M7210 Lecture 1 August 20, 2012

The Remainder Theorem. *Suppose a and b are integers with $b \neq 0$. Then, there are unique integers q and r such that:*

$$a = q\,b + r \quad \text{and} \quad 0 \leq r < |b|. \tag{$*$}$$

Proof of existence. Let $q\,b$ be the largest element of the set $\{\, p\,b \mid p\,b \leq a\,,\ p \in \mathbb{Z} \,\}$. Then

$$q\,b \leq a \quad \text{so} \quad 0 \leq a - q\,b,$$
$$q\,b + |b| > a \quad \text{so} \quad a - q\,b < |b|.$$

Thus, q and $r := a - q\,b$ satisfy $(*)$.

Proof of uniqueness. Suppose q' and r' also satisfy $(*)$. Then $q\,b + r = q'\,b + r'$, so $(q - q')\,b = r - r'$. Since the inequality in $(*)$ applies to both r and r', $-b < r - r' < b$. The only multiple of b in $(-|b|, |b|)$ is 0, so $q = q'$, and it follows that $r = r'$. /////

The Euclidean Algorithm. Given integers a and $b \neq 0$ and the corresponding q and r supplied by the Remainder Theorem, we make the following new notation:

$$r_{-1} := a\,,\ r_0 := |b|\,,\ q_1 := q\,b/|b|\,,\ r_1 := r.$$

Then line $(*)$ reads:

$$r_{-1} = q_1 r_0 + r_1 \quad \text{and} \quad 0 \leq r_1 < r_0. \tag{1}$$

If r_1 is not zero, the Remainder Theorem gives us unique q_2 and r_2 such that:

$$r_0 = q_2\,r_1 + r_2 \quad \text{and} \quad 0 \leq r_2 < r_1. \tag{2}$$

SImilarly, if r_2 is not zero, then there are unique q_3 and r_3 such that:

$$r_1 = q_3\,r_2 + r_3 \quad \text{and} \quad 0 \leq r_3 < r_2. \tag{3}$$

If r_3 is still non-zero, we may continue. The process leads to a strictly decreasing sequence. Let r_n be the last non-zero element. Then we have: $r_0 > r_1 > \cdots > r_n > r_{n+1} = 0$.

Euclidean Algorithm in Matrix Form. For $i = 1, 2, \ldots, n$,

$$r_{i+1} = r_{i-1} - q_{i+1}\,r_i.$$

Each r_j depends on the two previous elements in the sequence. Using matrix notation, we can carry forward all the data needed for each step:

$$\begin{pmatrix} r_i \\ r_{i+1} \end{pmatrix} = \begin{pmatrix} 0 & 1 \\ 1 & -q_{i+1} \end{pmatrix} \begin{pmatrix} r_{i-1} \\ r_i \end{pmatrix}.$$

Using this repeatedly, we find:

$$\begin{pmatrix} r_n \\ 0 \end{pmatrix} = \begin{pmatrix} 0 & 1 \\ 1 & -q_{n+1} \end{pmatrix} \cdots \begin{pmatrix} 0 & 1 \\ 1 & -q_1 \end{pmatrix} \begin{pmatrix} r_{-1} \\ r_0 \end{pmatrix}. \tag{4}$$

Notice that

$$\begin{pmatrix} q & 1 \\ 1 & 0 \end{pmatrix} \begin{pmatrix} 0 & 1 \\ 1 & -q \end{pmatrix} = \begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix},$$

so by repeatedly multiplying (4) on the left, we get:

$$\begin{pmatrix} q_1 & 1 \\ 1 & 0 \end{pmatrix} \cdots \begin{pmatrix} q_{n+1} & 1 \\ 1 & 0 \end{pmatrix} \begin{pmatrix} r_n \\ 0 \end{pmatrix} = \begin{pmatrix} r_{-1} \\ r_0 \end{pmatrix}. \tag{5}$$

Matrix equation (4) above shows:

