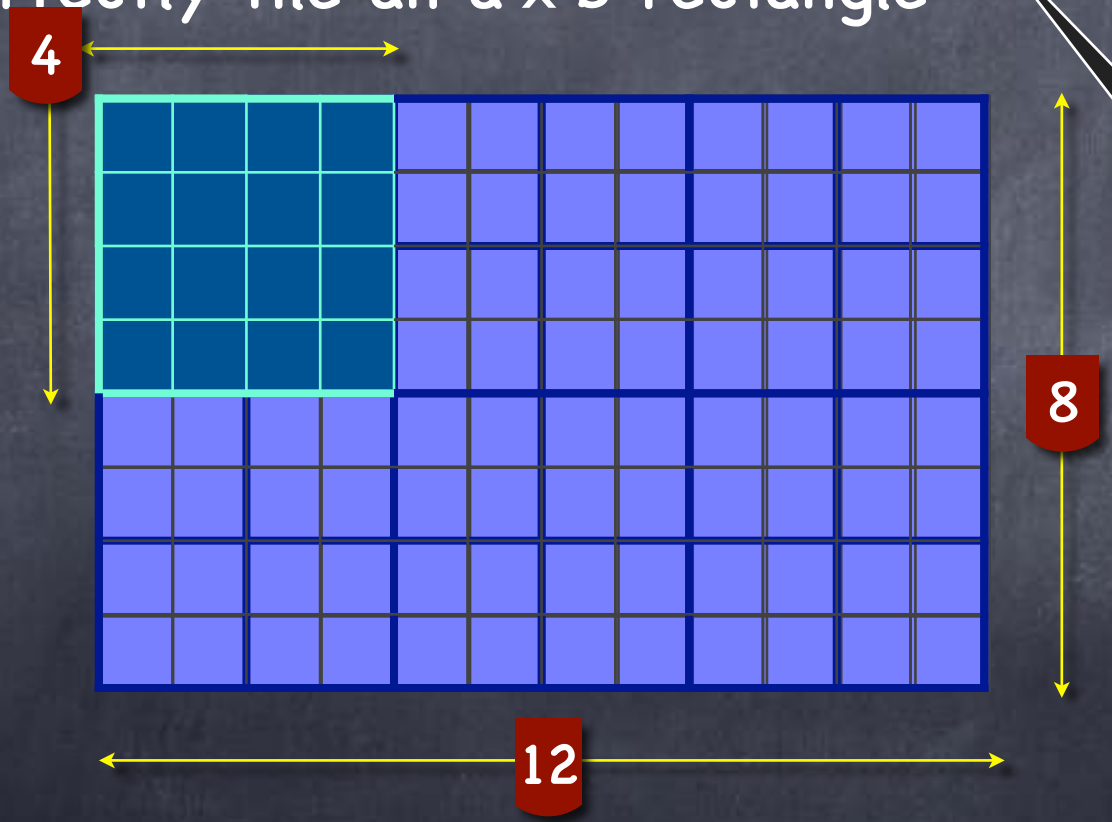
  - e.g. Divisors(12) = { ±1, ±2, ±3, ±4, ±6, ±12 }.
    Divisors(18) = { ±1, ±2, ±3, ±6, ±9, ±18 }.
    Common-divisors(12,18) = { ±1, ±2, ±3, ±6 }. gcd(12,18) = 6

  - e.g. If a|b and $(a,b)\neq(0,0)$, then gcd(a,b)=|a|.
    In particular, $\forall a\neq 0$ gcd(a,0) = |a|

GCD as Tiling

[Here all numbers are positive integers]

- d is a common factor of a & b, iff a d x d square tile can be used to perfectly tile an a x b rectangle



GCD: largest such square tile

Common Factors

- Common Divisor: c is a common divisor of integers a and b if c|a and c|b. [a.k.a. common factor]
- Greatest Common Divisor (for $(a,b) \neq (0,0)$)
  gcd(a,b) = largest among common divisors of a and b
- $\forall a,b,n \in \mathbb{Z}$, common-divisors(a,b) = common-divisors(a,b+na)
  - i.e., $(x|a \wedge x|b) \longleftrightarrow (x|a \wedge x|b+na)$. [Verify!]
- Hence, $\forall a,b,n \in \mathbb{Z}$, gcd(a,b) = gcd(a,b+na)
  - In particular, $\forall a,b \in \mathbb{Z}$, gcd(a,b) = gcd(a,r), where b = aq+r and $0 \leq r < a$

