papergrid®

Reflects You

Don't be afraid to give up the good to go for the great.

sooraj.ss1729@gmail.com +91-9400635788

INDEX

Appendix: 4-(2)

Name SOORAJ.S. Std Sec

Roll No. Subject School/College

SL No.	Date	Title	Page No.	Teacher Sign / Remarks
		QUANTUM COMPUTATION & QUANTUM INFORMATION		
		- Nielsen & Chuang		

Euler's theorem

If a is coprime to n, then,

$$a^{\phi(n)} = 1 \pmod{n}$$

where,

$\phi(n)$ is defined to be the # of +ve integers less than n which are coprime to n.

$$\gcd(a, n) = 1 \implies a^{\phi(n)} \equiv 1 \pmod{n}$$

Euler's theorem

Method: 1

PROOF

Lemma: Let $n > 1$ and $\gcd(a, n) = 1$.

If $a_1, a_2, \ldots, a_{\phi(n)}$ are the positive integers less than n and relatively prime to n, then

$$aa_1, aa_2, \ldots, aa_{\phi(n)}$$

are congruent modulo n to $a_1, a_2, \ldots, a_{\phi(n)}$ in some order.

Proof

$a_1, a_2, \ldots, a_{\phi(n)}$ are the positive integers less than n and relatively prime to n.

$a_i \neq a_j$ for $i \neq j$. & $\gcd(a_i, n) = 1$

$\gcd(a_i, n) = 1$ for all i and $\gcd(a, n) = 1$

$\Rightarrow \gcd(aa_i, n) = 1$ for all i

$\Rightarrow aa_i$ is coprime to n $\forall$ i

Uncle SC. Appendix-0

Let's define the sets.

$$A = \{aa_i \mid 1 \le a_i \le n,\ \gcd(a_i, n) = 1,\ \gcd(a, n) = 1\}$$

$$= \{aa_1, aa_2, \ldots, aa_{\phi(n)}\} \quad \text{such that } \gcd(aa_i, n) = 1$$

which has $\phi(n)$ elements and the set

$$B = \{a_i \mid 1 \le a_i \le n,\ \gcd(a_i, n) = 1,\ \gcd(a, n) = 1\}$$

$$= \{a_1, a_2, \ldots, a_{\phi(n)}\}$$

which has $\phi(n)$ elements.

$\gcd(a_i, n) = 1$ and $\gcd(a, n) = 1$

$\Longrightarrow \gcd(aa_i, n) = 1$

Euclidean Algorithm: $\gcd(aa_i, n) = \gcd(aa_i \bmod n, n) = 1$

$\Longrightarrow aa_i \bmod n \in B$.

$\therefore$ The map $f : A \to B$ defined by

$f(aa_i) = aa_i \bmod n$ is well defined.

Let's take 2 elements aa_i and aa_j in the set A and suppose that they have the same image in the set B,

i.e.,

$b = aa_i \bmod n \iff aa_i = b \pmod n$

$b = aa_j \bmod n \iff aa_j = b \pmod n$

$\Rightarrow aa_i - aa_j = 0 \pmod n$

with $1 \le i < j \le \phi(n)$

$\Rightarrow a(a_i - a_j) = 0 \pmod n$

$\Rightarrow a_i - a_j \mid n$

$\Rightarrow a_i = a_j \pmod n$. which is a contradiction

$\Rightarrow$ no two integers $aa_1, aa_2, \ldots, aa_{\phi(n)}$ are congruent modulo n.

$\therefore f : A \to B$ is one-one.

$|A| = |B| = \phi(n) \Rightarrow f : A \to B$ is a bijection.

$\therefore$ For a particular aa_i, there exists a unique integer b, where $0 \leq b < n$, for which $b \equiv aa_i \pmod{n}$ (or) $aa_i \equiv b \pmod{n}$.

$$\therefore aa_i \equiv a_{j(i)} \pmod{n}$$

$\therefore$

The numbers $aa_1, aa_2, \ldots, aa_{\phi(n)}$ and the numbers $a_1, a_2, \ldots, a_{\phi(n)}$ are identical (modulo n) in a certain order.

Proof: Euler's theorem

Let $a_1, a_2, \ldots, a_{\phi(n)}$ be the two integers less than n that are relatively prime to n. & we are given $\gcd(a, n) = 1$.

From Lemma,

$$aa_1 = a_1' \pmod{n}$$
$$aa_2 = a_2' \pmod{n}$$
$$\vdots \qquad\qquad \vdots$$
$$aa_{\phi(n)} = a_{\phi(n)}' \pmod{n}$$

where, $a_1', a_2', \ldots, a_{\phi(n)}'$ are the integers $a_1, a_2, \ldots, a_{\phi(n)}$ in some order.

