* Average gap b/w to primes is about $\ln n$.
* Twin primes $\exists$ infinitely many p such that both p & $p+2$ are primes.
* $\exists$ a constant c such that for infinitely many n, $[n, n+c]$ contains 2 primes.
* There exist infinitely many primes $\forall n\, P(n) \rightarrow P(n)$ holds for all n for sufficiently large.

  $\exists n_0\, \forall n\, [(n \geq n_0) \Rightarrow P(n)]$
* $\forall n\, \exists n_0\, [(n \geq n_0) \Rightarrow P(n)]$ ⟶ Always true
* $\exists$ infinitely many n satisfying $\boxed{P(n)\quad \forall n\, \exists n_0\, ((n_0 \geq n) \wedge P(n_0))}$

Induction principle

* Assumption about natural numbers :-

  Peano's Axioms :-

  ① 0 is a natural number

  ② If n is a natural number there is a unique natural number called $n+1$. & $\forall n$, $(n+1 \neq 0)$

$$\boxed{\forall n\, \exists m\quad m = n+1}$$

$$\forall n\, \forall m\, \forall k\, (m = n+1) \wedge (k = n+1) \Rightarrow (m = k)$$

$$\forall n\, \forall m\, \big((n+1) = (m+1) \Leftrightarrow (n = m)\big)$$

★ $\exists$ next(n,m) $\rightarrow$ there exist a predicate next(n,m) where n, m are natural numbers. that satisfies. this will be true if & only if $m = n+1$

(i). $\forall n \; \exists m \;$ next(n,m)

(ii) $\forall n, m, k \; (\text{next}(n,m) \wedge \text{next}(n,k) \Rightarrow (m=k))$

$\rightarrow$ predicate satisfying these properties are called functions.

$m = \text{next}(n) \longrightarrow m = n+1$ or $m = \text{succ}(n)$.

(iii) $\forall n \; \sim \text{next}(n, 0)$

(iv) $\forall n \forall m \forall k \; (\text{next}(n,k) \wedge \text{next}(m,k)) \Rightarrow (n=m)$

3 Induction:-

$\cancel{\forall P(x)} \quad \cancel{\forall (P(x)} \;/\; \cancel{(P(0)} \wedge (P(n))$

$$\forall P \quad [P(0) \wedge \forall n \, (P(n) \Rightarrow P(n+1))] \Rightarrow \forall n (P(n))$$

$P(n+1) \rightarrow$ true

$$\forall m \; [\text{next}(n,m) \Rightarrow P(m)]$$

or

$$\exists m \; (P(m) \wedge \text{next}(n,m))$$

★ add$(n,m) = k$

add(n,m,k) is a predicate such that for all m, n there is a unique k such that add(m,n,k) is true.

Add function

1) $\forall n$ $add(n, 0) = n$

$\forall n, m$ $add(n, m+1) = add(n, m) + 1$

add(n, m) is defined for all m, n → use induction on m.

This is already derived by induction on m.

Collate Problem

Consider the sequence defined by $x_0 = n$ for some $n \geq 1$

$$x_{i+1} = 1 \quad \text{if } x_i = 1$$
$$= \frac{x_i}{2} \quad \text{if } x_i \text{ is even and } > 1$$
$$= 3x_i + 1 \quad \text{if } x_i \text{ is odd } > 1$$

Conjecture for any initial value n the sequence becomes all 1's after some point.

Write this statement using predicates?

$$\forall n \left[(n > 0) \Rightarrow \forall x \left((x(0) = n) \wedge \forall i \left[(x(i) = 1 \Rightarrow x(i+1) = 1) \wedge (\quad \right] \right. \right.$$
$$\Rightarrow \exists_p \forall_j (x(j) = 1)$$

$\exists_n\ P(n) \Rightarrow Q(n) \longrightarrow \exists_n\ \sim P(n) \vee \exists_n\ P(n) \wedge Q(n)$

$\forall n\ P(n) \Rightarrow Q(n)$

$$\forall P \left[P(1) \wedge \forall i \left[P(i) \Rightarrow P(2i) \right] \wedge \forall i \left[P(6i+4) \Rightarrow P(2i+1) \right] \right.$$
$$\Rightarrow \forall_{i>0}\ P(i)$$

* If $P \Rightarrow R$ & $P \Rightarrow \sim R$ then this implies P is false.

* Rules to derive new statement :

A proof is a sequence of statements $P_1, P_2 \ldots P_n$ such that each P_i is either an axiom (or) is implied by the peano's statements $\forall_i (P_1 \wedge P_2 \wedge \ldots P_{i-1}) \Rightarrow P_i$

Once a proof has been found for a statement it can be treated as an axiom.