Lemma 1. *There are integers x and y with the property that*

$$x\,r_{-1} + y\,r_0 = r_n. \qquad /////$$

Example. Let us find integers x and y so that $x\,1441 + y\,1346 = 1$. We carry out the Euclidean Algorithm:

$$\begin{array}{rcllll} 1441 & = & 1\cdot 1346 & + & 95 & (1) \\ 1346 & = & 14\cdot 95 & + & 16 & (2) \\ 95 & = & 5\cdot 16 & + & 15 & (3) \\ 16 & = & 1\cdot 15 & + & 1 & (4) \\ 15 & = & 15\cdot 1 & + & 0 & (5). \end{array}$$

We have $n = 4$ and $q_1 = 1$, $q_2 = 14$, $q_3 = 5$, $q_4 = 1$, $q_5 = 15$. Using Equation (4):

$$\begin{aligned} \begin{pmatrix} 1 \\ 0 \end{pmatrix} &= \begin{pmatrix} 0 & 1 \\ 1 & -15 \end{pmatrix}\begin{pmatrix} 0 & 1 \\ 1 & -1 \end{pmatrix}\begin{pmatrix} 0 & 1 \\ 1 & -5 \end{pmatrix}\begin{pmatrix} 0 & 1 \\ 1 & -14 \end{pmatrix}\begin{pmatrix} 0 & 1 \\ 1 & -1 \end{pmatrix}\begin{pmatrix} 1441 \\ 1346 \end{pmatrix} \\ &= \begin{pmatrix} -85 & 91 \\ 1346 & -1441 \end{pmatrix}\begin{pmatrix} 1441 \\ 1346 \end{pmatrix}. \end{aligned}$$

We conclude, $1 = (-85)(1441) + (91)(1346)$. /////

Matrix equation (5) shows:

Lemma 2. *There are integers u and v such that*

$$u\,r_n = r_{-1} \quad \textit{and} \quad v\,r_n = r_0. \qquad /////$$

Definition. Suppose $a, b \in \mathbb{Z}$.

- We say *a divides b*—in symbols, $a|b$—to mean: there is $k \in \mathbb{Z}$ such that $k\,a = b$.
- We say *d is a common divisor of a and b* if $d|a$ and $d|b$.
- The *greatest common divisor of a and b*—denoted $\gcd(a, b)$—is the largest integer in the set of common divisors of a and b.

Exercise 1. *Suppose $a, b, d, x, y \in \mathbb{Z}$. If $d|a$ and $d|b$, then $d|(x\,a + y\,b)$.*

As a special case, we see that in equation $(*)$, if $d|a$ and $d|b$, then $d|r$.

Lemma 3. $r_n = \gcd(r_{-1}, r_0)$.

Proof. By Lemma 2, r_n is a common divisor of r_{-1} and r_0. Suppose c is a common divisor of common divisor of r_{-1} and r_0. Then, by Lemma 1 and Exercise 1, $c|r_n$. Since $0 < r_n$, $c \le r_n$. So, r_n is the largest element in the set of common divisors. /////

We may summarize our results up to this point by the following:

Theorem. *For any integers a and b, there are integers x and y such that*

$$\gcd(a, b) = x\,a + y\,b. \qquad /////$$

Corollary 1. *Suppose $c, m, n \in \mathbb{Z}$. If $c|mn$ and $\gcd(c, m) = 1$, then $c|n$.*

Proof. Select $k \in \mathbb{Z}$ such that $m\,n = c\,k$ and $x, y \in \mathbb{Z}$ such that $1 = c\,x + m\,y$. Multiply the latter by n to get $n = c\,n\,x + m\,n\,y = c\,n\,x + c\,k\,y = c\,(n\,x + k\,y)$. /////

Corollary 2. *Suppose $a, b, m \in \mathbb{Z}$. If $\gcd(a, b) = 1$, $a|m$ and $b|m$, then $ab|m$.*

Proof. Select $x, y \in \mathbb{Z}$ such that $1 = a\,x + b\,y$. Multiply by m to get $m = m\,a\,x + m\,b\,y = b\,(m/b)\,a\,x + a\,(m/a)\,b\,y$. Thus, $m = a\,b\,\big((m/b)\,x + (m/a)\,y\big)$. /////

Unique Factorization in $\mathbb{Z}$

An integer p is called *prime* if p is neither 1 nor -1 and $p = a\,b$ for some $a, b \in \mathbb{Z}$ implies either a or b is 1 or -1.

