Prime Numbers Modulo 4

Ismael El Yassini

University of Sherbrooke

August 21, 2020

Outline

Pigeonhole Principle (weak version)

Theorem

If n+1 objects are placed in n places, there must be at least two objects in the same place.

Proof.

Let assume the contrary, that every place there would have at most 1 object,we would have in all place a total at most n objects, which contradicts the hypothesis. □

Pigeonhole principle

Theorem

If n objects are placed in k places, there must be at least $\lceil \frac{n}{k} \rceil$ *objects in the same place.*

Where $\lceil x \rceil$ is the ceilling part of x, the smallest integer that is greater than or equal

Proof.

Let assume the contrary, that every place there would have at most $\lceil \frac{n}{k} \rceil - 1$ objects, we would have in all place a total of at most $k \times (\lceil \frac{n}{k} \rceil) - 1) < n$ objects because $\frac{n}{k} - 1 \leq (\lceil \frac{n}{k} \rceil - 1) < \frac{n}{k}$, which contradicts the hypothesis. □

Infinite Pigeonhole Principle

Theorem

Given an infinite number of objects , if they are placed in a finite number of places, there is at least one place with an infinite number of objects.

Proof.

Let assume the contrary, that every place there would have finitely object, we would have in all place finitely many objects, which contradicts the hypothesis. □

Prime numbers

Definition

A positive number $p \succ 1$ is a prime number if no integer $d > 1$ and $d \neq p$ such that $d|p$ d divise p.

We are interested in prime numbers since every tout entier $n \succ 1$ is either a prime number, or can be written as a unique product of prime numbers (ignoring the order).

Euclid Theorem

Theorem

There are infinitely many prime numbers

Proof.

Let assume the contrary, there exist finitely many prime numbers, the set is a part of the set of the non negative integers upper bounded nonempty because it contains 2, so the set has a maximum, let denote p this prime number. Let consider the number p!+1 greater that p so it is composite.
There existe a prime q that divides p!+1
We have $q \leq p$ hence $q|p!$
We deduce that $q|(p! + 1) - p! = 1$
Contradiction. □

Title page

Theorem

There are infinitly many prime numbers of the form 4k+3.

Proof.

Let assume the contrary that there exist only finitely many prime number of the form 4k+3.
Let denote this set P_3. This set is nonempty (for exemple 3).
P_3 is a part of the set of the non negative integers upper bounded nonempty, so the set has a maximum, let denote p this prime number. Let consider the number N=4p!-1 which is greater than p and congruent to 3 modulo 4.
Let assume the contrary that all divisors of N are of the form of 4k+1, so 4p!-1 remain of the form of 4k+1, contradiction. There exists a prime $q \equiv 3\,[4]$that divides p!+1
We have $q \leq p$ hence $q|4p!$
Thus $q \mid 4p! - (4p! - 1) = 1$ Contradiction.
Thus the result. □

Wilson's Theorem

Theorem

$(p-1)! + 1 \equiv 0\,[p]$ *if and only if p is prime.*

Proof.

$\Longrightarrow$ Let suppose that p divides (p-1)!+1, hence there existe an integer k such that: pk=(p-1)!+1
Hence gcd(p,i)=1 for $1 \leq i \leq p-1$
so the only positive divisor of p are 1 and p.
Therefore p is prime.
$\Longleftarrow$ Let suppose p is prime
We have p divides (p-1)!+1 for p=2,3.
For $p \geq 5$.
Method 1: Let $1 \leq k \leq p-1$, k is coprime with p, so $\{0, k, ..., (p-1)k\}$ is a complete system of residus modulo p (a permutation of $\{0, 1, ..., (p-1)\}$ *modulo* p) □

Proof.

We solve for x: $x^2 - 1 \equiv 0\,[p]$ for classes modulo p.
Since p is a prime,
$p \mid x^2 - 1p \iff \mid x - 1$ or $p/x + 1 \iff x \equiv 1\,[\,p]$ ou $x \equiv p - 1\,[p]$
By Bezout's Theorem, we multiply the distints pairs that have product 1 from (p-1)!,
so $(p-1)! \equiv 1 \times (p-1) \equiv -1(modp)$
Hence $(p-1)! + 1 \equiv (modp)$
Methode 2:
We consider the polynomial $X^{p-1} - \overline{1}$ in Z/pZ[X] that have as roots $\{\overline{1}, \overline{2}, ..., \overline{p-1}\}$ By Little Fermat Theorem.
Using Viet relation between coefficients and root of the polynomial, we have $\overline{1} \times \overline{2} \times ... \times \overline{p-1} = (-1)^{p-1} \times \overline{-1} = \overline{-1}$ since p-1 odd.
Therefore p divides (p-1)!+1 □

Theorem

Theorem

Let p is an odd prime number then
$\exists u \ / \ u^2 \equiv -1 \, (mod \ p \ ) \Longleftrightarrow p \equiv 1 \, (mod \ 4 \ )$ *[2]*

Proof.

