Mathematics 4300 – Foundations of Algebra – Fall 1999

7. The Fundamental Theorem of Arithmetic. We use our new proof tools to prove some more sophisticated properties of the natural numbers, including unique factorization (the fundamental theorem of arithmetic).

Proof of Division with Remainders: Recall the set-up. We are given natural numbers m and n with $m \leq n$. We want to prove that:

$n = mq + r$ for q a natural number and $0 \leq r < m$.

Consider the sentence $P(n)$:

"Given n, then $n = mq + r$ as above for every $m \leq n$"

Notice that by phrasing it this way, we do not have to assign m a particular value to make $P(n)$ into a statement, even though both m and n appear in the sentence. Thus we are in a position to fashion a:

Proof by Induction:

(a) $P(1)$. If $n = 1$, then $m = 1$ also and $1 = 1 \cdot 1 + 0$. So $q = 1$ and $r = 0$.

(b) Assume $P(n)$, so that $n = mq + r$ for every $m \leq n$.

Case 1. $n = mq + r$ and $r < m - 1$. Then

$$n + 1 = m \cdot q + (r + 1)$$

that is, we increase the remainder by 1.

Case 2. $n = mq + r$ and $r = m - 1$. Then

$$n + 1 = m \cdot q + m = m(q + 1) + 0$$

that is, we increase the quotient by 1 and set the remainder to 0.

This leaves one extra case because we haven't considered the possibility:

Case 3. $m = n + 1$. Then $n + 1 = (n + 1) \cdot 1 + 0$

Taken together, we have $P(n + 1)$, completing the proof by induction.

Next, I want to discuss:

Euclid's Algorithm: Starting with $m \leq n$, we repeatedly apply division with remainders in the following pattern:

$$n = mq_1 + r_1$$

$$m = r_1 q_2 + r_2$$

$$r_1 = r_2 q_3 + r_3$$

$$\vdots$$

$$r_{i-2} = r_{i-1} q_i + r_i$$

stopping only when we get a zero remainder.

Claim: Euclid's algorithm always stops.

Proof: Consider the set of nonzero remainders:

$$\{r_1, r_2, r_3, ...\}$$

Since we are using the r_{i-1} in place of m to construct r_i we know that $r_1 > r_2 > r_3 > ....$ In other words, this is a decreasing sequence. But by the smallest element axiom every set of natural numbers has a smallest element. We let r_k be the smallest. Then r_{k+1} **cannot be a natural number**, telling us that $r_{k+1} = 0$, and the algorithm stops there.

Example: $n = 1175, m = 395$.

$$1175 = 395 \cdot 2 + 385$$

$$395 = 385 \cdot 1 + 10$$

$$385 = 10 \cdot 38 + 5$$

$$10 = 5 \cdot 2 + 0$$

so the sequence of natural number remainders is $\{385, 10, 5\}$.

Definition: The **greatest common divisor** of m and n (written $\gcd(m, n)$) is the largest natural number d with the property that:

$$d|m \quad \text{and} \quad d|n.$$

Proposition 1: The last nonzero remainder in Euclid's algorithm is the greatest common divisor of m and n.

Proof: Let r_k be the last nonzero remainder in Euclid's algorithm. Then the last line of Euclid's algorithm gives:

$$r_{k-1} = r_k q_{k+1}$$

so that r_k divides r_{k-1}. The next-to-last line gives:

$$r_{k-2} = r_{k-1} q_k + r_k$$

so that since r_k divides both itself and r_{k-1}, it must also divide r_{k-2}. Proceed in this way up the sequence of divisions with remainders to conclude that r_k divides **all** the terms on the left side of the Euclidean algorithm, which incudes all the remainders, and finally m and n themselves.

But why is r_k the **largest** natural number to divide m and n?

To see this, we work back down the divisons with remainders. If $d|m$ and $d|n$, then $d|r_1$ because $r_1 = n - mq_1$. Then d divides r_2 because $r_2 = m - r_1 q_2$, and similarly d divides all the remainders down to r_k. But if $d|r_k$, then clearly $d \leq r_k$, and so all divisors of both m and n are no bigger than r_k, thus r_k is the greatest common divisor.

