Week 2 Notes

Justin Thomas

February 2019

1 Last Week's "To Think About"

Use Euclid's algorithm to compute gcd(21,13)

21=1(13)+8
13=1(8)+5
8=1(5)+3
5=1(3)+2
3=1(2)+1
2=2(1)

Note that the sequence of remainders is the Fibonacci Sequence backwards.

Compute gcd(F_{n+1}, F_n)
How many times does F_n go into F_{n+1}?

$F_{n+1} = 1(F_n) + F_{n-1}$
$F_n = 1(F_{n-1}) + F_{n-2}$

Note: $0 \leq F_{n-1} < F_n$ always holds for $n > 1$

The steps of Euclid's algorithm for Fibonacci numbers are:
$F_{n+1} = 1(F_n) + F_{n-1}$ where q=1 if n¿1 and r=F_{n-1}

Now we can take this and write an induction proof from here.

2 Divisibility (cont.)

2.1 Corollary 2-1

If $d = gcd(a, b)$ then there exists integers x and y such that $ax + by = d$.

Proof: Use the Euclidean algorithm backwards.

Suppose that we use the Euclidean algorithm and get equations
a=q$_0b + r_1$
b=q$_1r_1 + r_2$
r$_{n-1} = q_nr_n + 0$

Claim: There exist x_i and y_i such that $ax_i + by_i = r_i$ for each $i \geq 1$; and $ax_{i-2} + by_{i-2} = r_{i-2}$.

Proof By Induction:

Base Case: $i = 1$
r$_1 = a - q_0b$
Let $x_1 = 1$, $y_1 = -q_0$

Induction Step:
Suppose there exist x_{i-1} and y_{i-1} such that $ax_{i-1} + by_{i-1} = r_{i-1}$

We want to prove there exist x_i and y_i such that $ax_i + by_i = r_i$.

We know from before that $r_{i-2} = q_{i-1}r_{i-1} + r_i$so it follows that
$r_i = r_{i-2} - q_{i-1}r_{i-1}$
=(ax$_{i-2} + by_{i-2}) - q_{i-1}(ax_{i-1} + by_{i-1})$
=a(x$_{i-2} - q_{i-1}x_{i-1}) + b(y_{i-2} - qy_{i-1})$

We can define these quantities being multiplied to a and b as x_i and y_i.

When $i = n$ we have $ax_n + by_n = r_n = d = gcd(a, b)$.

2.2 Example

Find x and y such that $16x + 6y = gcd(16, 6) = 2$

$16 = 2(6) + 4$ can be rewritten to $4 = (16 - 2(6))$

$6 = 1(4) + 2$ can be rewritten to $2 = (6 - 1(4))$

It follows that:
$2 = 6 - 1(16 - 2(6))$
$2 = 6 - 1(16) + 2(6)$
$2 = 3(6) - 1(16)$

Thus, $x = -1$ and $y = 3$.

2.3 Corollary 2-2

If $gcd(a, b) = d$ there exist x and y such that $ax + by = c$ if and only if $d|c$.

Proof: $\Rightarrow$ Suppose $ax + by = c$ has a solution. We know that $d|a$ and $d|b$ so $a = df$ and $b = dg$. Then

$dfx + dgy = c$
$d(fx + gy) = c$

Thus, $d|c$.

$\Leftarrow$ Suppose $d|c$. This means that $c = de$. By our theorem, there exist x and y such that $ax + by = d$. Multiply through e
$a(xe) + b(ye) = de = c$

2.4 Definitions

1. p is a prime number if whenever $a|p$ and $a > 0$ then either $a = 1$ and $a = p$. (Definition 2-2)

2. We say that a and b are relatively prime if $gcd(a, b) = 1$. (Definition 2-3)

For ex. 10 and 21 are relatively prime.

Theorem: If $gcd(a, c) = 1$ and $a|bc$ then $a|b$

Proof: Since $gcd(a, c) = 1$ there exist x and y so that $ax + cy = 1$
Multiply through by b:
$abx + bcy = b$
Since $a|bc$ there exists f such that $af = bc$. So:
$abx + afy = b$
$a(bx + fy) = b$
So $a|b$

2.5 Corollary 2-3

If p is a prime number and $p|ab$ then either $p|a$ or $p|b$. (not both)

Proof: If $p|a$ we're done. So suppose it doesn't, then
$gcd(a, p) = 1$

By our theorem, $p|b$.

2.6 The Fundamental Theorem of Arithmetic

If $n \geq 2$ is an integer then there exists prime numbers $p_1 \leq p_2 \leq p_3 ... \leq p_k$

And this is unique n that if $p'_1 \leq p'_2 \leq ...p'_l$ are primes and $p'_1 p'_2 ... p'_l = n$ then $l = k$ and $p_i = p_i$

Proof by induction:

Base Case: $n = 2$; 2 is prime so we have a factorization into primes $p_1 = 2$ and is unique.

Induction: Assume that for every $1 < a < n$ a has a a unique factorization into primes.

Case 1: n is prime then $p_1 = n$ and we have a unique factorization of n.

Case 2: n is not prime. This means there exist a and b with $1 < a < n$ and $1 < b < n$ with $n = ab$.

By our induction hypothesis a and b factor uniquely into primes.

$a = p_1 p_2 ... p_k$
$b = p'_1 p'_2 ... p'_l$
So $n = p_1 p_2 ... p_k p'_1 p'_2 ... p'_l$

Reorder to get a factorization of n.

Regarding uniqueness:

So n has a factorization, need to show that it is unique.

Suppose this factorization is not unique. Then

$n = p_1 p_2 ... p_k = q_1 q_2 ... q_l$
Now $p_1 | n$ so $p_1 | q_1 q_2 ... q_l$
So either $p_1 | q_1$ or $p_1 | (q_2 ... q_l)$
By induction, $p_1 | q_i$ for some i thus
$p_1 = q_i$

Similarly, $q_i | p_j$ for some j and so $q_1 = p_j$
$p_1 = q_i = p_j \geq p_1$ so $j = i = 1$ and $p_1 = q_1$
$\frac{n}{p_1} = p_2 p_3 ... p_k = q_2 ... q_l$
$\frac{n}{p_1} < n$ so it factors uniquely (into prime numbers) so

$k = l$ and $p_i = q_i$