CS 173 Lecture 4

Divisibility

- "divides" : a divides b $(a \mid b)$ for $a, b \in \mathbb{Z}$ iff $b = an$ for some integer n

ex. $7 \mid 0$ since $0 = 7 \cdot n$, $n = 0$

$0 \nmid 7$ since $7 \neq 0 \cdot n$ $\forall n$

$-3 \mid 12$ since $12 = -3 \cdot -4$

Proof:

ex. prove: For any integers a, x, y, b, c, if $a \mid x$ and $a \mid y$ then $a \mid bx + cy$

Let $a, x, y, b, c \in \mathbb{Z}$ and let $a \mid x$ and $a \mid y$. By definition of divides, $x = a \cdot n$ and

variable declaration

assume hypothesis true

$y = a \cdot m$ for some $m, n \in \mathbb{Z}$. Then $bx + cy = b(an) + c(am) = a(bn + cm)$.

Since $b, n, c, m \in \mathbb{Z}$, $bn + cm \in \mathbb{Z}$, so $a \mid bx + cy$.

GCD and LCM

- GCD: greatest common divisors of integers a and b is the largest c such that $c \mid a$ and $c \mid b$
- If $\gcd(a, b) = 1$, a and b are relatively prime
- LCM: least common multiple of integers a, b is the smallest positive integer c such that $a \mid c$ and $b \mid c$

Congruence mod k

- If k is any positive integer, then a and b are congruent mod k iff $k \mid a - b$
- basically a and b differ by some multiple of k
- $a \equiv b \pmod{k} \leftrightarrow b \equiv a \pmod{k}$

not an operator

aka $a \equiv_k b$

ex. prove for any integers a, b, c, d, k where $k > 0$, if $a \equiv b \pmod{k}$ and $c \equiv d \pmod{k}$, then $(a + c) \equiv (b + d) \pmod{k}$

intermediate step

Lemma: Let's first prove that linearity of divides holds under addition. For $a, b, k \in \mathbb{Z}$, if $k \mid a$ and $k \mid b$, then $k \mid (a + b)$

Lemma proof: Let $a, b, k \in \mathbb{Z}$ and suppose $k \mid a$ and $k \mid b$. Then by definition of divides, $a = kn$ and $b = km$ for some $m, n \in \mathbb{Z}$. Then $a + b = kn + km = k(n + m)$, $n, m \in \mathbb{Z}$, $n + m \in \mathbb{Z}$, by definition of divides, $k \mid (a + b)$

Proof: Let $a, b, c, d, k \in \mathbb{Z}$ where $k > 0$ such that $a \equiv b \pmod{k}$ and $c \equiv d \pmod{k}$. By congruency mod k definition, $k \mid (a - b)$ and $k \mid (c - d)$. Using our lemma, $k \mid ((a - b) + (c - d))$. This is equivalent to $k \mid ((a + c) - (b + d))$, so by definition, we know $(a + c) \equiv (b + d) \pmod{k}$

Discussion Problems 2.2ab 2.3 a 2.4a

2.2 Thinking about number theory

(a) Is there an integer x satisfying both congruences simultaneously? $x \equiv 7 \pmod 9$ $x \equiv 5 \pmod{12}$

(b) Is there an integer x satisfying both congruences simultaneously? $x \equiv 5 \pmod 6$ $x \equiv 3 \pmod{10}$

2.3 Thinking about gcd

Are the following claims true or false? Give a counter-example (if false) or an informal explanation (if true).

(a) For any positive integers p, q, and r, if $\gcd(p, q) = 1$ and $\gcd(q, r) = 1$, then $\gcd(p, r) = 1$.

2.4 Proof using the divides relation

Prove the following claims directly from the definition of "divides":

(a) The divides relation is transitive, i.e. for any integers a, b, and c, if $a \mid b$ and $b \mid c$, then $a \mid c$.

2.2 a) By the definition of modular congruence, $x \equiv 7 \pmod 9$ means $x = 7+9n$ where $n \in \mathbb{Z}$ and $x \equiv 5 \pmod{12}$ means $x = 5+12m$ where $m \in \mathbb{Z}$. Then $7+9n = 5+12m$, $2 = 12m - 9n$, $\frac{2}{3} = 4m - 3n$, which is invalid because $m, n \in \mathbb{Z}$. Therefore, there does not exist some integer x s.t $x \equiv 7 \pmod 9$ and $x \equiv 5 \pmod{12}$

2.2b) By the definition of modular congruence, $x \equiv 5 \pmod 6$ means $x = 5+6m$ where $m \in \mathbb{Z}$ and $x \equiv 3 \pmod{10}$ means $x = 3+10n$ where $n \in \mathbb{Z}$. Then $5+6m = 3+10n$, $2 = 10n - 6m$, $1 = 5n - 3m$. If we let $n = 2$ and $m = 3$, the equation is satisfied $(1 = 5(2) - 3(3) = 10 - 9 = 1)$. Then $x = 5+6(3) = 3+10(2) = 23$, which satisfies $x \equiv 5 \pmod 6$ and $x \equiv 3 \pmod{10}$.

2.3a) False, let $p=4$, $q=5$, $r=8$, $\gcd(4,5)=1$ and $\gcd(5,8)=1$, but $\gcd(4,8) = 4 \neq 1$

2.4a) Proof: Let $a, b, c \in \mathbb{Z}$, let $a \mid b$ and $b \mid c$. By the definition of divides, $b = an$ and $c = bm$, where $m, n \in \mathbb{Z}$. Then $c = (an)m = a(mn)$, $mn \in \mathbb{Z}$, let $mn = p$, $c = ap$, $p \in \mathbb{Z}$ which matches the definition of divides, proving $a \mid c$.