Method: 2

Step 1:

On taking the product of these $\phi(n)$ congruences,

$$(aa_1)(aa_2)\cdots(aa_{\phi(n)}) \equiv a_1' a_2' \cdots a_{\phi(n)}' \pmod{n}$$

$$\equiv a_1 a_2 \cdots a_{\phi(n)} \pmod{n}$$

$$a^{\phi(n)}(a_1 a_2 \cdots a_{\phi(n)}) \equiv a_1 a_2 \cdots a_{\phi(n)} \pmod{n}$$

$\gcd(a_i, n) = 1$ for each i

$\rightarrow \gcd(a_1 a_2 \cdots a_{\phi(n)}, n) = 1$

Check Q.C Appendix 4-①

Inverse modulo n exists for $a_1 a_2 \cdots a_{\phi(n)}$.

$$\Rightarrow a^{\phi(n)} \equiv 1 \pmod{n}$$

Method: 2 $\gcd(a,n)=1 \implies a^{\phi(n)} \equiv 1 \pmod{n}$

Step 1: $a^{\phi(p^\alpha)} \equiv 1 \pmod{p^\alpha}$

For $\alpha=1$ the result is just Fermat's Little theorem. $\implies a^{p-1} \equiv 1 \pmod{p}$

Assume the result is true for $\alpha \geq 1$,

$$a^{\phi(p^\alpha)} \equiv 1 \pmod{p^\alpha}$$

$$\implies a^{\phi(p^\alpha)} = 1 + kp^\alpha \text{ for some } k \in \mathbb{N}$$

$$\left[\begin{array}{l} \phi(p^\alpha) = p^{\alpha-1}(p-1) \\ \to \phi(p^{\alpha+1}) = p^\alpha (p-1) \end{array}\right.$$

$$\begin{aligned} a^{\phi(p^{\alpha+1})} &= a^{p^\alpha (p-1)} \\ &= a^{p\phi(p^\alpha)} \\ &= (1+kp^\alpha)^p \\ &= 1 + \binom{p}{0} k^0 p^{0\alpha} + \binom{p}{1} k^1 p^{1\alpha} + \cdots + \binom{p}{p} k^p p^{p\alpha} \\ &= 1 + \sum_{j=1}^{p} \binom{p}{j} k^j p^{j\alpha} \end{aligned}$$

Skip 2:

Lemma 4.7A: Suppose p is prime & k is an integer in the range 1 to $p-1$. The p divides $\binom{p}{k}$.

$\therefore$

$p^{\alpha+1}$ divides every term in the sum, $\sum_{j=1}^{p} \binom{p}{j} k^j p^{j\alpha}$

So,

$$a^{\phi(p^{\alpha+1})} = 1 + qp^{\alpha+1} \quad \text{for some } q \in \mathbb{Z}$$

$$\Rightarrow a^{\phi(p^{\alpha+1})} \equiv 1 \pmod{p^{\alpha+1}}$$

By induction: $a^{\phi(p^{\alpha})} \equiv 1 \pmod{p^{\alpha}}$

Step 2 :

$\phi(mn) = \phi(m)\phi(n)$ given $\gcd(m,n) = 1$

$$a^{\phi(n)} = a^{\phi(p_1^{\alpha_1} p_2^{\alpha_2} \cdots p_m^{\alpha_m})}$$

$$= a^{\phi(p_1^{\alpha_1})\phi(p_2^{\alpha_2}) \cdots \phi(p_m^{\alpha_m})}$$

$$= a^{t\,\phi(p_j^{\alpha_j})} = \left(a^{\phi(p_j^{\alpha_j})}\right)^t$$

where,

$t = \phi(p_1^{\alpha_1}) \cdots \phi(p_{j-1}^{\alpha_{j-1}})\,\phi(p_{j+1}^{\alpha_{j+1}}) \cdots \phi(p_m^{\alpha_m})$

$= \dfrac{\phi(n)}{\phi(p_j^{\alpha_j})}$

$$= 1 + k\, p_j^{\alpha_j}$$

$a^{\phi(p_j^{\alpha_j})} = 1 \pmod{p^{\alpha_j}}$

$$\Longrightarrow a^{\phi(n)} = 1 \pmod{p_j^{\alpha_j}} \quad \text{for each } j$$

$$\therefore \quad a^{\phi(n)} = 1 \pmod{p_1^{\alpha_1}}$$

$$a^{\phi(n)} = 1 \pmod{p_2^{\alpha_2}}$$

$$\vdots$$

$$a^{\phi(n)} = 1 \pmod{p_m^{\alpha_m}}$$

Since $\gcd(p_i^{\alpha_i}, p_j^{\alpha_j}) = 1$ for $i \neq j$

the system of congruence has a unique solution and any two solutions to this system of equations are equal modulo $n = p_1^{\alpha_1} p_2^{\alpha_2} \cdots p_m^{\alpha_m}$, from the Chinese Remainder theorem.