Lemma 4. *If p is prime and $p|a\,b$, then $p|a$ or $p|b$.*

Proof. Suppose p does not divide a. Then $\gcd(a, p) = 1$. Now apply Corollary 2. /////

Lemma 5. *For all integers k other than 0, 1 and -1:*

$$\text{\textit{either k is prime or k is a product of (finitely many) primes.}} \qquad (\dagger_k)$$

Proof. It is enough to prove $(\dagger_k)$ for positive integers, since if p is prime, so is $-p$. We use induction, starting at 2:

(1) $(\dagger_2)$ is obviously true.
(2) Fix any integer $\ell > 2$, and assume the induction hypothesis: $(\dagger_k)$ holds when $2 \le k < \ell$. We must show $(\dagger_\ell)$. If ℓ is prime, then $(\dagger_\ell)$. If ℓ is not prime, $\ell = a\,b$ with $2 \le a < \ell$ and $2 \le b < \ell$. By the induction hypothesis, both a and b are either prime or products of primes. Therefore $a\,b$ has the same property. Thus, $(\dagger_\ell)$. /////

Lemma 6. *Suppose p_i, $i = 1, \ldots, m$ and q_j, $j = 1, \ldots, n$ are positive prime integers. If $\prod_{i=1}^{m} p_i = \prod_{j=1}^{n} q_j$, then $m = n$ and after renumbering, $p_i = q_i$ for $i = 1, \ldots, m$.*

Proof. Assume without loss of generality that $m \le n$; we will prove the lemma by induction on n, the $n = 1$ case being obvious. By Lemma 4, $q_n|p_i$ for some i. Renumbering, we may assume $i = m$. Thus, $p_m = kq_n$. Since p_m is prime, $k = 1$, so $q_n = p_m$. Now, cancel q_n and p_m from both sides. The remaining products have fewer factors, and hence by the inductive hypothesis, after renumbering, $p_i = q_i$ for $i = 1, \ldots, n - 1$. /////

Theorem. *Every integer > 1 factors uniquely as a product of positive primes.* /////

Homework. 1) Find the greatest common divisor of 933162 and 1051569 and express it in the form $933162\,x + 1051569\,y$, with $x, y \in \mathbb{Z}$. 2) Do Exercise 1 (page 2 of these notes). 3) In textbook, page 30, #4.

Extra. Various versions of following "urban legend" appear at several web sites:

> While a student at Cambridge, Paul Dirac—the father of relativistic quantum theory and the discoverer of the positron—heard the following problem:
>
> > After a big days catch, three fisherman go to sleep next to their pile of fish. During the night, one fisherman decides to go home. He divides the fish in three and finds that this leaves one extra fish. He throws this into the water, takes one third of the remaining fish, and departs. The second fisherman awakes. Not knowing that the first has left, he too divides the fish into three piles, finds one fish left over, discards it, and takes a third of the remainder. The third fisherman does the same. If the number of fish caught was not more than 40, what was it?
>
> Dirac proposed that they had begun with -2 fish. The first fisherman threw one into the water, leaving -3, and took a third of this, leaving -2. The second and third fisherman did the same.

a) What are the other solutions?

b) How would this generalize if there were n fishermen rather than 3?

c) Suppose (in addition) that the fishermen left in groups of size m. Then ...?

d) Suppose (in addition) that they always threw b fish back, rather than just 1. Then ...?