Summer High School 2009

Aaron Bertram

4. Greatest Common Divisors.

Definition 4.1. The *greatest common divisor (GCD)* of m and n is the largest natural number d such that $d|m$ and $d|n$.

Definition 4.2. m and n are *relatively prime* if their GCD is 1.

Observation. A prime p is relatively prime to every $m < p$.

Notation: GCD(m, n) will stand for the greatest common divisor.

Question 4.1. Can we determine GCD(m, n) quickly?

In contrast with Refined Question 1.4(b), the answer here is "Yes!"

Euclid's Algorithm: Given natural numbers m and n, with $m \leq n$ (otherwise switch them). Find the remainder when n is divided by m:

$$n \quad = \quad qm \quad + \quad r$$

If $r = 0$, STOP and ouput the number m.
Otherwise, replace $n := m$ and $m := r$ and REPEAT.
(Since each m is smaller than the previous, this will always stop.)

Example: Apply Euclid's algorithm to $m = 1001$ and $n = 3535$.

$$\begin{array}{rcccc} 3535 & = & 3(1001) & + & 532 \\ 1001 & = & 1(532) & + & 469 \\ 532 & = & 1(469) & + & 63 \\ 469 & = & 7(63) & + & 28 \\ 63 & = & 2(28) & + & 7 \\ 28 & = & 4(7) & + & 0 \end{array}$$

STOP. The output is 7.

Assertion 1. The output divides both m and n.

Proof: There are many m's and n's in Euclid's algorithm, since the assignment of m and n is adjusted each time the algorithm is repeated. The output of Euclid's algorithm divides *all of them*. That's because it divides the *last* m (which is itself!) and the *last* n (since the remainder was zero). And if it divides m and n at one step, then it divided r and m at the previous step. So must have divided n, since

$$n = qm + r$$

at that step, too. Now work your way all the way up. □

Example: In the example above, 7 divides 7 and 28 (last step), so:

7 divides 63, 7 divides 469, 7 divides 532, etc.

Definition 4.2. An integer d is a *linear combination* of m and n if there are integers a and b (usually one of them is negative) such that:

$$am + bn = d$$

(Notice that this is the same thing as saying that $am \equiv d \mod n$).

Assertion 2. The output is a linear combination of m and n.

Proof: The output of Euclid's algorithm is the remainder in the next-to-the last step. As in the previous assertion, it is easier to see that *every* n', m' and r' appearing in *every* step of Euclid's algorithm is a linear combination of m and n. This is true at the first step, since:

$$(0)m + (1)n = n, \quad (1)m + (0)n = m \text{ and } (-q)m + (1)n = r$$

Suppose it is true at one step. That is, suppose:

$$a_1m + b_1n = n', \quad a_2m + b_2n = m', \text{ and } a_3m + b_3n = r'$$

(we need "primes" on m, n, r to distinguish them from the originals) Then the n'', m'' and r'' of the next step are given by:

$$n'' := m', m'' := r' \text{ and } r'' = n'' + (-q'')m''$$

so n'' and m'' are linear combinations of m, n from the previous step. What about r''? Well, this is exactly the situation that matrices are designed for. If we represent the linear combinations giving m'' and n'' as the columns of a 2×2 matrix and multiply, we get:

$$\begin{pmatrix} a_2 & a_3 \\ b_2 & b_3 \end{pmatrix} \begin{pmatrix} 1 \\ -q'' \end{pmatrix} = \begin{pmatrix} a_2 + a_3(-q'') \\ b_2 + b_3(-q'') \end{pmatrix}$$

which is the column vector for the desired set of coefficients:

$$(a_2 + a_3(-q''))m + (b_2 + b_3(-q''))n = r'$$

Thus we can keep going. □

Example: In the example above, the column vectors are (in order):

$$\begin{pmatrix} 0 \\ 1 \end{pmatrix}, \begin{pmatrix} 1 \\ 0 \end{pmatrix}, \begin{pmatrix} -3 \\ 1 \end{pmatrix}, \begin{pmatrix} 4 \\ -1 \end{pmatrix}, \begin{pmatrix} -7 \\ 2 \end{pmatrix}, \begin{pmatrix} 53 \\ -15 \end{pmatrix}, \begin{pmatrix} -113 \\ 32 \end{pmatrix}$$

and so, finally, $(-113)(1001) + (32)(3535) = 7$.

Notice how easy this is to implement in practice!

These simple assertions are remarkably important. Here are the first few corollaries that we can draw from them:

Corollary 1: Every common divisor of m and n divides the output. In particular, the output of Euclid's algorithm is the GCD, and every common divisor of m and n also divides their GCD.

