Math 31 Lesson Plan

Day 8: Euclidean Algorithm

Elizabeth Gillaspy

October 4, 2011

Supplies needed:

- Quizzes
- Colored chalk
- Presentation sign-up sheet

Goals for students: Students will:

- Solidify their understanding of the Euclidean algorithm
- Get a better sense, by example, for what sort of writing I expect from their proofs
- Become more comfortable with the second form of induction

[**Lecture Notes: Write everything in blue, and every equation, on the board. [Square brackets] indicate anticipated student responses. *Italics* are instructions to myself.**]

- *Return Quizzes*
- *Reminder – resubmit starred problems to get credit!*
- *Reminder – Groups must pick a presentation date by Friday. If you're happy with your group membership, come do so ASAP!*

Today's a Number Theory day. We're going to talk about the Euclidean algorithm, and then if there's time we'll talk about the Fundamental Theorem of Arithmetic.

What's the point of the Euclidean Algorithm? [allows us to find gcd of two numbers; allows us to write the gcd as a linear combination of the two numbers] What does it rely on? [Division algorithm]

Example: Find $(60, 21)$. find integers x, y such that $60x + 21y = (60, 21)$.

By the division algorithm, we can write $60 = q21 + r$. What are q and r? [$q = 2, r = 18$]. If an integer k divides both 60 and 21, what can we say about r/k? [it's an integer, because $r = 60 - 21q$ and k divides the right hand side of this equation.]

Therefore, $(60, 21) = (21, 18)$. Who can tell me why? *Think-pair-share if need be.* [Any common divisor of 60 and 21 is also a common divisor of 21 and 18, by the argument above; hence (60,21) divides both 21 and 18, and (60, 21) $\leq (21, 18)$. Since $60 = q21 + r$, it also follows that (21, 18) divides both 21 and 60, and so $(21, 18) \leq (60, 21)$ as well. Hence they must be equal.]

So now, let's try to find (21,18). Should be simpler, because 18 is smaller than 60, right? We repeat the process for the new pair of integers:

$$21 = q_1 18 + r_1; \quad q_1 = 1, r_1 = 3.$$

What can we say about the relationship between (21, 18) and (18, 3)? [they're equal] So let's repeat for this pair:

$$18 = q_2 3 + r_2; \quad q_2 = 6, r_2 = 0.$$

A remainder of 0 means that $3|18$, so $(18,3) = 3$. Therefore, $(60,21) = 3$ also.

Questions?

Now, Let's find integers x, y such that $60x + 21y = (60,21) = 3$. To do this, we use the previous equations to rewrite 3:

$$3 = 21 - 18 = 21 - (60 - 2 \cdot 21) = 3 \cdot 21 - 60.$$

Thus $x = -1, y = 3$. Observe that x and y might be negative, but they're still integers!

OK, your turn. Please try to find someone to work with that you haven't worked with before!

in groups Find (121, 44); (357, 240). Find integers x, y so that $121x + 44y = (121, 44)$, and integers z, w so that $357z + 240w = (357, 240)$.

---

after groupwork Let's talk about the Fundamental Theorem of Arithmetic. *Any integer $n \geq 2$ can be written as the product of (not necessarily distinct) primes $p_1 p_2 \ldots p_r$. Moreover, any such factorization is unique (up to reordering the list of primes).*

Proof: How do we prove Existence of a factorization? [second form of induction] So what do we have to do? [Check base case] What's our base case this time? [$n = 2$] The base case is the smallest case, the place that you're starting from. Since 2 is prime, the statement $P(n) =$ "n can be written as the product of primes" is true for the case $n = 2$.

Now what? Now, suppose that $P(k)$ is true for all $2 \le k < n$. We want to show that $P(n)$ is true. There are two cases to check: what are they?

- n is prime;
- n is composite.

finish from here – shouldn't be hard.

Is everyone convinced of the proof that a factorization exists for each n?

What about the proof of Uniqueness? What proof technique do you want to try here? [contradiction/induction]

We will prove uniqueness using contradiction and induction. Observe that the base case is true; 2 has a unique factorization into primes. Now, suppose that for any number $k < n$, we can factor k uniquely into primes.

Suppose that $p_1 p_2 \dots p_r$ and $q_1 q_2 \dots q_s$ are two factorizations of n into primes. I claim that p_1 must equal q_i for some $1 \le i \le s$. How should we prove this sub-claim?

Let's suppose not, and try to reach a contradiction. What does that mean? [In other words, $p_1 \ne q_i$ for any i.] But we know $p_1 | n = q_1 q_2 \dots q_s$. If $p_1 \ne q_1$, then $(p_1, q_1) = 1$. Why? [because the only divisors of primes are themselves and 1] But then, by Theorem 4.3, we must have $p_1 | q_2 \dots q_s$. If $p_1 \ne q_2$, we use the same argument to see that $p_1 | q_3 \dots q_s$. Repeating the argument s times, we see that $p_1 | q_s$ – which is a contradiction to our assumption that $p_1 \ne q_i$ for any i.

Therefore, $p_1 = q_i$ for some i. So, we can cancel these out of the factorization: $p_2 p_3 \dots p_r = q_1 q_2 \dots \hat{q}_i \dots q_s$. *Explain notation!* But $p_2 \dots p_r = n/p_1 < n$, so we know the factorization of n/p_1 is unique. In other words, the primes $p_2, p_3, \dots, p_r$ are the same as the primes

$q_1, q_2, \ldots, \hat{q}_i, \ldots, q_s$. Therefore, since $p_1 = q_i$, the two factorizations $p_1 p_2 \ldots p_r$ and $q_1 \ldots q_s$ of n consist of precisely the same primes, so they're the same factorization. $\square$

Questions?