If x and x' are both solutions to the system of equations $x \equiv 1 \pmod{p_j^{\alpha_j}}$

then

$$x \equiv x' \pmod{n}, \text{ where } n = p_1^{\alpha_1} \cdots p_m^{\alpha_m}.$$

Since $x' = 1$ is a solution, any solution to the set of equations $x \equiv 1 \pmod{p_j^{\alpha_j}}$ must satisfy $x \equiv 1 \pmod{n}$.

Therefore,

$$a^{\phi(n)} = 1 \pmod{n}$$

Method: 3 Using Lagrange's theorem.

Z_n^* be the set of all elements in Z_n which have inverse modulo n, i.e., the set of all elements in Z_n which are coprime to n. Z_n^* forms a group of size $\phi(n)$ under multiplication.

The multiplicative group of integers modulo n, may be written as $(Z_n^*, \cdot)$ (or) $(\mathbb{Z}/n\mathbb{Z})^\times$ (or) $(\mathbb{Z}/n\mathbb{Z})^*$ (or) Z_n^*.

$$Z_n^* = (\mathbb{Z}/n\mathbb{Z})^\times = \left\{ a \in \mathbb{Z}/n\mathbb{Z} \mid \begin{array}{l} a \text{ is coprime to } n \\ \text{(or) } \gcd(a,n) = 1 \end{array} \right\}$$

We have,

$|\mathbb{Z}_n^*| = \phi(n)$: # of +ve integers less than n which are coprime to n.

Since 'a' is coprime to 'n', i.e., $\gcd(a,n) = 1$

'a' represents some $[a] \in \mathbb{Z}_n^*$, which we also denote by 'a' here.

$$\boxed{|G| = |G:H|\cdot|H|}$$

From Lagrange's theorem : For a group G & $a \in G$,

$\langle a \rangle$ is the smallest subgroup of G containing 'a'.

$$|\langle a \rangle| \,\big|\, |G| \quad \& \quad |a| = |\langle a \rangle|$$

$$\Longrightarrow |a| \,\big|\, |G| \Longrightarrow a^{|G|} = e.$$

$$\therefore a^{|\mathbb{Z}_n^*|} = [1]$$

$$\Longrightarrow a^{\phi(n)} \equiv 1 \pmod{n}$$

- Z_n^* forms a group of size $\phi(n)$ under the operation of multiplication modulo n.

- Let 'a' is an arbitrary element of Z_n^*. Then, $S = \{1, a, a^2, \cdots\}$ forms a subgroup of Z_n^* and the size of S is the least value of r such that $a^r = 1 \pmod n$.

- Suppose g is a generator for Z_n^*. Then g must have order $\phi(n)$.

Theorem A 4.10: Let p be an odd prime, α a positive integer. Then $\mathbb{Z}_{p^\alpha}^*$ is cyclic.

i.e., there is an element $g \in \mathbb{Z}_{p^\alpha}^*$ which generates $\mathbb{Z}_{p^\alpha}^*$ in the sense that any other element x may be written, $x = g^k \pmod{n}$ where $n = p^\alpha$, for some non-negative integer k.

PROOF

PART 1

* For a prime p, the group $\mathbb{Z}_p^*$ is cyclic.

- **Lemma 1**: Let G_1 be an abelian group.

(a) and let $a, b \in G_1$, then

$$|ab| \mid \operatorname{lcm}(|a|, |b|)$$

$$\gcd(|a|,|b|) \cdot \operatorname{lcm}(|a|,|b|) = |a| \cdot |b|$$

$\therefore$ If $|a|, |b|$ are coprime, i.e., $\gcd(|a|,|b|) = 1$

then $|ab| \mid |a||b|$

(b) Let a, b be elements of an abelian group G_1.

If $\langle a \rangle \cap \langle b \rangle = \{e\}$, then $|ab| = \operatorname{lcm}(|a|, |b|)$

Proof.

