

Homework 11, Math 310, due November 19th, 2012

- (1) Let $d > 0$ be an integer. We have checked that if we define a relation on \mathbb{Z} by $a \sim b$ if d divides $a - b$ (remember this means $a - b = dk$ for some $k \in \mathbb{Z}$), then it is an equivalence relation. If you have not checked this before, check it now. One writes this relation as $a \equiv b \pmod{d}$, read as ‘ a is congruent to b modulo d ’ when d divides $a - b$.
- (a) Prove that the above equivalence relation has precisely d distinct equivalence classes.
 - (b) If $a \equiv b \pmod{d}$ and $a' \equiv b' \pmod{d}$, prove that $a + a' \equiv b + b' \pmod{d}$ and $aa' \equiv bb' \pmod{d}$.
 - (c) Prove that given $a \in \mathbb{Z}$, there exists a b such that $ab \equiv 1 \pmod{n}$ if and only if $\gcd(a, d) = 1$.
- (2) Let $d, e > 0$ be integers with $\gcd(d, e) = 1$. Prove that if $a \equiv b \pmod{d}$ and $a \equiv b \pmod{e}$, then $a \equiv b \pmod{de}$.
- (3) Let a_1, a_2, \dots, a_n be integers with at least one of them non-zero. Prove that there exists a (unique) positive integer d such that $d|a_i$ for all i and if $e|a_i$ for all i , then $e|d$. This d is denoted by $\gcd(a_1, a_2, \dots, a_n)$.
- (4) If $d = \gcd(a_1, \dots, a_n)$, prove that there exists integers b_i such that $\sum_{i=1}^n a_i b_i = d$.
- (5) Let a, b be two *non-zero* integers. A positive integer l is called the *lowest common multiple* of a, b (abbreviated $\text{lcm}(a, b)$) if $a|l, b|l$ and for any positive integer m , if $a|m, b|m$, then $l|m$. Let $d = \gcd(a, b)$ and write $a = dA, b = dB$ for integers A, B . Prove that dAB satisfies both the properties of lcm above and thus $\text{lcm}(a, b) = dAB$.