Proof: If d divides m and n, then d divides any linear combination of m and n. Since the output is a linear combination, it follows that all common divisors divide the output. And of course all divisors are smaller than the number they divide, so the output is the GCD. □

Corollary 2: If $\mathrm{GCD}(m, n) = 1$, then m has a reciprocal mod n. If p is prime then each number not divisible by p has a reciprocal mod p.

Proof: If $\mathrm{GCD}(m, n) = 1$, then Assertion 2 gives:

$$am + bn = 1 \text{ for some integers } a, b$$

which is exactly what we require for reciprocals. And primes are relatively prime to every number that they don't divide. □

Corollary 3: Suppose p is a prime and $p|(mn)$. Then $p|m$ or $p|n$.

Proof: Suppose p doesn't divide m. Then $\mathrm{GCD}(p, m) = 1$, so:

$$ap + bm = 1 \text{ for some integers } a \text{ and } b$$

Now multiply this entire equation by n. This gives:

$$(an)p + b(mn) = n$$

so that n is a linear combination of p and mn. Since p divides both of these (by assumption), it must divide n as well! In other words, p must divide one or the other (or both) of m and n. □

Corollary 4 (Fundamental Theorem of Arithmetic (Part II)): In Part I, we saw that every natural number n is a product of primes. This part shows that there is **only one way** to do this.

Proof: Suppose $n = p_1 p_2 \cdots p_k$ is one way to write n as a product of primes, and q is another prime that divides n. Then $q|p_1(p_2 \cdots p_k)$, so by Corollary 4.5, $q|p_1$ or $q|p_2 \cdots p_k$. If $q|p_1$, then $q = p_1$ because they are both primes. But if p divides the product of the others, then the same argument shows that p must be one of the others. Thus q is one of the p_i. It follows that if $n = q_1 q_2 \cdots q_l$ is another way to write n as a product of primes, then $k = l$ and the p's and q's are the same. □

Remark: Factoring large numbers is hard (even for a computer)! Thus, for example, we could have factored:

$$1001 = 3 \cdot 7 \cdot 11 \text{ and } 3535 = 5 \cdot 7 \cdot 101$$

and concluded that 7 was the GCD, this is actually a lot harder to do than implementing Euclid's algorithm! If you don't believe me, choose two very large numbers (say, 40 digits) at random. It is easy to get a computer to run Euclid's algorithm, but factoring them takes forever.

Definition 4.3: The *Euler phi function* is defined by:

$$\phi(n) = \# \{\text{numbers from 1 to } n-1 \text{ that are relatively prime to } n\}$$

Examples:

$\phi(p) = p - 1$ if p is a prime (everything is relatively prime to p).

$\phi(4) = 2$ (only 1 and 3 are relatively prime to 4).

$\phi(6) = 2$ (only 1 and 5 are relatively prime to 6).

$\phi(8) = 4$ ($1, 3, 5$ and 7 are relatively prime to 8).

$\phi(9) = 6$ ($1, 2, 4, 5, 7, 8$ are relatively prime to 9).

$\phi(10) = 4$ (only $1, 3, 7$ and 9 are relatively prime to 10).

Two important features of the phi function make it easy to calculate:

Prime Powers: Suppose p^k is a prime power. Then the numbers from 1 to $p^k - 1$ that are relatively prime to p^k are exactly the numbers that are not divisible by p. These are $p - 1$ out of every p numbers:

$1, 2, \cdots, p-1$ from the first p numbers,

$p+1, p+2, \cdots, 2p-1$ from the next p numbers,

$2p+1, 2p+2, \cdots 3p-1$ from the next, all the way up to p^k. So:

$$\phi(p^k) = \left(\frac{p-1}{p}\right) p^k = p^k - p^{k-1}$$

That was easy. The next feature is much more surprising:

Relatively Prime Products: Suppose m and n are relatively prime. Then:

$$\phi(mn) = \phi(m)\phi(n)$$

(and this is definitely NOT true if m and n are not relatively prime!)

We will see why this is true later. But first notice that these features allow us to calculate the phi function of n *provided we can factor* n (but unlike Euclid's algorithm for GCD's, there is no shortcut here!).

Examples:

$91 = 7 \cdot 13$ so $\phi(91) = \phi(7) \cdot \phi(13) = 6 \cdot 12 = 72$.

$162 = 2 \cdot 3^4$ so $\phi(162) = \phi(2) \cdot \phi(3^4) = 1 \cdot (3^4 - 3^3) = 54$.

$144 = 2^4 \cdot 3^2$ so $\phi(144) = \phi(2^4) \cdot \phi(3^2) = (2^4 - 2^3)(3^2 - 3) = 48$.