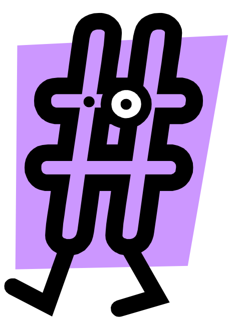
# PRIME, MODULAR ARITHMETIC, AND

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

**<u>Assumption</u>**: 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

$N = 4 * p_{1*}\ p_{2*} \ldots {}_{*}p_n - 1$

$\quad = 4\ [\ (p_{1*}\ p_{2*} \ldots {}_{*}p_n) - 1\ ] + 3$

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.

?

4N + 3

4N + 1

"a" does not belong to set P

$$N/a = (4 * p_{1*}\, p_{2*} \dots {}_{*}p_n - 1) / a$$

$$= (4 * p_{1*}\, p_{2*} \dots {}_{*}p_n) / a - 1/a$$

(1/a is not an integer)

**<u>Conclusion:</u>**

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:

$$M = [\, N * (N-1) * (N-2) *\dots 2 * 1]^2 + 1$$ (M $\in$ Z+ & M 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 term 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:

$$(p-1)/2 = 2n \qquad (n \in Z)$$

$$p = 4n + 1$$

# $a^p = a \pmod{p}$

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