Announcements

- **Reminder**: Quiz 1 is on Wednesday, here, first 15 minutes of class

  http://www.cs.uiuc.edu/class/sp10/cs173

The Division Theorem

- **Recap**: $a \mid b$ if $\exists n \in \mathbf{Z},\ b = a.n$

- **The Division Theorem**: $\forall a \in \mathbf{Z}, \forall b \in \mathbf{Z^+}, \exists!\ q \in \mathbf{Z}, \exists! r \in \mathbf{Z}$ such that $a = bq + r \quad \wedge \quad 0 \leq r < b$
  - q is the quotient and r is the remainder

- We get "uniqueness" by the fact that the remainder r is in $[0, b)$
  - we write the remainder on dividing a by b as $a \bmod b$
  - *Examples*: $12 \bmod 5 = 2 = 2 \bmod 5$, $-8 \bmod 3 = 1$

- Three important points about mod:

1. In this class, we will always use the above definition of mod
2. Use "mod" for this definition (not rem, %, etc. from programming)
3. When programming, check what your language does for negatives
   - Wikipedia has a good page

Well Ordering Property

- **Property**: Every *non-empty* set of natural numbers has a smallest element
- Note that a similar property does *not* hold for real numbers!

- **Proof of Division Theorem (existence)**:

  Let S = set of non-negative numbers of the form $a - bq$, where $q \in \mathbf{Z}$

  S is non-empty, so it has a smallest value r for some $q \in \mathbf{Z}$

  Hence $r \geq 0$ and $r = a - bq$ i.e., $a = bq + r$

  Suppose $r \geq b$. Then $r - b \in S$ because $r - b \geq 0$ and

  $r - b = a - bq - b = a - b(q+1) < r$

  This contradicts the fact that r is the *smallest* value in S

- **Proof of Division Theorem (uniqueness)**: Try a proof by contradiction!

Congruence mod *k*

- **Definition**: $a \in \mathbf{Z}$ is congruent to $b \in \mathbf{Z}$ mod k if $k \mid (a - b)$
  - Notation: $a \equiv b \pmod{k}$

- *Examples*: $17 \equiv 5 \pmod{12}$
  $-3 \equiv 4 \pmod{7}$
  $3 \not\equiv -3 \pmod{7}$

- **Theorem**: For all a, b, k, $a \equiv b \pmod{k} \leftrightarrow (a \bmod k) = (b \bmod k)$

- **Claim**: For all a, b, c, d, k, if $a \equiv b \pmod{k}$ and $c \equiv d \pmod{k}$ then $a + c \equiv b + d \pmod{k}$

- **Proof**: By definition, $k \mid (a - b)$ and hence $\exists n$, $(a - b) = kn$ and $k \mid (c - d)$ and hence $\exists m$, $(c - d) = km$. So
  $(a + c - (b + d)) = (a - b) + (c - d) = kn + km = k(n + m)$