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!
  - Because it reaches 1!
Integers: Basics

\( \mathbb{Z} \): set of all integers \{ ..., -2, -1, 0, 1, 2, ... \}

Operations addition, subtraction and multiplication (and their various properties)

**Definition:** For \( a, b \in \mathbb{Z} \), \( a \mid b \) (\( a \) divides \( b \)) if \( \exists q \in \mathbb{Z} \) \( b = qa \)

\( a \mid b \equiv b \text{ is a multiple of } a = a \text{ is a divisor of } b \)

**Multiples** of \( a \): \{ ..., -2a, -a, 0, a, 2a, ... \}

**Divisors** of \( b \): all \( a \) such that \( a \mid b \) [a.k.a. factors]
Consider the following two statements:

(I) $\forall a \in \mathbb{Z}, a \mid 0$

(II) $\forall b \in \mathbb{Z}, -1 \mid b$

A. One of them is undefined
B. (I) is true and (II) is false
C. (II) is true and (I) is false
D. Both are true
E. Both are false
Integers: Basics

Proposition: ∀ a, b, c ∈ ℤ if a|b, then a|bc

b = qa
⇒ bc = q′a,  where q′=qc

Proposition: ∀ a, b, c ∈ ℤ if a|b and a|c, then a|(b+c)

b = qa & c = q′a
⇒ b+c = q″a,  where q″=q+q′

Proposition: ∀ a, b, c ∈ ℤ if a|b and b|c, then a|c

c = qa & c = q′b
⇒ b+c = q″a,  where q″=qq′

Proposition: ∀ a, b, c ∈ ℤ if ac|bc and c ≠ 0, then a|b

bc = qac & c≠0
⇒ b = qa

Proposition: ∀ a, b, c ∈ ℤ if a|b and b≠0, then |a| ≤ |b|

b = qa & b≠0 ⇒ |b| = |q|⋅|a| where |q| ≥ 1
⇒ |b| = |a| + (|q|-1)⋅|a| ≥ |a|
Division

For any two integers \( a \) and \( b \), \( a \neq 0 \), there is a unique quotient \( q \) and remainder \( r \) (integers), such that
\[
b = q \cdot a + r, \quad 0 \leq r < |a|
\]

**Proof of existence**

- We shall prove it for all non-negative \( b \) and positive \( a \). Then, the other cases can be proven as follows:
  - \( a > 0, \ b < 0 \): \( b = -(b) = -(q \cdot a + r) = -(q+1)a + (a-r) \), and \( 0 \leq a-r < a \)
  - \( a < 0, \ b > 0 \): \( b = q \cdot (-a) + r = -qa + r \), and \( 0 \leq r < |a| \)
  - \( a < 0, \ b < 0 \): \( b = -(b) = -(q \cdot (-a) + r) = (q+1)a + (-a-r) \), and \( 0 \leq -a-r < |a| \)

- Fix any \( a > 0 \). We use strong induction on \( b \).
- Base cases: \( b \in [0,a) \). Then let \( q=0 \) and \( r=b \) : \( b = 0.a + b \).
- Induction step: We shall prove that for all \( k \geq a \),
  - (induction hypothesis): if \( \forall b \in \mathbb{Z}^+ \) s.t. \( b < k \), \( \exists q,r \) s.t \( b = qa + r \) & \( 0 \leq r \leq a \)
  - (to prove): then \( \exists q^*,r^* \) s.t. \( k = q^* \cdot a + r^* \) & \( 0 \leq r^* \leq a \).
  - Consider \( k' = k - a \). \( 0 \leq k' < k \). By ind. hyp. \( k' = q'a + r' \). Let \( q^* = q' + 1 \), \( r^* = r' \). \( \square \)
Division

For any two integers $a$ and $b$, $a \neq 0$, there is a unique quotient $q$ and remainder $r$ (integers), such that

$$b = q \cdot a + r, \quad 0 \leq r < |a|$$

**Proof of existence**

Also known as “Division Algorithm” (when you unroll the inductive argument, you get a (naïve) algorithm)

