Claim: base $b$ representation exists

- **Notn:** $(d_i)$ is shorthand for $(d_i, d_{i-1}, \ldots, d_1, d_0)$
- **Defn:** A base $b$ digit $d$ is a natural number with $0 \leq d < b$
- **Defn:** The base-$b$ interpretation of the digits $(d_i)$ is
  \[
  (d_i)_b := \sum_{i=0}^{\infty} d_i b^i
  \]
- **Defn:** A base-$b$ representation of $n \in \mathbb{N}$ is a sequence of digits $(d_i)$ with $n = (d_i)_b$

**Claim:** For all $a \in \mathbb{N}$, and $b > 1$, there is a sequence $(d_i)$ with $(d_i)_b = a$

**Proof idea/question:** We'll do an induction. When thinking inductively, you want to figure out how to make a little bit of progress to reduce the problem to a simpler problem. In this case, you're given $a$ and $b$ and want to find the digits of $a$. Is there any single digit of $a$ that you can express in terms of $a$ and $b$?

\[
a = (\ldots d_1 d_0, d_{i-1}, d_{i-2}, \ldots, d_2, d_1, d_0)_b
\]

- **use** $\text{quot}(a, b)$
- **exist by induction**
- **let** $d_j \ldots d_1 d_0$, be $d_{j-1}, d_{j-2}, \ldots, d_2, d_1, d_0$
- **let** $d_0 = \text{rem}(a, b)$
- **need to check** $(d_i)_b = a$
- **use** $a = q b + r$.
Divisors and divisibility

\( a \) "divides" \( b \) (evenly)

- \( \text{rem}(a, b) = 0 \) (equivalent, prove using def of uniqueness of \( \text{rem} \))
- \( \exists \, c \) such that \( a \cdot c = b \). \( \text{def} \) of \( a \) divides \( b \).

Notation: \( a \mid b \) means \( a \) divides \( b \).
Euclid's greatest common divisor algorithm

**Defn**: \( a \) divides \( b \) (written \( a \mid b \)) if there exists \( c \) with \( ac = b \).

**Claim**: Let \( g : \mathbb{N} \times \mathbb{N} \to \mathbb{N} \) be given as follows:

\[
\gcd(a, b) = \begin{cases} 
  a & \text{if } b = 0 \\
  \gcd(b, r) & \text{if } b > 0 
\end{cases}
\]

where \( r = \text{rem}(a, b) \), otherwise.

Then \( g(a, b) \) is the greatest common divisor of \( a \) and \( b \).

**Proof (common divisor):**

Proof by induction (on \( b \)).

Let \( P(b) \) be the statment: 

\[
\text{WTS: } \forall a, b : \gcd(a, b) \mid a \text{ and } \gcd(a, b) \mid b.
\]

We'll prove \( P(a) \) and \( P(b) \) assuming \( P(b-1) \).

\( P(0) \):

\[
\text{WTS: } \forall a, g(a, 0) \mid a \text{ and } g(a, 0) \mid 0.
\]

Choose any \( a \). WTS: \( g(a, 0) \mid a \text{ and } g(a, 0) \mid 0 \).

Well, \( g(a, 0) = a \).\( a \mid a \) since \( a = a \).
\( a \mid 0 \) since \( a \cdot 0 = 0 \).

\( P(b) \):

\[
\forall a, g(a, b) \mid a \text{ and } g(a, b) \mid b, \text{ assume } P(b-1), P(b-2).
\]

Choose other \( a \). We know \( b > 0 \), so \( g(a, b) = g(b, r) \) where \( r = \text{rem}(a, b) \).

We know \( g(b, r) \mid b \) and \( g(b, r) \mid r \) by \( P(r) \) applied to \( a = b \).

So \( g(b, r) \mid b \) and \( g(b, r) \mid r \) (have assumed \( P(r) \) since \( r < b \)).

So \( g(a, b) \mid b \) and \( g(a, b) \mid r \).

WTS \( g(a, b) \mid a \) and \( g(a, b) \mid b \).

\( g(a, b) \) divides \( a \) if \( \frac{a}{g(a, b)} = b \).

Similarly, \( b \) divides \( a \) if \( \frac{b}{g(a, b)} = r \).

WTS \( a = g(a, b) \).

Also, by defn of \( r \), \( a = qb + r \).

So \( a = g(a, b) \).

\[
= g \cdot q + g \cdot r.
\]

\[
= (bc + d)g.
\]

Let \( e = gc + d \).

Then \( a = e \cdot g \)

So \( g \mid a \). \( \checkmark \)
Euclid's greatest common divisor algorithm

**Defn:** a divides b (written \( a \mid b \)) if there exists c with \( ac = b \)

**Claim:** Let \( g : \mathbb{N} \times \mathbb{N} \rightarrow \mathbb{N} \) be given as follows:

\[
g(a, b) := \begin{cases} 
  a, & \text{if } b = 0 \\
  g(b, r) \text{ where } r = \text{rem}(a, b), & \text{otherwise}
\end{cases}
\]

Then \( g(a, b) \) is the greatest common divisor of a and b.

**Proof (greatest):**

- In fact, we'll show that every other common divisor actually divides \( g \).

- i.e. \( \forall c \), if \( c \mid a \) and \( c \mid b \) then \( c \mid g \).

**Proof by induction.**

Let \( P(b) = \forall c \mid a \text{ and } c \mid b \text{ then } c \mid g \).

**P(0):** Assume \( c \mid a \) and \( c \mid 0 \). \( \forall c \), \( c \mid g(a, 0) \). \( \forall c \), \( g(a, 0) = a \). \( \forall c \), \( c \mid a \). But we assumed \( c \mid a \).

**P(b):** Assume \( c \mid a \) and \( c \mid b \). \( \forall c \), \( c \mid g(a, b) \). \( \forall c \), \( c \mid g(a, b) \). \( \forall c \), \( g(a, b) = g(b, r) \). \( \forall c \), \( c \mid g(b, r) \). If we could show \( c \mid b \) and \( c \mid r \), then \( \forall c \), \( c \mid g(b, r) \). So \( \forall c \), \( c \mid a \) and \( c \mid b \). \( \forall c \), \( c \mid b \) by assumption. \( \forall c \), \( c \mid a \).