Greatest Common Divisor Investigations
Class Activity, Week 2

Divisibility of integers is one of the key concepts in number theory. Questions about primes and divisors were among the first questions considered about the properties of integers.

Recall how we defined the divisibility: A non-zero integer a *divides* an integer b if $b = ak$ for some integer k. The notation for a divides b is $a|b$.

Some straightforward properties of divisibility are listed below:
Theorem 1: (Properties of divisibility)

i. If $a \neq 0$, then $a|0$ and $a|a$.
ii. $1|b$ for every b (and $-1|b$).
iii. If $a|b$, then $a|bc$ for every c.
iv. If $a|b$ and $b|c$, then $a|c$.
v. If $a|b$ and $a|c$, then $a|(bx + cy)$.
vi. If $a|b$ and $b|a$, then $a = \pm b$.
vii. If $c \neq 0$, then $a|b$ if and only if $ac|bc$.

Note: For this course, a variable in lowercase Latin letters will represent an integer unless expressly stated to the contrary.

The Division Algorithm

Theorem 2: (The Division Algorithm) For any $b > 0$ and a, there exist unique integers q and r with $0 \leq r < b$ such that $a = bq + r$.

proof: We prove this statement in two parts. We first show that there are q and r which satisfy the requirements. Then we will show that there can be only one such q and only one such r.

Consider the set formed by $a - bk$'s where k is an integer and $a - bk \geq 0$. Let us refer to $a - bk$ as a "remainder" since this expression is what remains after we take away multiples of b from a. For example, $a = a - b \cdot 0$, $a - b = a - b \cdot 1$, $a + b = a - b \cdot (-1)$ (if they are non-negative) are all "remainders". If 0 is in this set, then $a = bk + 0$, which proves existence. If 0 is not in this set, then this set is a non-empty subset of natural numbers, and by the Well-ordering Principle there is a smallest remainder, say $a - bk_0$. This smallest remainder must satisfy $0 < a - bk_0 < b$. If $a - bk_0 > b$ (as in the first problem of the pre-class activity), then we can remove another b to obtain $a - bk_0 - b = a - b(k_0 + 1)$, which is a smaller remainder. But this contradicts the way we chose the smallest remainder.

To check that there can be only one such q and one such r, we use the standard technique of showing uniqueness: we assume there were two different q and two different r's, and conclude using algebra that each has to be unique. So suppose

$$a = bq + r = bq' + r' \quad \text{and} \quad 0 \leq r < b,\ 0 \leq r' < b$$

If $r = r'$, we are done. Because then by $bq + r = bq' + r'$, we find that $q = q'$ also.

Assume $r \neq r'$ and we will reach a contradiction. There are two cases: $r > r'$ or $r' > r$. There is no difference in how either case is handled, so we just pick one case, say $r > r'$. The other case will be similar. (This is what we mean when we use the phrase "without loss of generality".)

Using $bq + r = bq' + r'$, we find that $b(q' - q) = r - r' > 0$. Since $q' - q$ is an integer and $b > 0$, in order to have $b(q' - q) > 0$ we need $q' - q > 0$, which implies $b(q' - q) \geq b$. But $r - r' \leq r < b$ and we reach a contradiction. Hence $r \neq r'$ cannot be true, finishing the proof. $\square$

Greatest Common Divisor

Recall how we defined the greatest common divisor: The *greatest common divisor* (*gcd*) of two integers (not both 0) is the largest integer that divides them. By definition, greatest common divisor is a positive integer.

If $\gcd(a, b) = 1$, then a and b are said to be *relatively prime.* More generally, if given $a_1, \ldots, a_r$ we have $\gcd(a_i, a_j) = 1$ for $i \neq j$, then $a_1, \ldots, a_r$ are said to be *pairwise relatively prime.*

1. For $a \neq 0$, what is $\gcd(a, 0)$? What is $\gcd(a, 1)$?

2. Using your answers to the pre-class activity problems 2-5, think about how to complete the greatest common divisor properties below. No justification is needed (yet).

a. If $d|a$ and $d|b$, then ______________.

b. If $g = \gcd(a, b)$, then $\gcd(a/g, b/g) =$ _____.

c. $\gcd(ac, bc) =$________________.

d. If $d = \gcd(a, b)$, then _________________________ $ax + by$ for any x and y.

e. If $d = \gcd(a, b)$, then $\gcd(a, a - b) =$ _____.

In order to prove these properties and to efficiently calculate the greatest common divisor of any two numbers, we instead will use an alternative characterization of the greatest common divisor.

Theorem 3: (GCD as a linear combination) If a and b are not both zero and $d = \gcd(a, b)$, then d is the smallest element in the set of all positive integers of the form $ax + by$.

The expression $ax+by$ is called a linear combination of a and b with coefficients x and y, respectively.

proof: To prove this result, we consider the set A of all linear combinations of a and b which are positive. We can choose the coefficients to be a and b, respectively, so we can get $a^2 + b^2$ as a linear combination. Since this value is positive, the set A has at least one element and is non-empty. Hence, by the Well-ordering principle, there is a smallest element, say $e = ax_0 + by_0$, of A.

Our goal is to show that $e = d$. Note that since $d|a$ and $d|b$, then $d|e$, i.e. $d \leq e$. A standard way to prove two numbers are equal is to show that either one is less than or equal to the other. Since we already have $d \leq e$, we will now show $e \leq d$.

