7-15-2002

Greatest Common Divisors

- The **greatest common divisor** (m, n) of integer m and n is the largest integer which divides both m and n.
- The greatest common divisor can be found using the **Euclidean algorithm**, which is a process of repeated division.
- The greatest common divisor (m, n) of m and n is a **linear combination** of m and n.
- m and n are **relatively prime** if $(m, n) = 1$.

Definition. The **greatest common divisor** of two integers (not both zero) is the largest integer which divides both of them.

If a and b are integers (not both 0), the greatest common divisor of a and b is denoted (a, b).

(In Britain, the greatest common divisor is often called the **highest common factor**.)

Examples. $(4, 6) = 2$, $(17, 17) = 17$, $(42, 0) = 42$, $(12, -15) = 3$. □

Properties of the greatest common divisor Once and for all, in discussions of the greatest common divisor all the variables will denote integers, and it's understood that in (a, b) at least one of a and b is nonzero.

1. $(a, b) \geq 1$.

   Since $1 \mid a$ and $1 \mid b$, (a, b) must be at least as big as 1. □

2. $(a, b) = (|a|, |b|)$.

   $x \mid a$ if and only if $x \mid -a$; that is, a and $-a$ have the same factors. But $|a|$ is either a or $-a$, so a and $|a|$ have the same factors. Likewise, b and $|b|$ have the same factors. Therefore, x is a common factor of a and b if and only if it's a common factor of $|a|$ and $|b|$. Hence, $(a, b) = (|a|, |b|)$. □

Definition. a and b are **relatively prime** if $(a, b) = 1$.

For example, 49 and 54 are relatively prime, but 25 and 105 are not.

Proposition. If $d = (m, n)$, then $\left(\frac{m}{d}, \frac{n}{d}\right) = 1$.

Proof. Suppose $m = da$ and $n = db$. Then

$$\left(\frac{m}{d}, \frac{n}{d}\right) = (a, b).$$

Suppose that $p > 0$ and $p \mid a$, $p \mid b$. Then I can find e and f such that

$$a = pe \quad \text{and} \quad b = pf.$$

Thus,

$$m = dpe \quad \text{and} \quad n = dpf.$$

This shows that dp is a common factor of m and n. Since d is the *greatest* common factor, $d \geq dp$. Therefore, $1 \geq p$, so $p = 1$ (since p was a positive integer).

I've proven that 1 is the *only* positive common factor of a and b. Therefore, 1 is the greatest common factor of a and b:

$$\left(\frac{m}{d}, \frac{n}{d}\right) = (a, b) = 1. \quad \square$$

Properties of the greatest common divisor (continued)

3. $(m, n) = (m + kn, n)$ for any integer k.

   First, if x is a common factor of m and n, then $x \mid m$ and $x \mid n$. So $x \mid kn$, and hence $x \mid m + kn$. Thus, x is a common factor of $m + kn$ and n.
   Conversely, if x is a common factor of $m+kn$ and n, then $x \mid (m+kn)$ and $x \mid n$. Therefore, $x \mid kn$, so $x \mid [(m + kn) - kn] = m$. That is, x is a common factor of m and n.
   Since m, n and $m+kn$, n have the same set of common divisors, the two pairs must have the same greatest common divisor. $\square$

The last property says that I don't change the greatest common divisor if I add or subtract multiples of one member of the pair from the other. This yields the following **recursive procedure** for computing the greatest common divisor.

Euclidean Algorithm. Begin with a pair of nonnegative integers $\{m, n\}$, not both 0. (The absolute value property I stated earlier shows that there's no harm in assuming the integers are nonnegative.)

1. If one of the numbers is 0, the other is the greatest common divisor of the pair. (Stop.)
2. Otherwise, apply the Division Algorithm to write $m = qn + r$, where $0 \leq r < n$.
3. Replace the pair $\{m, n\}$ with the pair $\{n, r\}$.
4. Go to step 1.

At each step, both elements are ≥ 0, and each pass through step 3 decreases the second element. Since the second element always gets smaller, but can't be negative, Well-Ordering implies that algorithm must terminate in an $\{m, 0\}$ pair (in step 2) after a finite number of steps.

The preceding property shows that these steps produce new pairs of numbers *with the same greatest common divisor as the previous pairs*. Therefore, when the algorithm terminates, the greatest common divisor I've found is the greatest common divisor of the original pair.

Example. Use the Euclidean algorithm to compute $(124, 348)$.

Write the pair as $\{348, 124\}$.