Let $|a| = m$, $|b| = n$ and let $c = \text{lcm}(m, n)$

then: $c = rm$ for some $r \in \mathbb{Z}$

$= sn$ for some $s \in \mathbb{Z}$

$\therefore (ab)^c = a^c b^c$ [$ab = ba$ and $|a|, |b|$]

$= a^{rm} b^{sn}$

$= (a^m)^r (b^n)^s$

$= e^r e^s = e$

$\Rightarrow |ab| \mid c \Longrightarrow |ab| \mid \text{lcm}(|a|, |b|)$

⑥ Let a, b be elements of an abelian group G. If $|a|$ and $|b|$ are coprime, i.e., $\gcd(|a|, |b|) = 1$. then, $|ab| = |a||b|$

[Q.C.G.T ① $H \leq G$, $K \leq G$ $\Rightarrow H \cap K \leq G$]

Proof Consider $H = \langle a \rangle \cap \langle b \rangle$ & $H \leq G$, $H \leq \langle a \rangle$, $H \leq \langle b \rangle$

Lagrange's theorem: $|G| = |G:H||H|$ (Q.C.G.T 2)

$|H| \mid |\langle a \rangle|$ and $|H| \mid |\langle b \rangle| \Rightarrow |H| \mid |a|$ and $|H| \mid |b|$

$\Rightarrow |H| \mid \gcd(|a|, |b|)$

(C.N.T ①) $c \mid a$, $c \mid b$ $\Rightarrow c \mid \gcd(a, b)$

$\gcd(|a|, |b|) = 1 \Longrightarrow |H| \mid 1 \Longrightarrow |H| = 1$

$\therefore H = \langle a \rangle \cap \langle b \rangle = \{e\}$ ⑥ $\rightarrow |ab| = \text{lcm}(|a|, |b|) = |a||b|$

- **Lemma 2:** Let G be a finite abelian group. If n is the maximal order among the elements in G, then the order of every element divides n.

R.C.G.T (2) → $|g| \mid |g|_{max}$

Method:1

Let n be the maximal order of the element of $\mathbb{Z}_p^*$.

i.e., $|g| = n$ for some $g \in \mathbb{Z}_p^*$ such that $g^n \equiv 1 \pmod{p}$.

$$|\mathbb{Z}_p^*| = \phi(p) = p-1$$

$$\Longrightarrow n \leq p-1$$

The group $\mathbb{Z}_p^*$ is cyclic iff $n = p-1$

Assume that $n < p-1$,

For the group $\mathbb{Z}_p^*$,

Lemma 2 $\longrightarrow$ $a^n \equiv 1 \pmod{p}$ for all $a \in \mathbb{Z}_p^*$

since $|q| \mid n$.

Consider the following $(p-1) \times (p-1)$ matrix,

$$A = \begin{bmatrix} 1 & 1 & 1^2 & \cdots & 1^{p-2} \\ 1 & 2 & 2^2 & \cdots & 2^{p-2} \\ \vdots & \vdots & \vdots & \ddots & \vdots \\ 1 & p-2 & (p-2)^2 & \cdots & (p-2)^{p-2} \\ 1 & p-1 & (p-1)^2 & \cdots & (p-1)^{p-2} \end{bmatrix}$$

$n < p-1^{st} \implies n \leq p-2$

and $a^n \equiv 1 \pmod{p}$ for $a = 1, 2, \cdots, p-1$

$\Rightarrow$ the column with exponent n has all entries equal to $1 \pmod{p}$, so that column matches the 1^{st} column of $A \pmod{p}$

$\therefore \det(A) \equiv 0 \pmod{p}$ ——— (1)

For a Vandermonde matrix,

$$V = \begin{bmatrix} 1 & x_1 & x_1^2 & \cdots & x_1^{n-1} \\ 1 & x_2 & x_2^2 & \cdots & x_2^{n-1} \\ \vdots & \vdots & \vdots & & \vdots \\ 1 & x_m & x_m^2 & \cdots & x_m^{n-1} \end{bmatrix}$$ such that $\det(V) = \prod_{1 \leq i < j \leq n} (x_j - x_i)$

ILA (2)

Since A is a Vandermonde matrix (where $m = n$)

$$\det(A) = \prod_{1 \leq i < j \leq p-1} (j - i)$$

The differences $j-i$ are all nonzero mod p; so their product is nonzero mod p because p is prime.

$$\therefore \det(A) \not\equiv 0 \pmod{p}.$$

But, ① states that $\det(A) \equiv 0 \pmod{p}$ if $n < p-1$ & that is a contradiction.

$$\Rightarrow \underline{\underline{n = p-1}}.$$

$n = |g| = |\langle g \rangle|$ for some $g \in \mathbb{Z}_p^*$

$\langle g \rangle$ is the smallest subgroup of $\mathbb{Z}_p^*$ containing g.