* **Divisibility** :-

$$\forall_{n>0} \forall_n \exists_{q,r} \left(n = qm + r \wedge 0 \le r < m \right)$$

q & r are uniquely defined.

* $mod(0, m) = 0$

$mod(n+1, m) = mod(n, m) + 1$ if $(mod(n,m)+1 \; != m)$

$= 0$ otherwise.

* floor(n,m) =

$floor(0,m) = 0$

$floor(n+1, m) = floor(n,m)$ if $mod(n+1, m) != 0$

$= floor(n, m) + 1$ otherwise

$$\boxed{n = add(mult(floor(n,m)), mod(n,m))}$$

* Prove that every positive number can be written uniquely as $a_1 \times 1! + a_2 \times 2! + \dots + a_n \times n!$ for some n where $\boxed{0 \le a_i \le i}$ for $1 \le i \le n$ & $a_n > 0$

* Cantor representation $(a_1\ a_2 \dots a_m)$
$(b_1\ b_2 \dots b_m)$

Given Cantor representations of two numbers find the representation of their sum.

$$\begin{cases} n = a_1 \times 1! + a_2 \times 2! + \dots + a_n \times n! \\ m = b_1 \times 1! + b_2 \times 2! + \dots + b_m \times m! \end{cases}$$

for 1 → $a_1 = 1$

for $n+1$ →

a_1: 0, 1

b_1: 0, 1

$a_1 = \cancel{0}$ $b_1 = 1$

$a_1 = 1$ $b_1 = 0$

(0, 0)
(0, 1)
(1, 0)
(1, 1)

$1 \times 2!$

$1 + (a_2 + b_2)$

$e_2 = (d_1 + (a_2 + b_2)) \bmod 3$

$d_2 =$

$n = a_1 \times 1! + a_2 \times 2! + \dots + a_n \times n!$

$n+1$ 0 1   0 1 2.

$1 +$

$1 \times 2!$

$c_1 = (a_1 + b_1 + d_0) \bmod 2$

$d_1 = (a_1 + b_1)/2$

$\forall n\ \exists a_i\ \exists b_i$

$c_2 = (a_2 + b_2 + d$

$n = a_i d_2 = a_2 + b_2$

$(n = (a\_)\ m = (b\_)) \Rightarrow (n+m)$

$\forall n, m\ \exists a_i\ \exists b_i$

* Greatest Common Divisor

For any two positive numbers n and m, there exists a number g such that g/n and g/m and for any other number d such that d/n and $d/m \Rightarrow d/g$

$g/n \longrightarrow g$ divides n

* every common divisor of n and m is a divisor of g, which is itself a common divisor.

→ Prove by strong Induction on m, Assume for all numbers $< m$ and for all n, and prove for m:

Consider two cases :-

(i) If $m/n \Rightarrow$ take $g = n$ satisfies the property of gcd.

(ii) If $m \nmid n \Rightarrow \exists_{q,r}$ such that $n = qm + r$

division property and $0 < r < n$

by strong induction, $\exists$ a number g. g/m, g/r & for all d such that $d/m \wedge d/r \Rightarrow d/g$.

$n = qm + r$

Since g/m & $g/r \Rightarrow g/n$

$r = q_2 g$ $m = q_1 g$

$\boxed{n = (qq_1 + q_2)g}$

If d/n & d/m to show that d/g.

$n = q_1 d$ $m = q_2 d$ $\Rightarrow d/r$

$r = (q_1 - qq_2)d$ d is common divisor of m & r $\Rightarrow d/g$.

Using well ordering of natural numbers

Consider the set S of all possible integers linear combination of m & n.

$\hookrightarrow$ All numbers that can be written in the form $xm+yn$ where x, y are integers.

This set is not empty since $m, n \in S \Rightarrow$ It has a smallest element g.

Claim g is the gcd of m and n

Since $g \in S$

$g = xm + yn$ for some integers x, y.

Claim g divides every number in S

Suppose S contains a number k not divisible by g

$k = qg + r \qquad 0 < r < g.$

Since g & k are integer linear combinations of n and m, so is r.

This contradicts the assumption that g is the smallest element in S.

* gcd (m, n) is an integer linear combination of m & n

gcd (n, m) { $r = n \% m$; if $(r == 0)$ return m;
else return gcd (m, r) ; }

* If $n = qm + r$ by induction we can find $g = xm + yr$

$r = n - qm$

$g = (x - qy)m + yn$

If $m | n$ $g = m$, $\boxed{g = 1 \times m + 0 \times n}$.