If we can show that e is a common divisor of both a and b (if the theorem is true, this should be the case since e is supposed to equal d), then we will have $e \leq d$. So we apply the Division Algorithm to a divided by e: $a = qe + r$ with $0 \leq r < e$. We want r to be 0. Consider:

$$r = a - qe = a - q(ax_0 + by_0) = a(1 - qx_0) + b(-y_0)$$

This last expression is a linear combination of a and b, and it is non-negative. If it is not 0, then it is an element in our set A and it is smaller than e, which is a contradiction. Therefore, $r = 0$.

In a similar way, we can show that the remainder of b divided by e is also 0. Hence e divides both a and b, and $e \leq d$.

Since $e \leq d$ and $d \leq e$, the two numbers should be equal, finishing the proof.

□

Corollary: $\gcd(a, b) = 1$ if and only if there exist integers x and y such that $ax + by = 1$.
Note that this result is labeled as a *corollary* because it is a direct consequence of the previous theorem.

Using the property of greatest common divisor as a linear combination, we can also prove the first of the greatest common divisor properties you were asked to guess above:

Corollary: If $d|a$ and $d|b$, then $d| \gcd(a, b)$.
proof:

□

Another way to characterize the greatest common divisor is as follows:
Theorem 4: (GCD as the divisor that every divisor divides) $d = \gcd(a, b)$ if and only if $d > 0$, $d|a$, $d|b$ and for every common divisor f of a and b, $f|d$. (Proof omitted.)

We now focus on some prime number properties using the greatest common divisor as a tool. Recall how we defined a prime number: A *prime number* is a natural number that has no natural number divisors besides 1 and itself.

A very nice property of the prime numbers is that if a prime number p divides bc, then p divides b or p divides c (this is an inclusive 'or', meaning p is allowed to divide both numbers). This property is referred to as the *Euclid's Lemma.* Although this property can be proved using the prime factorization decomposition (which is in fact a deep result), we will show a more general result using the linear combination expression of the greatest common divisor.

Theorem 5: If $a|bc$ and $\gcd(a, b) = 1$, then $a|c$.

proof: We assume that $a|bc$ and $\gcd(a, b) = 1$ and will show that $a|c$.

Since $\gcd(a, b) = 1$, using the GCD as a linear combination result we have that ________________ ____. Therefore $c =$ ________________. We know that $a|bc$ by our assumption, so ________________________ by Divisibility property (v). Therefore ________________________. □

Corollary: (Euclid's Lemma) If p divides bc, then $p|b$ or $p|c$.

proof: Assume $p|bc$. We need to show $p|b$ or $p|c$.

If $p|b$, then we're done. Suppose $p \nmid b$. Then $\gcd(p, b) = 1$. Therefore, by the theorem above, $p|c$.

□

This result can be generalized using induction:
Corollary: If p divides $b_1 b_2 \cdots b_n$, then $p|b_i$ for some i.

proof: We will prove this result using induction.

Basis case:

Inductive step: Assume the statement is true for $n = k$, i.e. "if p divides $b_1 b_2 \cdots b_k$, then $p|b_i$ for some i." We want to show the statement is true for __________, i.e. ____________________ ____.

To show the 'if statement' we want to show, assume the hypothesis of the 'if statement', i.e. ____. We need to prove the conclusion, i.e. ____. Rewrite $b_1 b_2 \cdots b_{k+1} = (b_1 b_2 \cdots b_k) \cdot b_{k+1}$. So we have $p|b_1 b_2 \cdots b_{k+1} = (b_1 b_2 \cdots b_k) \cdot b_{k+1}$. Using the previous corollary, we therefore have ____. If $p|b_{k+1}$, then the conclusion is shown to be true. If $p|b_1 b_2 \cdots b_k$, then using the inductive hypothesis we know ____. Hence, again, the conclusion is true. This proves the inductive hypothesis.

Hence

□

Another corollary of Theorem 5 is as follows:
Corollary: If $a|c$, $b|c$ and $\gcd(a, b) = 1$, then $ab|c$.
Proof of this corollary is left to the reader as an exercise.

Let us wrap up the properties of greatest common divisor.
Theorem 6: (Properties of greatest common divisor)

i. If $g = \gcd(a, b)$, then $\gcd(a/g, b/g) = 1$.
ii. $\gcd(ac, bc) = c \gcd(a, b)$.
iii. If $d = \gcd(a, b)$, then d divides $ax + by$ for any x and y.
iv. $\gcd(a, b)$ is the smallest element in the set of all positive integers of the form $ax + by$.
v. $\gcd(a, b) = 1$ if and only if there exist integers x and y such that $ax + by = 1$.
vi. If $d|a$ and $d|b$, then $d| \gcd(a, b)$.
vii. $\gcd(a, b) = \gcd(a, a - bk)$ for any k.

Recall how we defined the least common multiple: The *least common multiple* (*lcm*) of two integers (not both 0) is the smallest integer that is a multiple of both a and b.

The least common multiple satisfies the following properties.
Theorem 7: (Properties of least common multiple)

i. $\mathrm{lcm}(ac, bc) = c \cdot \mathrm{lcm}(a, b)$.
ii. $\gcd(a, b) = 1$ if and only if $\mathrm{lcm}(a, b) = ab$.
iii. $\gcd(a, b) \cdot \mathrm{lcm}(a, b) = ab$.
iv. $m = \mathrm{lcm}(a, b)$ if and only if $m > 0$, $a|m$, $b|m$, and for every common multiple n of a and b, $m|n$.