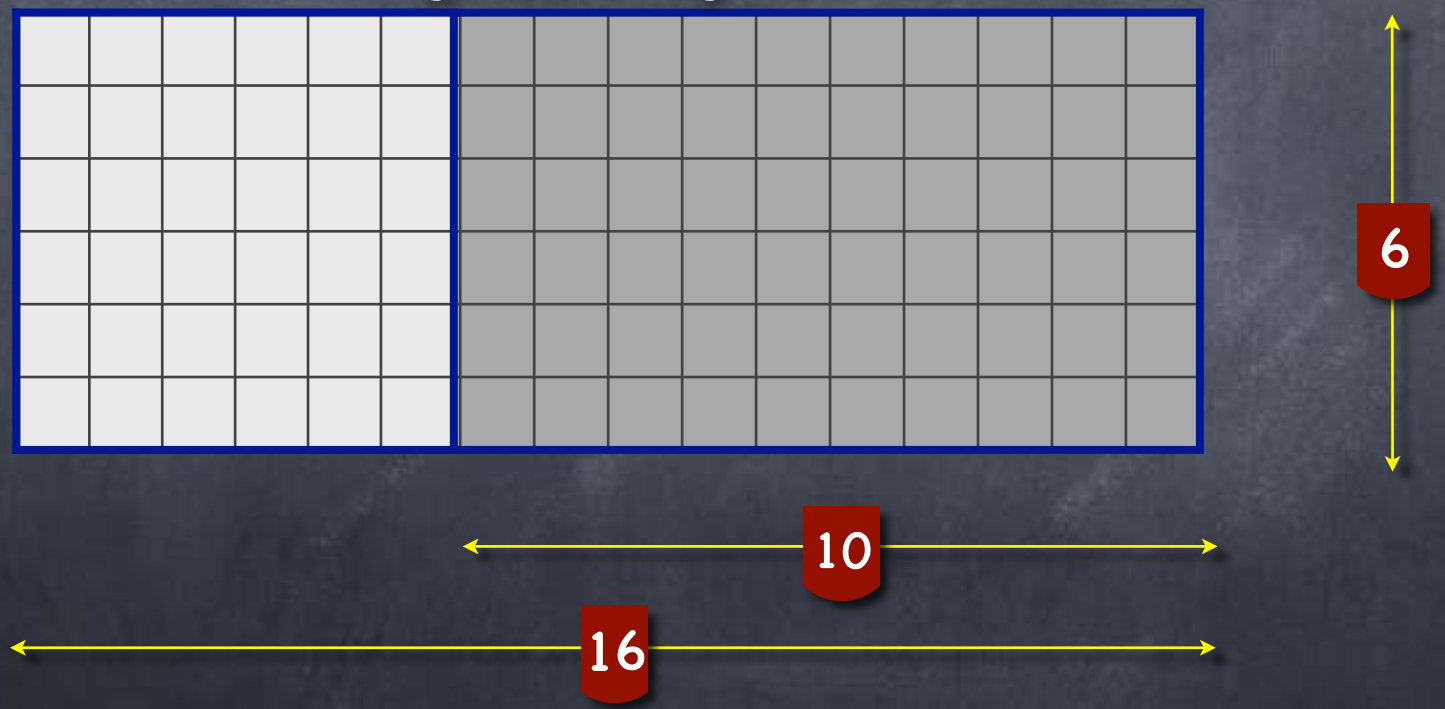
Euclid's GCD Algorithm

[Here all numbers are positive integers]

- Find the largest square perfectly tiling a x b rectangle

common-divisors(a,b) = common-divisors(a,b-a)

gcd(a,b) = gcd(a,b-a)



gcd(6,16)= gcd(6,10)

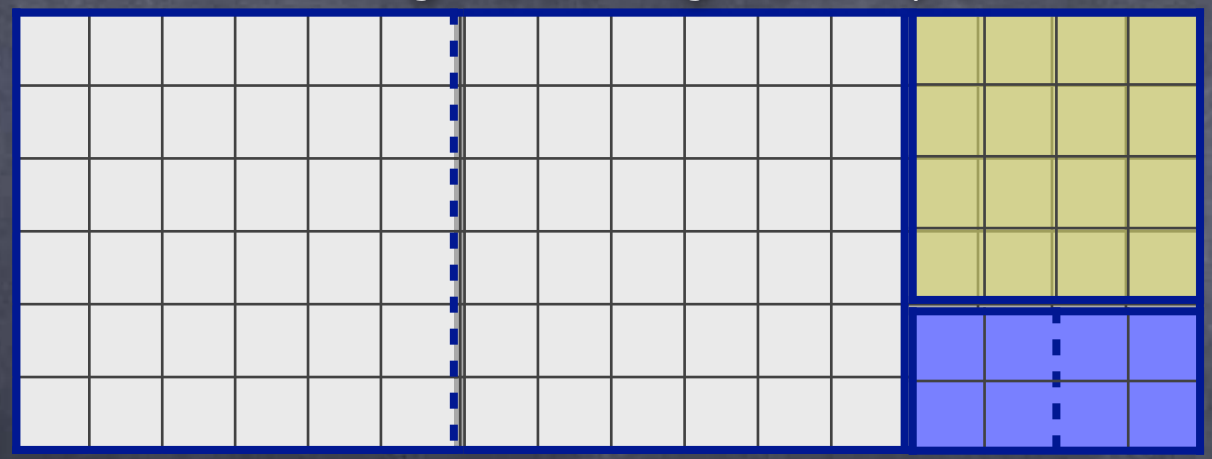
Euclid's GCD Algorithm

[Here all numbers are positive integers]