* If a/bc and $\gcd(a,b)=1 \Rightarrow a/c$

Since $\gcd(a,b)=1$, we can write $1 = xa + yb$ for some x, y. $c = xac + ybc$, a/bc & a/xac
$$\Downarrow$$
$$a/c$$

Uniqueness of Prime Factorization

Every number $n \geq 1$ can be written uniquely as $n = P_1 P_2 \ldots P_k$ where P_i is a prime and $P_1 \leq P_2 \leq P_3 \ldots \leq P_k$

Suppose $n = P_1 P_2 \ldots P_k = q_1 q_2 \ldots q_m$

Suppose $P_1 < q_1$ since P_1 divides n, $P_1 \mid (q_1)(q_2 \ldots q_m)$

$\gcd(P_1, q_1) = 1$ P_1 must divide $(q_2 \ldots q_m)$
$$\downarrow$$
this will finally give $P_1 \mid 1$ a contradiction!

* (1) Given two positive irrational numbers a, b such that $1/a + 1/b = 1$ show that every +ve integer n can be written as $\lfloor ka \rfloor$ or $\lfloor kb \rfloor$ for some integer k.

$a, b > 0$ & $\boxed{a, b > 1}$ $\lfloor a \rfloor \geq 1$ & $\lfloor b \rfloor \geq 1$

take $n=2$ for understanding

one of these must be 1

* Given n +ve numbers $a_1, a_2 \ldots a_n$ prove that $\exists$ a g such that $g/a_i \; \forall i$, $1 \leq i \leq n$ and for any d such that $\forall i \; d \mid a_i \Rightarrow d/g$

* Prove that a number is an integer linear combination of $a_1, a_2 \dots a_n$ iff it is a multiple of g.

* Given n - d dimensional vectors with integer coordinates prove that $\exists$ at most d vectors $b_1, b_2 \dots b_d$ such that every integer linear combination of $v_1, v_2 \dots v_n$ is an integer linear combination of $b_1, b_2 \dots b_d$ & viceversa

---

Modular Arithmetic

Two numbers a & b are congruent to each other mod n if a - b is divisible by n denoted by $a \equiv b \bmod n$

$a \equiv b \bmod n$

$b \equiv c \bmod n$

$\Rightarrow a \equiv c \bmod n$

$a \equiv b \bmod n$

$c \equiv d \bmod n$

$a+c \equiv (b+d) \bmod n$

$a * c = (b * d) \bmod n$

every number is congruent to a unique number in $\{0, 1, 2 \dots, n-1\}$ mod n $\longrightarrow$ division algorithm

* The congruence $ax \equiv 1 \bmod N$ has a solution mod n. iff $\gcd(a, n) = 1$ and if there is a solution it is unique mod n. $\rightarrow$ x is called the inverse of a mod N

* If $\gcd(a, n) = 1$ then $\exists$ p, q such that $pa + qn = 1$

$pa \equiv 1 \bmod n$

$x = p \bmod n$ is a solⁿ to $\boxed{ax = 1 \bmod n}$

If X_1 & X_2 are two solutions $aX_1 \equiv 1 \bmod n$ &

$aX_2 \equiv 1 \bmod n$ $a(X_1 - X_2) \equiv 0 \bmod n$

$\Rightarrow$ n divides $a(X_1 - X_2)$

since $\gcd(a,n) = 1$ $\Rightarrow$ n divides $(x_1 - x_2)$

★ Wilson's Theorm

$(n-1)! + 1 \equiv 0 \bmod n$ iff n is prime.

Suppose n is not a prime $\Rightarrow$ $\exists$ a divisor d of n

$1 < d < n$ $\quad d \mid (n-1)!$ $\quad d \mid n$

$(n-1)! + 1 = qn$ for some q

$\Rightarrow d \mid 1$ which is a contradiction.

Conversely if n is prime

$Z_n = \{0, 1, \text{---} n-1\}$

$(n-1)! = 1 \times 2 \times 3 \text{ ---- } \times n-1$

Consider this mod n.

$\{ 1, 2, 3, \text{ --- }, n-1$

look at pairs (a, a^{-1}) of $\}$.

If n is prime the only numbers that are their own inverses are 1 and $n-1$.

If x is its own inverse $x^2 \equiv 1 \bmod n \longrightarrow x^2 - 1 \equiv 0 \bmod n$

$(x-1)(x+1) \equiv 0 \bmod n$, since n is prime

either $x-1 \equiv 0 \bmod n$ or $x+1 \equiv 0 \bmod n$

$\Rightarrow x = +1$ or $x = n-1 \bmod n$.