**Proof of uniqueness:**

**Claim:** if $b = q_1 \cdot a + r_1 = q_2 \cdot a + r_2$, where $0 \leq r_1, r_2 < |a|$, then $q_1 = q_2$ and $r_1 = r_2$

- Suppose, $q_1 \cdot a + r_1 = q_2 \cdot a + r_2$. Then $(r_1 - r_2) = (q_2 - q_1)a$. i.e., $a|(r_1 - r_2)$.
- W.l.o.g, $r_1 \geq r_2$. So, $0 \leq (r_1 - r_2) < |a|$. Now, the only multiple of $a$ in that range is 0. So $r_1 = r_2$. Then $(q_1 - q_2)a = 0$. Since $a \neq 0$, $q_1 = q_2.$
For any two integers $a$ and $b$, $a \neq 0$, there is a unique quotient $q$ and remainder $r$ (integers), such that

$$b = q \cdot a + r, \quad 0 \leq r < |a|$$

<table>
<thead>
<tr>
<th></th>
<th>0</th>
<th>1</th>
<th>2</th>
<th>3</th>
<th>4</th>
<th>5</th>
<th>6</th>
</tr>
</thead>
<tbody>
<tr>
<td>-2</td>
<td>-14</td>
<td>-13</td>
<td>-12</td>
<td>-11</td>
<td>-10</td>
<td>-9</td>
<td>-8</td>
</tr>
<tr>
<td>-1</td>
<td>-7</td>
<td>-6</td>
<td>-5</td>
<td>-4</td>
<td>-3</td>
<td>-2</td>
<td>-1</td>
</tr>
<tr>
<td>0</td>
<td>0</td>
<td>1</td>
<td>2</td>
<td>3</td>
<td>4</td>
<td>5</td>
<td>6</td>
</tr>
<tr>
<td>1</td>
<td>7</td>
<td>8</td>
<td>9</td>
<td>10</td>
<td>11</td>
<td>12</td>
<td>13</td>
</tr>
<tr>
<td>2</td>
<td>14</td>
<td>15</td>
<td>16</td>
<td>17</td>
<td>18</td>
<td>19</td>
<td>20</td>
</tr>
</tbody>
</table>

**Example:**

- $a = 7$
- $b = 11$
- $q = 1$, $r = 4$
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)≠(0,0))**
\[ \text{gcd}(a,b) = \text{largest among common divisors of } a \text{ and } b \]

Well-defined: 1 is always a common factor. And, no common factor is larger than \( \min(|a|,|b|) \) (unless \( a=b=0 \)). So \( \text{gcd}(a,b) \) 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 \}. \( \text{gcd}(12,18) = 6 \)

**e.g.** Divisors(0) = \( \mathbb{Z} \). \( \forall x \neq 0 \) \( \text{gcd}(x,0) = |x| \).
Also, \( \forall x,a \in \mathbb{Z}, |x| \in \text{Divisors}(ax) \). If \( x \neq 0 \), \( \text{gcd}(x,ax)=|x| \).
GCD as Tiling

[Here all numbers are positive integers]

A common factor of a & b, iff a d x d square tile can be used to perfectly tile an a x b rectangle
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)≠(0,0))
\[ \gcd(a,b) = \text{largest among common divisors of } a \text{ and } b \]

\[ \forall a,b,n \in \mathbb{Z}, \text{common-divisors}(a,b) = \text{common-divisors}(a,b+na) \]

i.e., \((x|a \land x|b) \iff (x|a \land x|b+na)\). [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 \times b rectangle

\text{common-divisors}(a,b) = \text{common-divisors}(a,b-a)

\text{gcd}(a,b) = \text{gcd}(a,b-a)

\text{gcd}(6,16) = \text{gcd}(6,10)
Euclid's GCD Algorithm

[Here all numbers are positive integers]

Find the largest square perfectly tiling a × b rectangle

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

gcd(a,b) = gcd(a,b−qa)

∀ a,b ∈ ℤ
∃ u,v ∈ ℤ

gcd(a,b) = u·a + v·b

3·6−1·16 = 6−(16−2·6) = 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: $L(a,b)$ consists of exactly all the multiples of $\gcd(a,b)$

Proof: Note that $\gcd(a,b)$ divides every element in $L(a,b)$. i.e., every element in $L(a,b)$ is a multiple of $\gcd(a,b)$. We shall prove below that $\gcd(a,b) \in L(a,b)$, so that all its multiples are also in $L(a,b)$ ($L(a,b)$ being closed under multiplication by integers).

