Group 5 Notes 9/19
MA 330
Andrew Stewart, Rebecca Mickelson, and James Drury

A few Kuttaka Problems

6.) $n \equiv 2 \mod 3$

$n \equiv 3 \mod 5$

$n \equiv 5 \mod 7$

Our idea to solve was to find a m such that

$m \equiv 0 \mod 3$

$m \equiv 0 \mod 5$ m= 15 works

$m \equiv 1 \mod 7$

$m \equiv 0 \mod 3$

$m \equiv 1 \mod 5$ m= 21 works

$m \equiv 0 \mod 7$

$m \equiv 1 \mod 3$

$m \equiv 0 \mod 5$ $m= 35 \equiv 2 \mod 3$ so m=70 will work

$m \equiv 0 \mod 7$

This provides us with the answer

$2(70) + 3(21) + 5(15) = 278 = n$

This works because 70 is congruent to 1 mod 3 but 0 mod 3 and 0 mod 5 and there are similar patterns with 21 and 15 so we are confident that 278 = n.

To get a general answer we can add any multiple of 3*5*7, which is equal to 105, to 278 and the number will still satisfy all the congruencies so a general answer is $n = 278 + 105t$ for any t. Also since 278 > 105 we can subtract 105 without changing the congruence.

$278-105 = 173-105 = 68 \Rightarrow n= 68 + 105t$ for any t

This trick also works with ideals

$\mathbb{Z}$ is the integers

$\mathbb{Q}$ ($\sqrt{5}$)= {a + b$\sqrt{5}$ | a,b ∈ $\mathbb{Q}$ }

Special thing about $\mathbb{Z}$ is that it includes prime numbers and a fundamental theorem on integers.

The theorem states that every integer is uniquely a product of primes up to order.

Let A= $\mathbb{Z}$ ($\sqrt{5}$)

Can we say that A= {a + b$\sqrt{5}$ | a,b ∈ $\mathbb{Z}$ } like we did with the rational numbers?

Consider ($\sqrt{5} + 1$) ($\sqrt{5} - 1$) = 5−1= 4 but 4= 2^2

So, the question is how does 2 factor?

In $\mathbb{Z}$ we have "2"

So an ideal is $\mathbb{Z}$ /(2)= {[0], [1]} where [0] is all even numbers and [1] is all odd numbers.

We can do operations such as [0] + [1] = [1], [1] * [1] = [1], and [0] * [1] = [0]

What if we consider A/(2)= {[0], [1], [$\sqrt{5}$]}

Let $\bar{A}$ = {∝ ∈ $\mathbb{Q}(\sqrt{5})$ integral over $\mathbb{Z}$}

Integral mean that $\propto^n + a_1 \propto^{n-1} + \cdots + a_n = 0$

Is A= $\bar{A}$?

We have information to assume an equation of the form $\propto^2 + a_1 \propto + a_2 = 0$

Something worth trying

$\sqrt{5} + 1$ ∈ A but is $\frac{\sqrt{5}+1}{2}$ ∈ $\bar{A}$?

Fermat's Last Theorem

Suppose $n \geq 3$ then $x^n + y^n = z^n$ has a solution (x, y, z) = (a, b, c) iff one of a, b, or c is 0

This was proved by Andrew Wiles in 1994.

If n is odd, then $x^n + y^n = (x + y)(x + \omega y)$ .... $(x + \omega^{n-1} y)$ with $\omega^n = 1$

Ex. $x^3 + y^3 = (x + y)(x^2 + xy + y^2) = (x + y)(x + \omega y)(x + \omega^2 y)$

To be true $1 + \omega + \omega^2 = 0$

Ideals and rings

Let R be a ring. Then $(a_1, \dots, a_n)$ is an ideal generated by $a_1, \dots, a_n$

$(a_1, \dots, a_n) = \{x_1 a_1 + \cdots + x_n a_n | \, x_i \in$ R.