# Week 1 Notes: 2019 August 26-28

MATH 465/565
Towson University

Monday, 2018 August 26

## 1 Unique Factorization

**Definition** (Unique factorization)**.** Given an integer $n > 1$, there is a unique way to write $n = p_1 \cdot p_2 \cdot \ldots \cdot p_k$ as a product of prime numbers (up to changing the order of the primes).

"Bigger" sets of integers: Gaussian integers

**Gaussian integers** are of the form $a + b\sqrt{-1} = a + bi$, $a, b \in \mathbb{Z}$.

Multiplying Gaussian integers yields a Gaussian integer. Gaussian integers also have unique factorization.

Replace $\sqrt{-1}$ with $\sqrt{-5}$; "integers" look like $a + b\sqrt{-5}$, $a, b \in \mathbb{Z}$. We can add, subtract, multiply, and divide these. Unique factorization fails in this ring.

**Example 1.**

$$\begin{aligned} 6 = 2 \cdot 3 &= (2 + 0\sqrt{-5})(3 + 0\sqrt{-5}) \\ &= (1 + \sqrt{-5})(1 - \sqrt{-5}) \\ &= 1 - (-5) \\ &= 6 \end{aligned}$$

It turns out that 2, 3, $1 + \sqrt{-5}$, and $1 - \sqrt{-5}$ are all irreducible. So, unique factorization is broken.

## 2 Division with Remainder

**Lemma** (Euclid's division lemma)**.** *For any $j, k \in \mathbb{Z}$, where $k > 0$, $\exists q, r \in \mathbb{Z}$ st*

$$j = qk + r,$$

*where $0 \leq r < k$, $q$ denotes the quotient, and $r$ denotes the remainder.*

*Proof.* Suppose we're given $j, k \in \mathbb{Z}$ w/ $k > 0$. Set $q = \left\lfloor \frac{j}{k} \right\rfloor$ then set $r = j - qk$, so $j = qk + r$. It remains to show that $0 \leq r < k$. We know $q = \left\lfloor \frac{j}{k} \right\rfloor$, so $\frac{j}{k} - 1 < \left\lfloor \frac{j}{k} \right\rfloor \leq \frac{j}{k}$ by the properties of the floor function. Multiply through by $k$ to get $j - k < qk \leq j$. Note that get $qk$ in the middle because $q = \left\lfloor \frac{j}{k} \right\rfloor$. Take the second half of this inequality:

$$\begin{aligned} qk &\leq j \\ 0 &\leq j - qk = r \end{aligned}$$

Now, take the first half of the inequality:

$$\begin{aligned} j - k &< qk \\ j - qk &< k \end{aligned}$$

So, we have $r = j - qk < k$ and $0 \leq r < k$ as desired. □

**Definition.** Say that $a$ **divides** $b$, denoted by $a \mid b$ if $\exists q \in \mathbb{Z}$ st $aq = b$. Note that anything divides 0 since for any $a$, we can take $q = 0$ and $a \cdot 0 = 0$.

**Example 2** (p. 15)**.** For each nonzero integer $a$, $a \mid 0$.

**Definition.** If $a, b \in \mathbb{Z}$, we say that $d = \gcd(a, b)$ is the **greatest common divisor** of $a, b$ if $d \mid a$, $d \mid b$, and if $f \mid a$, $f \mid b$, then $f \mid d$.

**Example 3** (p. 16)**.** The positive divisors of 12 are 1, 2, 3, 4, 6, and 12. The positive divisors of $-8$ are 1, 2, 4, and 8. Thus, the positive common divisors of 12 and $-8$ are 1, 2, and 4; hence, $\gcd(12, -8) = 4$.

**Theorem.** *Given any two integers $a, b$, their greatest common divisor $d = \gcd(a, b)$ exists.*

*Proof.* We will prove this by construction, using Euclid's division lemma. Take $a, b$, and assume $a \geq b$. Call $r_0 = b$. Use Euclid's division lemma to get $a = q_1 b + r_1$. If $r_1 \neq 0$, then define $q_2$, $r_2$ by $r_0 = b = q_2 r_1 + r_2$. If $r_2 \neq 0$, then $r_1 = q_3 r_2 + r_3$. Keep going until eventually, we get $r_{n-2} = q_n r_{n-1} + r_n$, where $r_n = 0$. How do we know this is a finite process? This has to terminate bc $r_1 > r_2 > r_3 > ...$ and the numbers are all $\geq 0$.

