Lecture 15: Induction & algorithms, base b representation

- Finish proof of Euclidean division algorithm
- "Executing" proofs
- Uniqueness of quotient & remainder
- "Base b" number representations

Applications
- Proof execution: program synthesis
- Base b: encoding data (necessary for building computers)
(proof cont from last time / sides)

Case: \( r' = b - 1 \) 

Know \( a = q b + r' + 1 \) 

\( WTS \) \( a \geq q b + r \) with \( a = q b + r \).

Know \( a = q' b + (b-1) + 1 \)

\[ = q' b + b = (q' + 1) b + 0 \]

So, if we let \( q = q' + 1 \), \( r = 0 \), then \( a = q b + r \) and \( 0 \leq r < b \). √
Want to find $b$ so that $a = 2b + r$ (and $0 < r < 2$)

1. Find $q', r'$ st. $a' = 2q' + r'$
   1a. Find $q'', r''$ st. $a'' = 2q'' + r''$
      1a(i) Find $q''$, $r''$ st. $q'' - 0$, $r'' - 0$
      0 = $2q'' + r''$
      $r'' + 1 = 1 < b^2$

1a(ii) So $q'' = 0$
      $r'' = r'' + 1$
      $a'' = 2q'' + r'' = 2 \cdot 0 + 1$

1b. $r'' + 1 < b$ ? No, $r'' + 1 = 2 = b$ (i.e., $r'' = b - 1$)

2. So let $q'' = q'' + 1 = 1$
   $r'' = 0$
   $a'' = 2q'' + r''$
   $2 = 1 \cdot 2 + 0$

2. $r'' + 1 = 1 < b = 2$

$a = 3 = q b + r = 1 \cdot 2 + 1$. 
Claim: If \( a = qb + r \) with 0 \( \leq r < b \), then \( \{q, r\} \) are unique.

Proof: Assume \( a = q_1b + r_1 \) and \( a = q_2b + r_2 \) with 0 \( \leq r_1, r_2 < b \).

Then \( r_1 = r_2 \).

Since \( a = q_1b + r_1 \) and \( a = q_2b + r_2 \), it is possible to write:

\[ a = q_1b + r_1 = q_2b + r_2 \]

Therefore, \( q_1b + r_1 = q_2b + r_2 \).

Subtracting \( q_1b \) and \( q_2b \) from both sides gives:

\[ r_1 - r_2 = (q_1 - q_2)b \]

Since 0 \( \leq r_1, r_2 < b \), this implies \( r_1 = r_2 \).

Thus, \( \{q_1, r_1\} = \{q_2, r_2\} \).

Therefore, \( \{q, r\} \) are unique.
base $b$ representation:
write its using digits $0, 1, 2, \ldots, b-1$

$$6\cdot10^4 + 1\cdot10^3 + 2\cdot10^2 + 3\cdot10^1 + 4\cdot10^0$$

(base 10)

$$\begin{array}{c}
\text{digits 0, 1, } 2 \\
\text{base 2}
\end{array}$$

$$1\cdot2^3 + 0\cdot2^2 + 1\cdot2^1 + 0\cdot2^0 = (10)_2$$

**Defn:** If $d_i$ is a sequence of digits $d_j d_{j-1} \ldots d_2 d_1 d_0$ then $(d_i)_b = d_j b^j + d_{j-1} b^{j-1} + \ldots + d_1 b^1 + d_0 b^0 = \sum_i d_i b^i$
Claim: For all $n$, $b \geq 2$, $\exists$ a base-$b$ representation of $n$.

Proof:
- Use induction on $n$.

In inductive step:
- How do you find the last digit of $n$?
- Use induction to find rest of the digits of $n$.