$\therefore \langle g \rangle \leq \mathbb{Z}_p^*$ such that $n = |\langle g \rangle| = |\mathbb{Z}_p^*| = p-1$

$$\Rightarrow \langle g \rangle = G$$

$\therefore G$ is cyclic

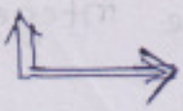
Reduction of factoring to order-finding

One of the most celebrated achievements in Quantum Algorithms was Peter Shor's algorithm to factor large numbers.

There is no known polynomial time algorithm that can factor numbers on a classical computer despite a great deal of effort.

Besides the fact that this is a fundamental mathematical problem, the hardness of factoring is the basis of certain cryptographic schemes, including RSA.

The problem of factoring numbers on a classical computer turns out to be equivalent to another problem – order-finding problem.



→ Quantum Computers are able to quickly solve the order-finding problem, & thus can factor quickly.

∴

* Suppose N is a positive integer, and x is coprime to N, $1 \leq x < N$.

The order of x modulo N is defined to be the least +ve integer r such that $x^r = 1 \pmod N$.

The order-finding problem is to determine r, given x and N.

* The order of x modulo N must divide $\phi(N)$.

Proof

Euler's theorem: $\gcd(x,N)=1 \Rightarrow x^{\phi(N)} \equiv 1 \pmod N$

$\phi(N)$: # of the integers less than N which are coprime to N.

G.C.G.T ② Let G be a group and $g \in G$ be of order n. Then $g^m = e$ for some $m \in \mathbb{N}$ iff $n \mid m$.

Lagrange's theorem: $|G| = |G:H||H|$

$|H| \mid |G|$

$|g| = |\langle g \rangle| \mid |G|$

$\therefore x^{\phi(N)} \equiv 1 \pmod N \Rightarrow r \mid \phi(N)$

The reduction of factoring to order-finding proceeds in 2 basic steps:

(i) We can compute a factor of N if we can find a non-trivial solution $x \neq \pm 1 \pmod N$ to the equation $x^2 = 1 \pmod N$.

(ii) A randomly chosen y co-prime to N is quite likely to have an order r which is even, and such that $y^{r/2} \neq \pm 1 \pmod N$, and thus $x = y^{r/2} \pmod N$ is a solution to $x^2 = 1 \pmod N$.

* **Theorem A4.11:** Suppose N is a composite number L bits long, and x is a non-trivial solution to the equation $x^2 = 1 \pmod N$ in the range $1 \le x \le N$, and neither $x = 1 \pmod N$ nor $x = N-1 = -1 \pmod N$, i.e., $x \neq \pm 1 \pmod N$. Then, at least one of $\gcd(x-1, N)$ and $\gcd(x+1, N)$ is a non-trivial factor of N that can be computed using $O(L^3)$ operations.

Proof

$$x^2 = 1 \pmod N \quad \text{and} \quad x \neq \pm 1 \pmod N$$

where $1 \le x < N$, $x, N > 0$.

$$\Rightarrow (x^2 - 1) = 0 \pmod N$$

$$\rightarrow (x-1)(x+1) = 0 \pmod N$$

$\therefore N$ divides $(x-1)(x+1)$

$x \neq \pm 1 \pmod N \longrightarrow (x \mp 1) \neq 0 \pmod N$

$\therefore$ N does not divide $(x \pm 1)$.

i.e.,
neither $(x+1)$ nor $(x-1)$ alone is a multiple of N.

$\Rightarrow$ $\gcd(x-1, N)$ and $\gcd(x+1, N)$ give non-trivial factors of N.

- The algorithm for factoring will work as follows:

- Pick x at random from $\{2, \ldots, N-1\}$
- If $\gcd(x, N) \neq 1$ then $\gcd(x, N)$ is a non-trivial divisor of N. + we're done
- Otherwise compute $r = \text{ord}(x) = |x|$

  If r is odd, start again

  If r is even, and $x^{r/2} = -1 \pmod N$, start again.

- Otherwise $x^{r/2}$ is a non-trivial square-root of $1 \Longrightarrow$ Use it to factor N.

What's the probability that one iteration of the above algorithm will succeed ?

$$\mathbb{Z}_N^* = \{ a \pmod N \mid \gcd(a, N) = 1 \}$$

—

$\mathbb{Z}_N^*$ is a group under multiplication.

