PRIME, MODULAR ARITHMETIC, AND

By: Tessa Xie & Meiyi Shi
OBJECTIVES

- Examine Primes In Term Of Additive Properties & Modular Arithmetic
- To Prove There Are Infinitely Many Primes
- To Prove There Are Infinitely Many Primes of The Form 4n+2
- To Prove There Are Infinitely Many Primes of The Form 4n
- To Prove There Are Infinitely Many Primes of The Form 4n+3
- To Prove There Are Infinitely Many Primes of The Form 4n+1
Proof: Primes in Form of 4n+3

Prove By Contradiction

**Assumption:** Assume we have a set of finitely many primes of the form

\[ 4n+3 \]

\[ P = \{ p_1, p_2, \ldots, p_n \}. \]

Construct a number \( N \) such that

\[
N = 4 \times p_1 \times p_2 \times \ldots \times p_n - 1
= 4 \left[ (p_1 \times p_2 \times \ldots \times p_n) - 1 \right] + 3
\]

\( N \) can either be prime or composite.

If \( N \) is a prime, there’s a contradiction since \( N \) is in the form of 4n+3 but does not equal to any of the number in the set \( P \).

If \( N \) is a composite, there must exist a prime factor “a” of \( N \) such that a is in the form of 4n+3.
All the primes are either in the form of $4n+1$ or in the form of $4n+3$. If all the prime factors are in the form of $4n+1$, $N$ should also be in the form of $4n+1$. There should exist at least one prime factor of $N$ in the form of $4n+3$. 
“a” does not belong to set P

\[ \frac{N}{a} = \frac{(4 \times p_1 \times p_2 \times \ldots \times p_n - 1)}{a} \]

\[ = \frac{(4 \times p_1 \times p_2 \times \ldots \times p_n)}{a} - \frac{1}{a} \]

(1/a is not an integer)

Conclusion:

a is a prime in the form of 4n+3, but a does not belong to set P. Therefore, we proved by contradiction that there exists infinitely many primes of the form 4n+3.
Proof: Primes in Form of 4n+1

Prove by Fermat’s Little Theorem

Let N be a positive integer

Let M be a positive integer in the form:
\[ M = [N \times (N-1) \times (N-2) \times \ldots \times 2 \times 1]^2 + 1 \quad (M \in \mathbb{Z}^+ \& M \text{ is odd}) \]

\[ = (N!)^2 + 1 \]

Let P be a prime number greater than N such that p|M (p is odd)
\[ M \equiv 0 \pmod{p} \]

Then, we can rewrite M in terms of N:
\[ (N!)^2 + 1 \equiv 0 \pmod{p} \]
\[ (N!)^2 \equiv -1 \pmod{p} \]
Fermat’s Little Theorem:

\[ a^{p-1} \equiv 1 \pmod{p} \]

In order to use Fermat’s Little Theorem in the proof, we would like to convert the left hand side of the equation in the form of \( a^{p-1} \), which can be achieved by raising the equation to the power of \((p-1) / 2\).

\[ [(N!)^{2}]^{(p-1)/2} \equiv [-1 \pmod{P}]^{(p-1)/2} \]

We get:

\[ (N!)^{p-1} \equiv (-1)^{(p-1)/2} \pmod{p} \]

Notice that the left hand side of the equation is in the form of \( a^{p-1} \) where \( N! \) represents \( a \).

By Fermat’s Little Theorem, we can rewrite the equation as:

\[ 1 \pmod{p} \equiv (-1)^{(p-1)/2} \pmod{p} \]
Since $p$ is odd, $1 \neq -1 \pmod{p}$.

Then,

$$1 = (-1)^{(p-1)/2}$$

The only case for this equation to hold true is when $(p-1)/2$ is even.

If $(p-1)/2$ is even, it can be represented as:

$$(p-1)/2 = 2n \quad (n \in \mathbb{Z})$$

Therefore,

$$p = 4n + 1$$

$$a^p = a \pmod{p}$$
Since \( p \) is greater than \( N \) and \( N \) can get infinitely large, as \( N \) approaches infinity, \( p \) also approaches infinity.

**Conclusion:**

We proved by Fermat’s Little Theorem that there exists infinitely many primes in the form of \( 4n+1 \).

**Gratitude to Fermat!!**
Special Thanks To:

Lillian
Corina
Maria
& All the People who helped us