By the well-ordering principle, let $d$ be the smallest element in $L^+(a,b) \triangleq L(a,b) \cap \mathbb{Z}^+$.

Let $d=au+bv$. Let $a=dq+r$, where $0 \leq r < d$. So, $r=a-(au+bv)q \in L(a,b)$. Since $r<d$, we require $r \notin L^+(a,b)$. So $r=0$. i.e., $d|a$.

Similarly, $d|b$. That is, $d$ is a common divisor. So, $d \leq \gcd(a,b)$.

But $d \in L(a,b) \Rightarrow \gcd(a,b)|d \Rightarrow \gcd(a,b) \leq d$. So $\gcd(a,b) = d \in L(a,b)$
Primes

Definition: \( p \in \mathbb{Z} \) is said to be a prime number if \( p \geq 2 \) and the only positive factors of \( p \) are 1 and \( p \) itself.

2, 3, 5, 7, 11, 13, 17, 19, 23, 29, 31, 37, 41, 43, 47, 53, 59, 61, ...

Unique Factorisation
(Fundamental Theorem of Arithmetic):
\[ \forall a \in \mathbb{Z}, \text{ if } a \geq 2 \text{ then } \exists! (p_1, \ldots, p_t, d_1, \ldots, d_t) \text{ s.t.} \]
\[ p_1 < \ldots < p_t \text{ primes, } d_1, \ldots, d_t \in \mathbb{Z}^+, \text{ and } a = p_1^{d_1} p_2^{d_2} \ldots p_t^{d_t} \]

Recall: We already saw that prime factorisation exists (using strong induction)

Will prove uniqueness now
Primes

Definition: \( p \in \mathbb{Z} \) is said to be a prime number if \( p \geq 2 \) and the only positive factors of \( p \) are 1 and \( p \) itself.

\[
\text{Euclid's Lemma}
\]
\[\forall a, b, p \in \mathbb{Z} \text{ s.t. } p \text{ is prime } (p \mid ab) \rightarrow (p \mid a \lor p \mid b)\]

Since the only positive factors of \( p \) are 1, \( p \), we have \( \gcd(a,p) = 1 \) or \( \gcd(a,p) = p \).

If \( \gcd(a,p) = p \), then \( p \mid a \checkmark \)

If \( \gcd(a,p) = 1 \), \( \exists u, v \text{ s.t. } 1 = au + pv \Rightarrow b = bau + bpv \Rightarrow b \in \mathbb{L}(ab,p) \)

But \( p \mid ab \) and \( p \mid p \). So \( p \mid b \).
Primes

Definition: \( p \in \mathbb{Z} \) is said to be a **prime number** if \( p \geq 2 \) and the only positive factors of \( p \) are 1 and \( p \) itself.

**Euclid’s Lemma**

\[ \forall a, b, p \in \mathbb{Z} \text{ s.t. } p \text{ is prime } (p \mid ab) \rightarrow (p \mid a \vee p \mid b) \]

Generalisation of Euclid’s Lemma (Prove by induction):

\[ \forall a_1, \ldots, a_n, p \in \mathbb{Z} \text{ s.t. } p \text{ is prime, } (p \mid a_1 \cdots a_n) \rightarrow \exists i, \ p \mid a_i \]

**Uniqueness of prime factorisation**: Suppose \( z \) is the smallest positive integer with two distinct prime factorisations as \( z = p_1 \cdots p_m = q_1 \cdots q_n \). \( \max\{p_1, \ldots, p_m\} \neq \max\{q_1, \ldots, q_n\} \) (Why?). So w.l.o.g., \( p_m > q_i \), \( i = 1 \) to \( n \). Now, \( p_m \mid q_1 \cdots q_n \Rightarrow p_m \mid q_i \) for some \( i \) (by Lemma). This contradicts \( p_m > q_i \).