# of elements in $\mathbb{Z}_N^*$ is given by the Euler function, $\phi(N)$

i.e., $|\mathbb{Z}_N^*| = \phi(N)$: # of the integers less than N which are coprime to N.

$$\phi(p) = p-1$$

$$\phi(p^\alpha) = p^\alpha\left(1-\frac{1}{p}\right) = p^{\alpha-1}(p-1)$$

$$\phi(N) = \phi(p_1^{\alpha_1}\cdots p_j^{\alpha_j}) = \phi\left(\prod_{j} p_j\right)$$

$$= \prod_j p_j^{\alpha_j}\left(1-\frac{1}{p_j}\right) = \prod_j p_j^{\alpha_j-1}(p_j-1)$$

What's the probability that an element x randomly chosen from $\mathbb{Z}_N^*$ has even order and if so satisfies $x^{r/2} \neq -1 \pmod N$??

Lemma A4.12: Let p be an odd prime. Let $2^{d'}$ be the largest power of 2 dividing $\phi(p^\alpha)$. Then with probability exactly one-half $2^{d'}$ divides the order modulo p^α of a randomly chosen element of $\mathbb{Z}_{p^\alpha}^*$.

$$x \in \mathbb{Z}_{p^\alpha}^*$$
$$\phi(p^\alpha) = 2^{d'}(\text{odd } \#)$$
$$\left.\begin{aligned} P(2^{d'} \mid |x|) &= \tfrac{1}{2} \\ P(2^{d'} \nmid |x|) &= \tfrac{1}{2} \end{aligned}\right\}$$

Proof $N = p^\alpha$ for odd prime p

$$\phi(N) = \phi(p^\alpha) = p^\alpha(p-1)$$

$\Rightarrow \phi(p^\alpha)$ is even since p is odd

$$\therefore \phi(p^\alpha) = 2^{d'}(\text{odd prime } \#)$$

for $d' \geq 1$

Theorem A4.10: Let p be an odd prime, α a positive integer. Then $\mathbb{Z}_{p^\alpha}^*$ is cyclic.

$\therefore$ The group $\mathbb{Z}_{p^\alpha}^*$ has a generator g

so an arbitrary element may be written in the form $g^k \pmod{p^\alpha}$ for some k in the range 1 through $\phi(p^\alpha)$.

$$\mathbb{Z}_{p^\alpha}^* = \left\{ g \pmod{p^\alpha}, g^2 \pmod{p^\alpha}, \ldots, g^{\phi(n)} \pmod{p^\alpha} = 1 \pmod{p^\alpha} \right\}.$$

If $g^y = 1 \pmod{N}$ then $|g| \mid y$ or $\phi(N) \mid y$

since $|g| = |\langle g \rangle| = |\mathbb{Z}_N^*| = \phi(N)$

Let's take a random element x of $\mathbb{Z}^*_{p^\alpha}$

i.e., $x = g^k \pmod{p^\alpha}$

and let r be the order of x

$$x^r = g^{kr} = 1 \pmod{p^\alpha}$$

g is the generator of $\mathbb{Z}^*_{p^\alpha}$.

$$\Rightarrow |g| = |\langle g \rangle| = |\mathbb{Z}^*_{p^\alpha}| = \phi(p^\alpha)$$

$$\therefore g^{\phi(p^\alpha)} = 1 \pmod{p^\alpha}$$

$$\therefore \phi(p^\alpha) \mid kr$$

$\phi(p^\alpha)$ divides kr evenly

$$\phi(p^\alpha) = 2^{d'} \text{ (odd prime \#)} = 2^{d'} O_1 \quad \& \quad t\,\phi(p^\alpha) = kr$$

$$\Rightarrow kr = t\,\phi(p^\alpha) = t\,2^{d'} O_1 = 2^{d'} (O_2)$$

k is odd : $\phi(p^\alpha) = p^{\alpha-1}(p-1) = 2^{d'}O_1$ is even

$\Rightarrow$ kr is even

$\Rightarrow$ r is even

$kr = t\,\phi(p^\alpha) = O_t\, 2^{d_t} 2^{d'} O_1$

$\Rightarrow r = 2^{d_t} 2^{d'}$ where $d_t \geq 0$

$\therefore \underline{2^{d'} \mid r}$.

