MATH CIRCLE-PART I

TOPIC: Unique Factorization

We start with something familiar. What is the factorization of 120 into the smallest possible components?

Definition The **integers** are the numbers $\ldots, -2, -1, 0, 1, 2, 3, \ldots$. We denote this set of numbers by $\mathbb{Z}$.

Definition A **prime number** is a positive integer greater than 1 whose only positive divisors are 1 and itself.

Example We learned how to factor integers in elementary school: $120 = 2^3 \cdot 3 \cdot 5$. Although we could make various tree diagrams of factorization, the end result would be the same.

This is a result of the **Fundamental Theorem of Arithmetic**.

Fundamental Theorem of Arithmetic Every integer greater than 1 is a prime or a product of primes. This product is unique, except for the order in which the factors appear; thus, if $n = p_1 p_2 \cdot \cdots \cdot p_s$ and $n = q_1 q_2 \cdot \cdots \cdot q_t$, where all the p's and q's are primes, then $t = s$ and after renumbering the q's, we have $p_i = q_i$, for all i.

This basically says that the integers, $\mathbb{Z}$, have **unique factorization**. We can extend this idea to a larger class of objects than just the integers. Before doing so, we'll provide an example where unique factorization fails.

FACTORIZATION OF POLYNOMIALS

Next, we want to generalize the idea of Unique Factorization beyond the integers, $\mathbb{Z}$, to polynomials. First we need a couple of definitions.

Definition An element with a multiplicative inverse is called a **unit**.

Definition An element r is called **irreducible** if whenever $r = ab$, the a or b must be a unit.

Example (*prime, but not irreducible*) In $\mathbb{Z}_6$, called "the integers modulo 6", we have the numbers {0,1,2,3,4,5}, which represent the only possible remainders

when an integer is divided by 6. Note that 2 is a prime number, but 2 is not irreducible, since $2 = 2 \cdot 4$.

Example (*irreducible, but not prime*) In $\mathbb{Z}[\sqrt{-5}]$, $2 + \sqrt{-5}$ is irreducible, but not prime.

Recall that we can factor a polynomial $2X^3 + 12X^2 + 16X$ into $2X(X + 4)(X + 2)$. However, we can not factor $X^2 + 1$ over $\mathbb{Z}$. We would need to introduce the complex numbers in order to factor this second polynomial. When a polynomial can not be factored, we say that it is irreducible.

Unique Factorization in $\mathbb{Z}[X]$ Every polynomial in $\mathbb{Z}[X]$ that is not the zero polynomial or a unit in $\mathbb{Z}[X]$ can be written in the form $cp_1(X)p_2(X) \cdot \cdots \cdot p_m(X)$, where c is a constant and the $p_i(X)'$s are irreducible polynomials of positive degree. Furthermore, if

$$cp_1(X)p_2(X) \cdot \cdots \cdot p_m(X) = dq_1(X)q_2(X) \cdot \cdots \cdot q_n(X),$$

then $c = \pm d$, $n = m$, and after renumbering the $q(x)'s$, $p_i(x) = \pm q_i(x)$, for $i = 1, 2, \ldots, m$.

In the above example, $c = 2, p_1(X) = X - 0, p_2(X) = X + 4$, and $p_3(X) = X + 2$.

We need not restrict ourselves to polynomials over $\mathbb{Z}$. It is common to consider polynomials with coefficients over $\mathbb{Q}$ or $\mathbb{C}$.

In our second example, we can not factor $X^2 + 1$ over $\mathbb{Z}$ or $\mathbb{Q}$, but we CAN factor it over $\mathbb{C}$, into $(X - \sqrt{-1})(X + \sqrt{-1})$.

Let's consider factorization over $\mathbb{Q}$.

Eisenstein's Irreducibility Criteria (1850) Let $f(X) = a_nX^n + a_{n-1}X^{n-1} + \cdots + a_1X + a_0 \in \mathbb{Z}[X]$. If there is a prime p such that $p \dagger a_n, p|a_{n-1}, \ldots, p|a_0$, and $p^2 \dagger a_0$, then $f(X)$ is irreducible over $\mathbb{Q}$.

Example $3X^5 + 15X^4 - 20X^3 + 10X + 20$. We can't choose $p = 3$ since 3 divides the leading coefficient. Similarly, we can't choose $p = 2$ since 4 divides the constant term 20. So let $p = 5$.

Non-Example: *Eisenstein's doesn't always work* X^2+1 Note that $a_2 = 1, a_1 =$

0, and $a_0 = 1$. Let p be any prime. Then p does not divide a_2 or a_0, but it does divide a_1. Moreover, p^2 does not divide a_0. Therefore, by Eisenstein's Criteria, $X^2 + 1$ is irreducible over $\mathbb{Q}$.

HISTORY

Extensions of $\mathbb{Z}$ have interested mathematicians for centuries. For example, Gauss proved that the elements of $\mathbb{Z}[i]$ admit unique factorization into prime elements, just like the ordinary integers, and he exploited this fact to prove other results.

Besides Gauss, other number theorists like Euler, Dirichlet, and Kummer realized the usefulness of adjoining solutions of polynomial equations to $\mathbb{Z}$ and used this idea to prove some special cases of Fermat's (1601-1665) Last Theorem. They used $\mathbb{Z}[\zeta_p]$, where ζ is a p^{th} root of unity.

Definition The $\mathbf{p^{th}}$ **roots of unity** are the roots of the polynomial $x^p - 1$.

Example The second roots of unity are ± 1. They are the only solutions to the equation $x^2 - 1 = 0$.

Example The third roots of unity are 1, $\frac{-1}{2} + \frac{\sqrt{-3}}{2}$, and $\frac{-1}{2} - \frac{\sqrt{-3}}{2}$. Again, these are the solutions to the equation $x^3 - 1 = 0$. We have $x^3 - 1 = (x - 1)(x^2 + x + 1)$, and we use the quadratic formula to determine the complex roots.

Number theorists were able to solve many particular cases of Fermat's Last Theorem. They thought that they also had a proof for other n, but it was pointed out that they were assuming unique factorization of the cyclotomic integers, which is false in certain cases. The basic idea was to write:

$$x^p = z^p - y^p = \prod_{j=0}^{p-1} (z - y\zeta_p^j).$$

In particular, for $p = 23$, $\mathbb{Z}[\zeta_p]$ does not have unique factorization.

It has been conjectured that Fermat's famous "proof" consisted of an idea similar to the one given by number theorists of the nineteenth century, mistakenly assuming the existence of unique factorization.