Equation	Pair of numbers
$346 = 2 \cdot 124 + 100$	$\{124, 100\}$
$124 = 1 \cdot 100 + 24$	$\{100, 24\}$
$100 = 4 \cdot 24 + 4$	$\{24, 4\}$
$24 = 6 \cdot 4 + 0$	$\{4, 0\}$

At this point, one of the numbers is 0, so the greatest common divisor is the other number: $(348, 124) = 4$.
$\square$

Example. You can also form the greatest common divisor of more than two numbers, in the obvious way. For instance, $(42, 105, 91) = 7$. $\square$

Definition. If x and y are numbers, a **linear combination** of x and y (with integer coefficients) is a number of the form

$$ax + by, \quad \text{where} \quad a, b \in \mathbb{Z}.$$

Example. $29 = 2 \cdot 10 + 1 \cdot 9$ shows that 29 is a linear combination of 10 and 9. $7 = (-2) \cdot 10 + 3 \cdot 9$ shows that 7 is a linear combination of 10 and 9 as well.

The next result is extremely important, and is often used in proving things about greatest common divisors.

Theorem. (m, n) is the smallest positive linear combination of m and n. In particular, there are integers a and b (not necessarily unique) such that

$$(m, n) = am + bn.$$

Example. I showed above that $(348, 124) = 4$. The theorem says that there are integers a and b such that

$$4 = a \cdot 348 + b \cdot 124.$$

In fact,

$$4 = 5 \cdot 348 + (-14) \cdot 124.$$

This combination is not unique. For example,

$$4 = 129 \cdot 348 + (-362) \cdot 124. \quad \square$$

I'll give a few easy corollaries before proving the theorem.

Corollary. If $d \mid m$ and $d \mid n$, then $d \mid (m, n)$.

Proof.

$$(m, n) = am + bn \quad \text{for some} \quad a, b \in \mathbb{Z}.$$

Therefore, $d \mid m$ and $d \mid n$, then $d \mid (am + bn = (m, n)$. $\square$

This says that the greatest common divisor is not only "greatest" in terms of *size*; it's also "greatest" in the sense that any other common factor must *divide* it.

Corollary. m and n are relatively prime if and only if

$$am + bn = 1 \quad \text{for some} \quad a, b \in \mathbb{Z}.$$

Proof. ($\Rightarrow$) Suppose m and n are relatively prime. Then $(m, n) = 1$. By the theorem,

$$(m, n) = am + bn \quad \text{for some} \quad a, b \in \mathbb{Z}.$$

Therefore,

$$am + bn = 1 \quad \text{for some} \quad a, b \in \mathbb{Z}.$$

($\Leftarrow$) Suppose

$$am + bn = 1 \quad \text{for some} \quad a, b \in \mathbb{Z}.$$

This says that 1 is a positive linear combination of m and n, so (since 1 is the smallest positive integer) it's the *smallest* positive linear combination of m and n. By the theorem, this implies that 1 is the greatest common divisor, and m and n are relatively prime. □

Proof of the theorem. I'll use the Euclidean algorithm.

The initial pair $\{m, n\}$ consists of two numbers m and n. Each of these numbers is a linear combination of m and n.

The only changes the algorithm makes are to switch the elements or to subtract a multiple of one element from the other. I have to show that neither changes the fact that the two elements are linear combinations of m and n.

If two elements are each linear combinations of m and n, this obviously remains true if I the swap the elements.

For subtracting a multiple, suppose I have the pair $\{x, y\} = \{am + bn, cm + dn\}$. I divide x by y:

$$x = qy + r, \quad \text{where} \quad 0 \leq r < y.$$

The new pair is

$$\{y, r\} = \{y, x - qy\} = \{cm + dn, (am + bn) - q(cm + dn)\} = \{cm + dn, (a - qc)m + (b - qd)n\}.$$

Each element of this new pair is a linear combination of m and n.

I know the algorithm terminates in $\{(m, n), 0\}$. It follows that (m, n) must be a linear combination of m and n.

Now suppose p is a positive linear combination of m and n:

$$p = am + bn \quad \text{for some} \quad a, b \in \mathbb{Z}.$$

$(m, n) \mid m$ and $(m, n) \mid n$, so $(m, n) \mid p$. Both of these numbers are positive, so $(m, n) \leq p$. Since (m, n) is smaller than any positive linear combination of m and n, (m, n) must be the *smallest* positive linear combination of m and n. □

Example. $(42, 105) = 21$, so the theorem asserts that the set of all linear combinations of 42 and 105 — that is, the set of all numbers of the form $42a + 105b$ — is

$$\ldots, -42, -21, 0, 21, 42, 63, \ldots.$$

Notice that the greatest common divisor is the smallest positive element of this set.

If you know a little group theory, you may recognize this as the result that *subgroups of cyclic groups are cyclic.* □