<u>Claim:</u> $r_{n-1} = \gcd(a, b)$, where $r_{n-1}$ is the last nonzero remainder.

*Proof.* (Of the claim) We need to show that $r_{n-1} \mid a$ and $r_{n-1} \mid b$ and that if $f \mid a$ and $f \mid b$, then $f \mid r_{n-1}$. Use induction to show that $r_{n-1}$ divides $r_1$ for any $0 \leq i \leq n-1$. Base case: $r_{n-1} \mid r_{n-2}$. We know $r_{n-2} = q_n r_{n-1} + 0$, so $r_{n-1} \mid r_{n-2}$ by the definition of divides. Reverse induction step: Suppose $r_{n-1}$ divides both $r_i$ and $r_{i+1}$. We want to show it divides $r_{i-1}$. We know that $r_{i-1} = q_{i+1}(r_i) + r_{i+1}$. Since $r_{n-1} \mid r_i$, $existsq$ w/ $r_i = q r_{n-1}$ and since $r_{n-1} \mid r_{i+1}$, $\exists q'$ st $r_{i+1} = q' r_{n-1}$. So,

$$\begin{aligned} r_{i-1} &= q_{i+1}(q r_{n-1}) + q' r_{n-1} \\ &= [q_{i+1} \cdot q + q'] r_{n-1} \end{aligned}$$

So, $r_{n-1} \mid r_{i-1}$ and $r_n \mid r_0 = b$. Similarly, $r_{n-1} \mid a$. □

□

## Wednesday, 2018 August 28

**Example 4.** Use Euclid's Algorithm to find $\gcd(391, 272)$.

$$\begin{aligned} \gcd(391,272) &= \gcd(272,119) \qquad 391 = 272(1) + 119 \\ &= \gcd(119,34) \qquad 272 = 119(2) + 34 \\ &= \gcd(34,17) \qquad 119 = 34(3) + 17 \\ &= \boxed{17} \end{aligned}$$

# 3 Extended Euclidean Algorithm

**Theorem.** *If $\gcd(a, b) = d$, then $\exists x, y \in \mathbb{Z}$ st $ax + by = d$.*

*Proof.* Claim: $\exists x_i, y_i$ st $ax_i + by_i = r_i$ for each $r_i$ in Euclid's Algorithm.

*Proof.* Induct on $i$. Base case: let $i = 1$. Recall from Euclid's Algorithm that $a = q_1 b + r_1$. We can take $x_1 = 1$ and $y_1 = q_1$. So, the base case holds. Inductive step: suppose the claim is true for all integers up to $i$. Namely, $\exists x_i, y_i$ where $ax_i + by_i = r_i$. We want to show that the claim is true for $r_{i+1}$. Recall Euclid tells us that

$$r_{i-1} = q_{i+1} r_i + r_{i+1} \qquad (\star).$$

We know $r_{i-1} = ax_{i-1} + by_{i-1}$ and $r_i = ax_i + by_i$ by the inductive step. Plugging them into $(\star)$, we get

$$ax_{i-1} + by_{i-1} = q_{i+1}(ax_i + by_i) + r_{i+1}.$$

So,

$$r_{i+1} = \underbrace{(-q_{i+1}x_i + x_{i-1})}_{x_{i+1}} a + \underbrace{(-q_{i+1}y_i + y_{i-1})}_{y_{i+1}} b$$

Both $x_{i+1}$ and $y_{i+1}$ are integers. □

□

**Example 5.** Find $x, y$ st $391x + 272y = 17$

We know from Example 2 that

$$\begin{aligned} 17 &= 119 - 3(34) \\ 34 &= 272 - 2(119) \\ 119 &= 391 - 1(272) \end{aligned}$$

So, we obtain the following result

$$\begin{aligned} 17 &= 119 - 3(34) \\ &= 119 - 3(272 - 2(119)) \\ &= 7(119) - 3(272) \\ &= 7(391 - 1(272)) - 3(272) \\ &= 7(391) - 10(272) \end{aligned}$$

So, $\boxed{x = 7,\ y = -10}$.

