Lecture 15: base b, divisibility, gcd

**Defn:** A base b digit d is just a number d with $0 \leq d < b$

**Defn:** $(d)_b := \sum_{i \geq 0} d_i b^i = d_0 b^0 + d_1 b + d_2 b^2 + \cdots + d_i b^i$

**Claim:** For all $a \in \mathbb{N}$, and any $b \geq 2$, there exists base $b$ digits $(d_i)_b$ such that $a = (d)_b$.

**Proof:** By induction on $a$. Let $P(a)$ be the statement "$a$ is a base $b$ number." We will show $P(0)$ and $P(a)$, assuming $P(a - 1)$.

Idea: let's build one digit, do rest inductively.

\[
\text{rem}(a, b) = \text{last digit (least place)}
\]

\[
\text{rem}(a, 10) = 3
\]

\[
\text{quot}(a, 10) = 125
\]

\[
\text{digits of quot}(a, b) = \text{rest} + \text{the digits}
\]

**P(0):** Was a sequence of digits $W$ with $(d_i)_b = 0$

\[
\text{let } d_0 = 0 \text{ then } (d_0)_b = \sum_{i=0}^\infty d_i b^i = 0.
\]

**Alt:** $d_0 = 0, d_1 = 0$ then $(00)_b = 0 \cdot b + 0 \cdot 1 = 0$

**Alt:** let $(d_i)$ be the empty sequence

\[
\text{convention: } \emptyset \text{ anything } = 0
\]

**P(a):** Assume $P(a - 1), P(a - 2), \ldots, P(0)$

\[
\text{let } d_0 = \text{rem}(a, b)
\]

\[
\text{let } d_1, \ldots, d_i = \text{digits of quot}(a, b).
\]

\[
\text{exit because quot}(a, b) < a
\]

\[
\text{so we have } P(\text{quot}(a, b))
\]

Let $q = \text{quot}(a, b), r = \text{rem}(a, b)$

By $P(q)$, know $\exists (d_i')$ with $(d_i')_b = q$

\[
\text{let } d_1 = d_0', d_2 = d_1', \ldots
\]

\[
d_i+1 = d_i'
\]

then $a = qb + r$ (defn of $a, b, r$

\[
= qb + d_0 \cdot b^0
\]

\[
= b (d_0')_b + d_0 \cdot b^0 \quad \text{(defn of } d_i')
\]

\[
= (b \sum_{i=0}^\infty d_i' b^i) + d_0 b^0 \quad \text{(defn of base } b)
\]

\[
= \sum_{i=0}^\infty d_i \cdot b^i + d_0 b^0 \quad \text{defn of } a
\]

\[
= \sum_{i=0}^\infty d_i \cdot b^i + d_0 b^0 = \sum_{i=0}^\infty d_i b^i = (d_i)_b.
\]
Working with base $b$ representations

Claim (base $b$ representation is unique): If $(d_i)_b = (d'_i)_b$ and neither $d_i$ nor $d'_i$ start with a zero, then $(d_i) = (d'_i)$.

Proof sketch: By induction on the length of $(d_i)$; use uniqueness of quotient and remainder

Claims: Your familiar digit-by-digit algorithms for working in base 10 (e.g. long addition, subtraction, multiplication, division) also work in base $b$

Proofs: Later, when we have better tools for working with strings

\[
\begin{align*}
26 &= 3 \cdot 7 + 5 \\
9 &= 1 \cdot 7 + 2 \\
35 &= 5 \cdot 7 + 0
\end{align*}
\]
Divisibility

**Defn:** If \( a, b \in \mathbb{N} \) then we say “\( a \) divides \( b \)” (evenly) if

A. \( b/a \) is defined
B. \( \exists k \in \mathbb{N} \) such that \( ab = k \)
C. \( \exists k \in \mathbb{N} \) such that \( ka = b \)
D. \( \exists k \in \mathbb{N} \) such that \( a = kb \)
E. Unsure/other

**Notation:** “\( a \mid b \)” is shorthand for “\( a \) divides \( b \)”

3 divide 6? ✓ yes
6 divide 3? no
Let $g : \mathbb{N} \times \mathbb{N} \to \mathbb{N}$ be given by:

$$g(a, b) = a \cdot b$$

where $g(1, b) = \text{gcd}(1, b)$ is the greatest common divisor. Euclid's algorithm is defined inductively by:

$$a = bq + r$$

where $r < b$. So, $r \leq b$ eventually. So we can use the inductive rule:

$$g(a, b) = g(b, r)$$

and $g$ is a valid function.
GCD is a common divisor

**Defn:** \( a \mid b \) means there exists \( k \) such that \( ka = b \) if \( b > 0 \)

**Defn:** \( g(a, 0) := a \), and \( g(a, b) := g(b, r) \) where \( r = \text{rem}(a, b) \) (so \( a = qb + r \))

**Claim:** For all \( a \in \mathbb{N}, b \in \mathbb{N} \), \( g(a, b) \mid a \) and \( g(a, b) \mid b \)

**Proof:** Claim is the same as \( \forall b \in \mathbb{N}, g(a, b) \mid a \) and \( g(a, b) \mid b \)

we'll prove this by induction on \( b \). Let \( P(b) := \)

\( P(0) := \forall a \in \mathbb{N}, g(a, 0) \mid a \) and \( g(a, 0) \mid 0 \).

well \( g(a, 0) = a \) by defn.

\( a \mid a \) because \( 1 \cdot a = a \)

\( a \mid 0 \) because \( 0 \cdot a = 0 \)

\( P(b) \), assuming \( P(b-1), ..., P(0) \):

\( \forall a \in \mathbb{N}, g(a, b) \mid a \) and \( g(a, b) \mid b \)

know \( g(a, b) := g(b, r) \), and \( P(r) \) tells:

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

... finish next time
GCD is the greatest common divisor

**Defn:** \( a \mid b \) means there exists \( k \) such that \( ka = b \)

**Defn:** \( g(a, 0) := a \), and \( g(a, b) := g(b, \text{rem}(a, b)) \) where \( r = \text{rem}(a, b) \) (so \( a = qb + r \))

**Claim:** For all \( a, b, c \in \mathbb{N} \), if \( c \mid a \) and \( c \mid b \) then \( c \leq g(a, b) \)

**Proof:** (next time (exercise))