Lecture 19

Instructor's Comments: Existence repeated here for convenience or if you didn't want to do it before

Theorem: (Unique Factorization Theorem) (UFT) (Fundamental Theorem of Arithmetic)

Every integer $n > 1$ can be factored uniquely as a product of prime numbers, up to reordering.

Note: Prime numbers are just the product of a single number.

Proof: Existence.

Assume towards a contradiction that not every number can be factored into prime numbers. Let n be the smallest such number (which exists by WOP). Then either n is prime, a contradiction, or $n = ab$ with $1 < a, b < n$. However, since $a, b < n$, the numbers a and b can be written as a product of primes (since n was minimal). Thus $n = ab$ is a product of primes, contradicting the definition of n.

Uniqueness

Instructor's Comments: Cannot do uniqueness yet

Assume towards a contradiction that there exists a natural number $n > 1$ such that

$$n = p_1 p_2 ... p_k = q_1 q_2 ... q_m$$

where each p_i and q_j are primes (not necessarily distinct) and further assume that this n is minimal (WOP). By definition, $p_1 \mid n = q_1 q_2 ... q_m$. Hence, by the generalized Euclid's Lemma, we see that $p_1 \mid q_j$ for some $1 \leq j \leq m$. Hence, since p_1 and q_j are prime numbers, we have that $p_1 = q_j$. Without loss of generality, we may reorder the primes q_j so that q_j is the first prime, that is, $p_1 = q_1$. Canceling out these primes gives

$$N_0 := p_2 ... p_k = q_2 ... q_m$$

Now $N_0 < n$ and so, the above representations must be equal up to reordering by the minimality of n. Hence, $k = m$ and we may reorder so that

$$p_\ell = q_\ell \qquad \text{for all } 2 \leq \ell \leq k$$

Multiplying N_0 by p_1 shows that the two representations of the factorizations of n are the same up to reordering. This contradicts the existence of n hence all numbers can be written uniquely as a product of primes up to reordering of primes.

Instructor's Comments: This is a difficult proof. I would advise taking some time and really going through it. Call this 10 minutes

Theorem: (Euclid's Theorem) (ET) There exists infinitely many primes.

Proof: Assume towards a contradiction that there exists finitely many primes, say $p_1, p_2, ..., p_n$. Consider the number

$$N = 1 + \prod_{i=1}^{n} p_i$$

By the Fundamental Theorem of Arithmetic (UFT), N can be written as a product of primes. In particular, there exists a prime $p \mid N$ by the Generalized Euclid's Lemma. Since we have only finitely many primes, $p = p_1$ for some $1 \leq i \leq n$. Since $p \mid N$ and $p \left| \prod_{i=1}^{n} p_i \right.$, we conclude by Divisibility of Integer Combinations that

$$p \left| \left(N - \prod_{i=1}^{n} p_i \right) \right. = 1$$

This is a contradiction since no prime divides 1 (you could use Bounds by Divisibility since primes are bigger than 1). Hence, there must be infinitely many primes. ■

To complete the gaps in the previous proofs, we need to talk about the two forms of Euclid's Lemma. To do this, we will need to talk about greatest common divisors and more importantly, Bézouts Lemma.

Instructor's Comments: This is the 7 minute mark

Instructor's Comments: Think of this as a sort of 'converse' to BL

Theorem: GCD Characterization Theorem (GCDCT) If $d > 0$, $d \mid a$, $d \mid b$ and there exist integers x and y such that $ax + by = d$, then $d = \gcd(a, b)$.

Proof: Let $e = \gcd(a, b)$. Since $d \mid a$ and $d \mid b$, by definition and the maximality of e we have that $d \leq e$. Again by definition, $e \mid a$ and $e \mid b$ so by Divisibility of Integer Combinations, $e \mid (ax + by)$ implying that $e \mid d$. Thus, by Bounds by Divisibility, $|e| \leq |d|$ and since $d, e > 0$, we have that $e \leq d$. Hence $d = e$. ■

Example: $6 > 0$, $6 \mid 30$, $6 \mid 42$ and $30(3) + 42(-2) = 6$ and hence by the GCD Characterization Theorem, we have that $\gcd(30, 42) = 6$.

Example: Prove if $a, b, x, y \in \mathbb{Z}$, are such that $\gcd(a, b) \neq 0$ and $ax + by = \gcd(a, b)$, then $\gcd(x, y) = 1$.

Proof: Since $\gcd(a, b) \mid a$ and $\gcd(a, b) \mid b$, we divide by $\gcd(a, b) \neq 0$ to see that

$$\frac{a}{\gcd(a, b)} x + \frac{b}{\gcd(a, b)} y = 1$$

Since $1 \mid x$ and $1 \mid y$ and $1 > 0$, GCD Characterization Theorem implies that $\gcd(x, y) = 1$. ■

Instructor's Comments: This is the 20 minute mark

Handout or Document Camera or Class Exercise

Prove or disprove the following:

(i) If $n \in \mathbb{N}$ then $\gcd(n, n+1) = 1$.

(ii) Let $a, b, c \in \mathbb{Z}$. If $\exists\ x, y \in \mathbb{Z}$ such that $ax^2 + by^2 = c$ then $\gcd(a, b) \mid c$.

(iii) Let $a, b, c \in \mathbb{Z}$. If $\gcd(a, b) \mid c$ then $\exists\ x, y \in \mathbb{Z}$ such that $ax^2 + by^2 = c$.

Solution:

(i) $n + 1 = n(1) + 1$ and so by the GCD Characterization Theorem, $\gcd(n+1, n) = \gcd(n, 1) = 1$. Hence this is true.

(ii) $\gcd(a, b) \mid a$ and $\gcd(a, b) \mid b$. Thus, by Divisibility of Integer Combinations, $\gcd(a, b) \mid (ax^2 + by^2)$ which implies that $\gcd(a, b) \mid c$. Hence this is true.

(iii) This is false. Suppose that $a = 3$, $b = 0$ and $c = 6$. Then $\gcd(a, b) = 3 \mid 6 = c$ however, $3x^2 + 0y^2 = 6$ implies that $x^2 = 2$, a contradiction.

Instructor's Comments: This is the 30-35 minute mark. At the end of this lecture, I think it would be wise to talk about the midterm a bit. It is coming up so I've left a bit of extra time to review for the midterm.