**Corollary.** *For any integers $a, b$ w/ $\gcd(a, b) = d$, then $\exists x, y$ st $ax + by = c$ iff $d \mid c$.*

*Proof.* ($\Leftarrow$) First, suppose $d \mid c$. By the definition of divides, $\exists e$ st $c = de$. By Extended Euclid, $\exists x', y'$ st $ax' + by' = d$. Multiply by $e$:

$$a\underbrace{(x'e)}_{x} + b\underbrace{(y'e)}_{y} = de = c$$

($\Rightarrow$) Suppose $ax + by = c$ for some $x, y \in \mathbb{Z}$. Since $d \mid a$ and $d \mid b$ (from $\gcd(a, b) = d$), we can write $a = df$ and $b = dg$. Plug these into the linear combination to get

$$(df)x + (dg)y = c \Leftrightarrow d(fx + gy) = c.$$

So, $d \mid c$ by definition. □

**Definition.** We say $p$ is **prime** if whenever $p = ab$, then either $a = \pm 1$ or $b = \pm 1$. We say that $a, b$ are **coprime** or **relatively prime** if $\gcd(a, b) = 1$.

**Example 6** (p. 20)**.** The positive divisors of 7 are 1 and 7. The positive divisors of 27 are 1, 3, 9, and 27. Since 1 is the only positive common divisor of 7 and 27, these two integers are coprime.

**Theorem.** *If $\gcd(a, c) = 1$ and $a \mid bc$, then $a \mid b$.*

*Proof.* Bc $\gcd(a, c) = 1$, we know $\exists x, y$ st $ax + cy = 1$. Multiply this through by $b$:

$$abx + cby = b.$$

Since $a \mid bc$, $\exists e$ st $bc = ae$. Plug this in:

$$\begin{aligned} abx + aey &= b \\ a(bx + ey) &= b \end{aligned}$$

So, $a \mid b$. □

**Corollary.** *If $p$ is a prime number and $p \mid ab$, then either $p \mid a$ or $p \mid b$.*

*Proof.* If $p \mid a$, then we're done. Suppose $p \nmid a$. Since $p$ is prime, $\gcd(p, a) = 1$. By the theorem, $p \mid b$. □

**Theorem** (The Fundamental Theorem of Arithmetic)**.** *If $n > 1$ factors into prime numbers $n = p_1 \cdot p_2 \cdot ... \cdot p_k$, then this factorization is unique.*

*Proof.* Induct on $n$. Base case: let $n = 2$. 2 is prime, so this factorization is unique. So, the base case holds. Inductive step: suppose the theorem is true for all integers $m$, $1 < m < n$. We must consider two cases:

Case 1: $n$ is prime. By the definition of prime, the factorization $n = n$ is a unique factorization into primes.

Case 2: $n$ is not prime. This means $\exists a, b < n$ st $ab = n$. Since $a, b < n$, they factor uniquely as $a = q_1 q_2 ... q_j$ and $b = r_1 r_2 ... r_\ell$. We get a factorization of $n$ now by concatenating these two factorizations and reordering.

$$n = (q_1 ... q_j)(r_1 ... r_\ell) = p_1 p_2 ... p_k$$

It remains to show that this factorization is unique. Suppose it isn't unique. This means that

$$\begin{aligned} n &= p_1 p_2 ... p_k \\ &= s_1 s_2 ... s_j \quad \text{(different factorization)} \end{aligned}$$

Take $p_1$ so $p_1 \mid s_1 ... s_j$. Since $p_1$ is prime, it must divide one of the $s_i$ from this list. By the corollary, say it divides $s_i$. $s_i$ is also prime and divisible by $p_1$. So $s_i = p_1$. Remove both of these numbers from the two factorizations.

$$\frac{n}{p_1} = p_2 p_3 ... p_k = s_1 s_2 ... s_{i-1} s_{i+1} ... s_j$$

Since $\frac{n}{p_1} < n$, it has a unique factorization. So $k = j$ and the list of $p_i$ is the same as the list of $s_i$. □

**Problem to think about:** Let $\{F_n\}$ be the sequence of Fibonacci numbers. What is $\gcd(F_n, F_{n-1})$? How many steps does it take to compute w/ Euclid's Algorithm? Can you find other numbers smaller than $F_n$ that require more steps?