Example: $5 = \gcd(1175, 395)$

(and this method is a good deal quicker than factoring the two numbers!)

Remark: We proved something even better than the proposition. Namely, looking at the last paragraph, we see that every common divisor of m and n actually **divides** the greatest common divisor.

Proposition 2: If $d = \gcd(m, n)$, then there are integers a and b so that:

$$d = am + bn$$

Proof: We prove the sentence below for all i by complete induction.

$P(i)$: **Every** r_i in Euclid's algorithm satisfies $r_i = a_i m + b_i n$.

(see the exercises in the previous section on complete induction)

(a) $P(1)$ and $P(2)$. Since $n = mq_1 + r_1$, we get:

$$r_1 = (-q_1)m + n$$

Similarly, we get:

$$r_2 = -q_2 r_1 + m = -q_2(-q_1 m + n) + m = (q_1 q_2 + 1)m - q_2 n$$

(b) Given $P(1), ..., P(i)$ with $i \geq 2$, then:

$$r_i = a_i m + b_i n \text{ and } r_{i-1} = a_{i-1} m + b_{i-1} n$$

From Euclid's algorithm, we also have:

$$r_{i-1} = r_i q_{i+1} + r_{i+1}$$

so substituting for r_i and r_{i-1} gives:

$$(a_{i-1} m + b_{i-1} n) = (a_i m + b_i n) q_{i+1} + r_{i+1}$$

and collecting the coefficients of m and n on one side gives:

$$r_{i+1} = (a_{i-1} - a_i q_{i+1})m + (b_{i-1} - b_i q_{i+1})n$$

which gives us $P(i+1)$ with $a_{i+1} = a_{i-1} - a_i q_{i+1}$ and $b_{i+1} = b_{i-1} - b_i q_{i+1}$.

This proves $P(i)$ by complete induction. If we apply it to the **last** natural number remainder r_k, then it gives the result we want since r_k is the gcd.

Recall that p is a **prime** number if 1 and p are the only natural numbers that divide p. This tells us in particular that if $m < p$, then $\gcd(m, p) = 1$. Similarly, if $p < m$ and p does not divide m, then $\gcd(p, m) = \gcd(m, p) = 1$ (because the gcd must divide p and cannot be equal to p). The Proposition we have just proved therefore tells us:

$$1 = am + bp$$

for some integers a and b whenever p does not divide m.

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

Proof: Let's suppose p does not divide m. Then by the discussion above:

$$1 = am + bp.$$

Multiplying through by n gives:

$$n = a(mn) + bpn$$

but since p divides mn, this equation tells us that it must also divide n. Thus **if** p doesn't divide m, then it **must** divide n. This proves the proposition!

Now for the fundamental theorem of arithmetic.

Unique Factorization: Every $n > 1$ is a product of finitely many prime numbers, and there is only one way to factor n as a product of primes.

Proof: We use the smallest element axiom. Let S be the set of natural numbers which are bigger than 1 and not a product of finitely many primes, and suppose s is the smallest element of S. Then either:

(i) s is a prime, or else

(ii) $s = mn$ for some m, n such that $1 < m < s$ and $1 < n < s$.

But (i) is not allowed since then s would be a product of **one** prime, so not an element of S. And since s is smallest, we see that if (ii) occurs, then m and n are not in S, so they must be products of finitely many primes, say $m = p_1....p_i$ and $n = q_1...q_j$, so that $s = p_1....p_i q_1....q_j$ would also be a product of finitely many primes. That is, $s \notin S$. Thus we've discovered that there cannot be a smallest element of S, so we must have $S = \emptyset$, proving that every $n > 1$ is a product of finitely many primes.