- Find the largest square perfectly tiling a x b rectangle

common-divisors(a,b) = common-divisors(a,b-qa)

gcd(a,b) = gcd(a,b-qa)



$\forall\ a,b \in \mathbb{Z}$

$\exists\ u,v \in \mathbb{Z}$

gcd(a,b) = u·a + v·b

$3 \cdot 6 - 1 \cdot 16 = 6 - (16 - 2 \cdot 6) = 6 - 4 = 2$

gcd(6,16)= gcd(6,4) = gcd(2,4) = 2

The Hoppy Bunny

- A bunny is sitting on an infinite number line, at position 0

- The bunny has two hops — of lengths a and b, where $a,b \in \mathbb{Z}$
  - Can hop to left or right (irrespective of the sign of a,b)
- What all points can the bunny reach?
- After u a-hops and v b-hops (u, v could be negative, indicating direction opposite a or b's sign), bunny is at $a \cdot u + b \cdot v$
- For any $a,b \in \mathbb{Z}$, let L(a,b) be the set of all integer combinations of a, b. i.e., $L(a,b) = \{ au+bv \mid u,v \in \mathbb{Z} \}$

The One Dimensional Lattice

- For any $a,b \in \mathbb{Z}$, let L(a,b) be the set of all integer combinations of a, b. i.e., $L(a,b) = \{ au+bv \mid u,v \in \mathbb{Z} \}$
- Claim 1: $\forall x \in L(a,b)$ $\gcd(a,b) \mid x$
- Proof: Fix any $x \in L(a,b)$. Let $x = au+bv$ for $u,v \in \mathbb{Z}$.
  - Let $g = \gcd(a,b)$. Then, can write $a = gp$, $b = gq$ for $p,q \in \mathbb{Z}$
  - Then, $x = gpu+gqv = g(pu+qv)$. Hence $g \mid x$

The One Dimensional Lattice

- For any $a,b \in \mathbb{Z}$, let L(a,b) be the set of all integer combinations of a, b. i.e., $L(a,b) = \{ au+bv \mid u,v \in \mathbb{Z} \}$
- Claim 1: $\forall x \in L(a,b)$ $\gcd(a,b) \mid x$
- Claim 2: $\gcd(a,b) \in L(a,b)$
- Proof: d be the least in $L^+(a,b) \triangleq L(a,b) \cap \mathbb{Z}^+$. [Well-Ordering]
  - Let $d=au+bv$ [Def of L(a,b)] & $a = dq+r$, $0 \le r < d$. [Q-R Theorem]
  - $r \notin L^+(a,b)$ since $r<d$. But $r=a-(au+bv)q \in L(a,b) \Rightarrow r=0$. i.e., $d|a$.
  - Similarly $d|b \Rightarrow$ d common divisor $\Rightarrow d \le \gcd(a,b)$ [Def of gcd]
  - But $d \in L(a,b) \Rightarrow \gcd(a,b) \mid d$ [Claim 1] $\Rightarrow \gcd(a,b) \le d$ [since $d \neq 0$].
  - So $\gcd(a,b) = d \in L(a,b)$

The One Dimensional Lattice

- For any $a,b \in \mathbb{Z}$, let L(a,b) be the set of all integer combinations of a, b. i.e., $L(a,b) = \{ au+bv \mid u,v \in \mathbb{Z} \}$
- Claim 1: $\forall x \in L(a,b)$ $\gcd(a,b) \mid x$
- Claim 2: $\gcd(a,b) \in L(a,b)$

Bézout's Identity

$\forall\ a,b \in \mathbb{Z}\ \ \exists\ u,v \in \mathbb{Z}$

$\gcd(a,b) = u \cdot a + v \cdot b$

- **Theorem**: L(a,b) consists of exactly all the multiples of gcd(a,b) i.e., $\forall x \in \mathbb{Z}$ $x \in L(a,b) \leftrightarrow g|x$, where $g \triangleq \gcd(a,b)$.
- Proof: By Claim 1, $x \in L(a,b) \rightarrow g|x$.
- Conversely, consider arbitrary x s.t. g|x. Say $x = g \cdot h$
  - By Claim 2, $g \in L(a,b)$. i.e., $g = au + bv$ for some $u,v \in \mathbb{Z}$
  - So $x = g \cdot h = a(uh) + b(vh) \in L(a,b)$.