Friday

Number Theory

Note that we are not covering all number theory topics in class today; make sure you review the textbook to be sure you understand all the topics, *e.g.,* primes, euclidean algorithm.

Divisibility

divides: a divides b ($a \mid b$) for $a, b \in \mathbb{Z}$ if and only if $b = an$ for some integer n. Some special cases:

- $7 \mid 0$ since $0 = 7 \cdot 0$
- $0 \nmid 7$ since $7 \neq 0 \cdot n$
- $-3 \mid 12$ since $12 = -3 \cdot -4$

Divisibility example: Prove the following claim by direct proof: for any integers a, x, y, b, c, if $a \mid x$ and $a \mid y$, then $a \mid bx + cy$.

Let $a, x, y, b, c \in \mathbb{Z}$ s.t. $a \mid x$ and $a \mid y$.
By the definition of divides, $x = an$ and $y = am$ for some $n, m \in \mathbb{Z}$.
So $bx + cy = ban + cam = a(bn + cm)$.
$bn + cm \in \mathbb{Z}$ since $b, n, c, m \in \mathbb{Z}$.
Therefore, $a \mid (bc + cy)$ by the definition of divides.

GCD and LCM

GCD: the greatest common divisor of integers a and b is the largest integer c that divides both a and b.
e.g., $\gcd(6, 10) = 2$
if $\gcd(a, b) = 1$ we call a and b relatively prime

LCM: the least common multiple of integers a and b is the smallest *positive* integer c such that both a and b divide c.
e.g., $\mathrm{lcm}(6, 10) = 30$

Modular Arithmetic

congruence mod k: if k is any positive integer, $a, b \in \mathbb{Z}$ are congruent mod k (written $a \equiv b \pmod{k}$) if and only if $k \mid (a - b)$. In other words, a and b differ by a factor of k.
e.g., $17 \equiv 5 \pmod{12}$, $5 \equiv 12 \pmod{12}$, $38 \equiv 3 \pmod{7}$
note: mod is not an operation; we are saying a and b are congruent to each other under some special mathematical system; *i.e.,* when we divide by k and find the remainder

Modular arithmetic example: Prove the following claim by direct proof: for any integers a, b, c, d, k with $k > 0$, if $a \equiv b \pmod{k}$ and $c \equiv d \pmod{k}$ then $(a + c) \equiv (b + d) \pmod{k}$.

Lemma: Let's first prove that linearity of divides holds over addition. In other words, for $a, b, k \in \mathbb{Z}$, if $k \mid a$ and $k \mid b$ then $k \mid a + b$.
Let $a, b, k \in \mathbb{Z}$ such that $k \mid a$ and $k \mid b$.

Since $k \mid a$ and $k \mid b$ by definition of divides $a = km$ and $b = kn$ for $n, m \in \mathbb{Z}$. So $a + b = km + kn = k(m + n)$ and since $m, n \in \mathbb{Z}$ then $m + n$ is also $\in \mathbb{Z}$ thus $k \mid a + b$. Thus we have shown that the linearity of division hold over addition.

Main proof: Let $a, b, c, d, k \in \mathbb{Z}$ with $k > 0$ s.t. $a \equiv b \pmod{k}$ and $c = d \pmod{k}$.

From the definition of mod we get $k \mid a - b$ and $k \mid c - d$.

From linearity of divides we get $k \mid (a - b) + (c - d)$ which is equivalent to $k \mid (a + c) - (b + d)$, so $(a + c) \equiv (b + d) \pmod{k}$.