* Any polynomial of degree d has atmost d roots in Z(n→prime) $\boxed{P_d(x) = 0 \bmod n}$

Fermat's Little Theorm:

If n is a prime number and $\gcd(a,n) = 1$, then

$a^{n-1} \equiv 1 \bmod n$ if n is prime $a^n \equiv a \bmod n$

$\gcd(a,n) = 1$

$Z_n = \{1, 2, \ldots, n-1\}$ ✓

$aZ_n = \{a, 2a, \ldots, (n-1)a\}$ ✓

↓

$\bmod n = \{1, \ldots, n-1\}$

$\boxed{a^{n-1} \equiv 1 \bmod n}$

for any b, $ax \equiv b \bmod n$ has a unique solution.

$(n-1)! \equiv a^{n-1}(n-1)! \bmod n$

$\gcd((n-1)!, n) = 1 \Rightarrow \quad a^{n-1} \equiv 1 \bmod n$

* Z_n when n is prime number ⇒ Every nonzero number has a multiplicative inverse mod n.

* $$\begin{bmatrix} 3 & 4 \\ 2 & 1 \end{bmatrix}\begin{bmatrix} x_1 \\ x_2 \end{bmatrix} = \begin{bmatrix} 1 \\ 4 \end{bmatrix} \bmod 7$$

$\mathbb{Z}_n \rightarrow$ finite field, if n is prime

Chinese Remainder Theorem

If $\gcd(m_1, m_2) = 1$ then for all a_1, a_2 the congruences $x \equiv a_1 \bmod m_1$ $x \equiv a_2 \bmod m_2$ has a unique solution $\bmod\ m_1 m_2$

$\exists\ p, q$ $\quad pm_1 + qm_2 = 1$

$$x = pm_1 a_2 + qm_2 a_1$$

$$= pm_1 a_2 + (1 - pm_1) a_1$$

$x \equiv a_1 \bmod m_1$ $\quad x \equiv a_2 \bmod m_2$

$y_1 \equiv a_1 \bmod m_1$ $\quad x_1 \equiv a_1 \bmod m_1$

$y_1 \equiv a_2 \bmod m_2$ $\quad x_1 \equiv a_2 \bmod m_2$

$\gcd(m_1, m_2) = 1$ $\quad (x_1 - y_1) \equiv 0 \bmod m_1$

$(x_1 - y_1) \equiv 0 \bmod m_2$

$\boxed{x_1 - y_1 \equiv 0 \bmod m_1 m_2} \Rightarrow \left\{ \begin{array}{l} x_1 \equiv \alpha \bmod m_1 m_2 \\ y_1 \equiv \alpha \bmod m_1 m_2 \end{array} \right\}$

Primality Testing :-

Given a large number with n decimal digits is it prime!

$\rightarrow$ efficient algorithm

① Try dividing by each number b/w 2 to $n-1$, if any one divides then not prime else it is.

② $(n-1)! + 1 \equiv 0 \bmod n$ iff n is prime

$\hookrightarrow$ inefficient

* If n is prime & $\gcd(a,n)=1$ then $a^{n-1} \equiv 1 \bmod n$
  the converse is not true.

  $a^{n-1} \bmod n$ can be computed efficiently.

* $x^2 \equiv 1 \bmod n$ if $x=1$ (or) $x=n-1$ only if n is prime.

Miller – Rabin Test: (Randomized Algorithm)

Given n, pick a random number a such that $2 \le a \le n$
if $\gcd(a,n) \ne 1$ then not prime
else Compute $a^{n-1} \bmod n \longrightarrow$ if this is not 1 then n is not prime.

Assume n is odd number and $n-1 = 2^k m$ for some $k>0$ and m an odd number.

Consider the sequence
$a^m \bmod n$, $a^{2m} \bmod n$, $a^{4m} \bmod n$
--- $a^{2^{k-1}m} \bmod n$ $a^{2^k m} \bmod n$

$a^{2^{k-1}m} \bmod n \longrightarrow$ Can be 1 (or) -1

$a^{2^k m} \bmod n \longrightarrow 1$

Keep going backward in this sequence, if we get something other than 1 (or) $n-1$ then n is composite.

Output Composite if $\exists$ a number in the sequence $\ne 1$ and the last number is $\ne n-1$.

* If n is composite for atleast $1/2$ the possible choices of "a" the Miller-Rabin test will violate that n is composite.

AKS

$(1+x)^n \equiv (1+x^n) \bmod n$ iff n is prime
$\hookrightarrow$ polynomial in x.

$(1 + \_\_\_\_ x^n) \bmod (x^r - 1)$

$\downarrow$

if $n > r$ $\boxed{x^n \equiv x^{n \% r} \bmod (x^r - 1)}$

* These tests only indicate whether a number is prime or not. No idea about a factor if n is Composite.

No efficient algorithm known for actually finding a factor for large number n.