Now to show that there is only one factorization. Suppose

$$n = p_1...p_i \quad \text{and} \quad n = q_1...q_j.$$

Then $p_1 | q_1....q_j$, so by the Proposition above, either p_1 divides q_1 or else it divides $q_2....q_j$. Similarly, either p_1 divides q_2 or it divides $q_3....q_j$. Eventually, we find that p_1 must divide **one of** $q_1, ..., q_j$, implying that p_1 must be **equal** to one of the $q_1, ..., q_j$ since each p and q is a prime. Similarly, p_2 must be **equal** to one of the other q's, etc. and it follows that the p's and q's are the same primes(!) Thus there is only one way to factor n.

Euclid's proof that there are infinitely many primes: Suppose there were only finitely many primes. Then we could list them:

$$p_1, p_2, ..., p_m$$

so that the list stops at p_m. We would then have the peculiar number:

$$n = p_1 p_2 ... p_m + 1$$

which cannot be a prime (because it is bigger than all the primes) and cannot have any prime factors, because none of the list $p_1, ..., p_m$ of primes divides it (they all divide $n-1$, so they can't divide n). But then n would not factor as a product of primes, and we've just shown that **every** natural number factors as a product of primes. So this peculiar n does not exist, and therefore there must be infinitely many primes!

Finding gcd's by factoring: Suppose we are given m and n, together with their factorizations into primes:

$$m = p_1^{n_1} p_2^{n_2} ... p_i^{n_i} \text{ and } n = q_1^{m_1} q_2^{m_2} ... q_j^{m_j}$$

(the same primes are collected together, so that $p_1 \neq p_2 \neq ... \neq p_i$ and similarly for the q's). Then we get a factorization of the $\gcd(m, n)$ by the following procedure. We try to locate each p as a q. If it is not a q, it doesn't factor the gcd. If it is a q, then it does factor, and the smaller of the two exponents is the exponent which occurs in the factorization of the gcd.

Example: $720 = 2^4 \cdot 3 \cdot 5$ and $200 = 2^3 \cdot 5^2$ so

$$\gcd(720, 200) = 2^3 \cdot 5 = 40$$

(Why does this procedure work?)

Exercises:

1. Prove by induction that:

(a) $r^m r^n = r^{m+n}$ and

(b) $(r^m)^n = r^{mn}$

(Hint: Think about the proof of division with remainders.)

2. For each of the following pairs of numbers m and n, first find their gcd (call it d), and second, find integers a and b so that $d = am + bn$.

Example: $m = 395, n = 1175$. Going up Euclid's algorithm we get:

$$5 = (-38)10 + 385 = (-38)(395 - 385) + 385 = (-38)395 + (39)385$$
$$= (-38)395 + (39)(1175 - 2 \cdot 395) = (-38 - 2 \cdot 39)395 + (39)1175$$
$$= (-116)395 + (39)1175$$

(a) $m = 24$ and $n = 61$

(b) $m = 24$ and $n = 62$

(c) $m = 24$ and $n = 63$

(d) $m = 232617$ and $n = 533127$

3. The **least common multiple** of m and n, written $\mathrm{lcm}(m, n)$, is the smallest natural number e such that both:

$$m|e \text{ and } n|e$$

(a) Let $d = \gcd(m, n)$. Prove that $\mathrm{lcm}(m, n) \leq \frac{mn}{d}$.

(b) Prove that $\mathrm{lcm}(m, n)$ **divides** mn.

(Hint: If $\mathrm{lcm}(m, n) = ma$ and $\mathrm{lcm}(m, n) = nb$, then $\gcd(a, b) = 1$.)

(c) Prove that $d \geq \frac{mn}{\mathrm{lcm}(m,n)}$.

(d) Conclude that: $\mathrm{lcm}(m, n) \cdot \gcd(m, n) = m \cdot n$.

(e) If we are given the prime factorizations of m and n then what is the prime factorization of the $\mathrm{lcm}(m, n)$? (Model your answer on the procedure for finding the prime factorization of the gcd.)

4. If p is a prime and $m < p$, prove that p divides $\binom{p}{m}$.

(Hint: p divides $p! = \binom{p}{m} \cdot m! \cdot (p - m)!$)