k is even : $x \equiv g^k \pmod{p^\alpha}$ & $x^r \equiv g^{kr} \equiv 1 \pmod{p^\alpha}$

$$x^{\phi(p^\alpha)/2} = (g^k)^{\phi(p^\alpha)/2} = g^{k\phi(p^\alpha)/2} = \left(g^{\phi(p^\alpha)}\right)^{k/2} \equiv 1^{k/2} \equiv 1 \pmod{p^\alpha}$$

$\Rightarrow r \mid \phi(p^\alpha)/2$

$\Rightarrow qr = \frac{\phi(p^\alpha)}{2} = \frac{2^{d'} O_1}{2} \Rightarrow r = \frac{2^{d'} O_1}{2q} = \frac{2^{d'-d''} O_1}{q'}$

$d' - d'' < d'$

$\therefore \underline{2^{d'} \nmid r}$.

When k is odd : $2^{d'} \mid r$

$\Rightarrow$

When k is even : $2^{d'} \nmid r$

Theorem A 4.13: Suppose $N = P_1^{\alpha_1} \cdots P_m^{\alpha_m}$ is the prime factorization of an odd composite +ve integer. Let x be chosen uniformly at random from $\mathbb{Z}_N^*$, and r be the order of x modulo N. Then,

$$P\left(r \text{ is even } \& \; x^{r/2} \not\equiv -1 \pmod N\right) \geq 1 - \frac{1}{2^m}$$

$$\Updownarrow$$

$$P\left(r \text{ is odd or } x^{r/2} \equiv -1 \pmod N\right) \leq \frac{1}{2^m}$$

Proof Applying the Chinese remainder theorem,

Since $p_1^{\alpha_1}, p_2^{\alpha_2}, \ldots, p_m^{\alpha_m}$ be non-zero integers that are pairwise relatively prime i.e., $\gcd(p_i^{\alpha_i}, p_j^{\alpha_j}) = 1$ for $i \neq j$ then for all integers $a_1, a_2, \ldots, a_m$ the system of congruences

$$x = x_1 \pmod{p_1^{\alpha_1}}$$

$$x = x_2 \pmod{p_2^{\alpha_2}}$$

$$\vdots$$

$$x = x_m \pmod{p_m^{\alpha_m}}$$

has a solution & any two solutions to this system of equations are equal modulo $N = p_1^{\alpha_1} p_2^{\alpha_2} \cdots p_m^{\alpha_m}$.

i.e., $x = x' \pmod{N}$

Let $N = p_1^{\alpha_1} \cdots p_m^{\alpha_m}$,

$\Longrightarrow$ For any sequence $x_1, x_2, \ldots, x_m$ such that $0 \le x_j \le p_j^{\alpha_j} - 1$ there is exactly one $x \in \{0, \ldots, N-1\}$ such that $x_i = x \pmod{p_i^{\alpha_i}}$ for $i = 1, \ldots, m$.

This gives us an alternative way of generating a random element of $\mathbb{Z}_N^*$.

$\therefore$

By the Chinese remainder theorem, choosing x uniformly at random from $\mathbb{Z}_N^*$ is equivalent to choosing x_j independently and uniformly at random from $\mathbb{Z}_{p_j^{\alpha_j}}^*$, and requiring that $x = x_j \pmod{p_j^{\alpha_j}}$ for each j.

Let r_j be the order of x_j modulo $p_j^{\alpha_j}$ and r be the order of x modulo N.

Let 2^{d_j} be the largest power of 2 that divides r_j and 2^d be the largest power of 2 that divides r.

i.e., $r_j = 2^{d_j}(\text{odd prime \#})$ for $j = 1, 2, \ldots, m$

$r = 2^d(\text{odd prime \#})$

$x^r = 1 \pmod N$

$\rightarrow x^r = 1 + 2N$

$= 1 + 2P_1^{\alpha_1} \cdots P_j^{\alpha_j}$

$= 1 + 2^{d'} P_j^{\alpha_j}$

$= 1 \pmod{P_j^{\alpha_j}}$

Case 1 : When r is odd

$x^r = 1 \pmod N \Longrightarrow x^r = 1 \pmod{P_j^{\alpha_j}}$

$x_j = x_j \pmod{P_j^{\alpha_j}} \Longrightarrow x_j^r = x_j^r \pmod{P_j^{\alpha_j}}$

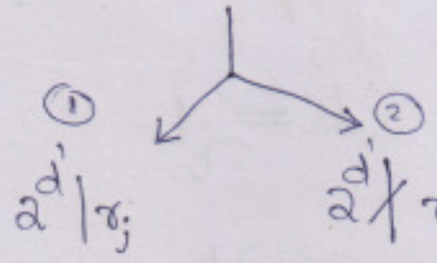
$\therefore \quad x_j^r = 1 \pmod{P_j^{\alpha_j}}$

$\Longrightarrow r_j \mid r \Longrightarrow r = t r_j$

$\therefore$ If r is odd then all r_j are odd.