$\Longrightarrow$

Let suppose that $\exists u \ / \ u \equiv -1 \, (mod \ p \ )$

$u^2 \equiv -1 \, (mod \ p \ )$

$\left(u^2\right)^{\frac{p-1}{2}} \equiv (-1)^{\frac{p-1}{2}} \, (mod \ p \ )$

$u^{p-1} \equiv (-1)^{\frac{p-1}{2}} \, (mod \ p \ )$

$u^{p-1} \equiv (-1)^{\frac{p-1}{2}} \, (mod \ p \ )$

Using Little Fermat Theorem, this is true if and only if $p \equiv 1 \, (mod \ 4 \ )$ $\square$

Proof.

$\Longleftarrow$ Let suppose that $p \equiv 1 \, (mod \ 4 \ )$

By Wilson Theorem

$$-1 \equiv \ (p-1)! \ (mod \ p \ )$$

$$\equiv \ [(1)(p-1) \ ][(2)(p-2) \ ] \ldots \left[\left(\frac{p-1}{2}\right)\left(\frac{p+1}{2}\right) \ \right](mod \ p \ )$$

$$\equiv \ [(1)(-1) \ ][(2)(-2) \ ] \ldots \left[\left(\frac{p-1}{2}\right)\left(-\frac{p-1}{2}\right) \ \right](mod \ p \ )$$

$$\equiv \ (-1)^{\frac{p-1}{2}} \left[\left(\frac{p-1}{2}!\right)\right]^2 (mod \ p \ )$$

$$\equiv \ \left[\left(\frac{p-1}{2}!\right)\right]^2 (mod \ p \ )$$

We take $u = \left[\left(\frac{p-1}{2}!\right)\right]^2$ $\square$

Theorem

There are infinitely many prime numbers of the form 4k+1

Proof.

Let assume the contrary that there exist only finitely many prime number of the form 4k+1.
Let denote this set P_1. This set is nonempty (for exemple 5).
P_1 is a part of the set of the non negative integers upper bounded nonempty, so the set has a maximum, let denote p this prime number. Let consider the number $N = [(2p)!]^2 + 1$ which is greater than p and let put $u = [(2p)!]^2$.
Using the last theorem, the prime divisor(s) are of the form 4k+1.
Let q be one of these divisors.
We have $q \leq p$ hence $q | [(2p)!]^2$
We deduce that $q|([(2p)!]^2 + 1) - [(2p)!]^2 = 1$
Contradiction. □

Comment: Dirichlet Theorem states: for any two positive coprime integers a and b, there are infinitely many primes of the form a + nb (congruent to a modulo b), where n is also a positive integer.
The proof requires some calculus and analytic number theory. For the special case a=1 can be proven by cyclotomic polynomials.

An Introduction to Cyclotomic Polynomial

Definition

For a positive integer d, define the polynomial $\Phi_d(X)$ by
$\Phi_d(X) = \prod_{1 \leq k \leq d \ gcd(d,k)=1} (X - e^{\frac{2\pi ik}{n}})$

Theorem

For a positive integer n $X^n - 1 = \prod_{d|n} \Phi_d(X)$

and $deg(\Phi_d(X)) = \phi(d)$
where $\phi(d)$ is the Euler indicator,ie. the number of number less than equal to d ,and coprime with d.
A well known result is $n = \sum_{d|n} \phi(d)$

Lemma

Lemma

For two integers n et u, il existe x , y not bot 0 such that

$$-\sqrt{n} \leq x \leq \sqrt{n}\ , -\sqrt{n} \leq x \leq \sqrt{n}$$

and x-uy is divisible by n. [1]

Proof.

Let $k+1 = \lfloor \sqrt{n} \rfloor$ be the largest integer that is smaller than or equal to $\sqrt{n}$. We consider the numbers of the form $x - uy$ where x and y in $\{0, 1, ..., k\}$ Each integer has k + 1 options, so there are $(k+1)^2 \succ n$ possible options.

By the pigeonhole principle, there are two numbers of the form x-uy that leave the same remainder modulo n. □

Proof.

Let $x_1 - uy_1$ and $x_2 - uy_2$ the two integers, their difference is divisible by n. Let put $x = x_1 - x_2$ and $y = y_1 - y_2$, these integers are not both 0, since (x_1, y_1) and (x_2, y_2) are distincts. □

Fermat's Theorem

Theorem

Every prime number p of the form 4k+1 can be written as sum of two squares. [1]

Proof.

Let u be an integer such that $u^2 + 1$ is divisible par p.
Using proposition , there exist two integers x and y not both 0 such that x-uy is divisible by p and

$$-\sqrt{n} \leq x \leq \sqrt{n}\ , -\sqrt{n} \leq x \leq \sqrt{n}$$

Hence $x^2, y^2 \leq p$.
Since p is a prime number the inequalities are strict.
We have $x \equiv uy\,(modp)$, hence $x^2 \equiv (uy)^2 \equiv -y^2\,(modp)$ hence $x^2 + y^2$ is divisible by p . □

Proof.

By the double inequality $0 \prec x^2 + y^2 \prec 2p$.
We deduce that $x^2 + y^2 = p$. □

References


Pablo Soberón.
Problem-Solving methods in combinatorics.
Springer, 2013.


Justin Stevens and David Altizio.
Olympiad number theory through challenging problems.