Lemma A 4.1Q $\Rightarrow 2^{d'}$ divides the group $\mathbb{Z}^*_{P_j^{\alpha_j}}$

into two sets



Odd r_j does not fall in the set 1 and not all elements in set 2 have r_j odd.

$\therefore$

$$P(r_j \text{ is odd}) \leq \frac{1}{2}$$

Since the r_j are chosen independently and each r_j is odd with probability $\leq$ at most $1/2$.

$$\Longrightarrow P(r \text{ is odd}) \leq \frac{1}{2^m}$$

Case 2: When r is even & $x^{r/2} = -1 \pmod N$

$$x^{r/2} = -1 \pmod N \longrightarrow x^{r/2} = -1 \pmod{p_j^{\alpha_j}}$$

$$x_i = x_j \pmod{p_j^{\alpha_j}} \Longrightarrow x_j^{r/2} = -1 \pmod{p_j^{\alpha_j}}$$

$$\therefore \; r_j \mid r \;\; \& \;\; r_j \nmid r/2$$

As defined, $r_j = 2^{d_j}(\text{odd prime \#}) = 2^{d_j} \times O_1$

and $r = 2^{d}(\text{odd prime \#}) = 2^{d} \times O_2$

$$r_j \mid r \longrightarrow d - d_j \geq 0 \Rightarrow d \geq d_j$$

$$r_j \nmid r/2 \Longrightarrow d - 1 - d_j < 0 \Rightarrow d_j > d-1 \Rightarrow d_j \geq d$$

$$\therefore \; d_j = d \;\; \forall \; j$$

i.e., $r_j = 2^{d}(\text{odd prime \#}) = 2^{d} \times O_1$

Lemma A4.12 $\Longrightarrow$ Exactly half the elements of $\mathbb{Z}^*_{p_j^{\alpha_j}}$ have $d_j = d'$ where d' is the largest power of 2 dividing $\phi(p_j^{\alpha_j})$

i.e., $P(d_j = d') = 1/2$

$\therefore$

$P(d_j = \text{any particular value}) \leq 1/2$

Sarada 19/11/22

$\longrightarrow P(d_j = d) \leq 1/2$

When r is odd, $\cdot\ r_j / r$ for each j

$\therefore\ r_j$ is odd $\Longrightarrow d_j = 0 \quad \forall\ j = 1, 2, \cdots, k$

$\therefore$

To have r odd or $x^{r/2} = -1 \pmod N$
it is necessary that d_j takes the same value for all values of j.

$$P(d_j = \text{any particular value}) \leq 1/2$$

$\therefore$

$$P(r \text{ is odd or } x^{r/2} = -1 \pmod N) \leq \frac{1}{2^m}$$

Theorems A4.11 and A4.13 can be combined to give an algorithm which, with high probability, returns a non-trivial factor of any composite N. All the steps in the algorithm can be performed efficiently on a classical computer except (as far as known today) an order-finding subroutine which is used by this algorithm.

By repeating the algorithm we may find a complete prime factorization of N.

Algorithm

① If N is even, return the factor 2

② Use the algorithm of Exercise 5.17 to determine whether $N = a^b$ for integers $a \geq 1$ & $b \geq 2$, and if so return the factor a.

③ Randomly choose x in the range 1 to $N-1$. If $\gcd(x, N) > 1$ then return the factor $\gcd(x, N)$

④ Use the order-finding subroutine to find the order r of x modulo N.

⑤ If r is even & $x^{r/2} \neq -1 \pmod{N}$ then compute $\gcd(x^{r/2}-1, N)$ and $\gcd(x^{r/2}+1, N)$, and test to see which is a non-trivial factor, returning that factor. Otherwise, the algorithm fails.

Steps 1 and 2 of the algorithm either return a factor, or else ensure that N is an odd integer with more than one prime factor.

Step 3 either returns a factor, or produces a randomly chosen element x of $\mathbb{Z}_N^*$.

Step 4 calls the order-finding subroutine, computing the order r of x modulo N.

Step 5 completes the algorithms, since theorem A4.12 guarantees that with probability at least one-half r will be even and $x^{r/2} \neq -1 \pmod{N}$, and then theorem A4.11 guarantees that either $\gcd(x^{r/2}-1, N)$ or $\gcd(x^{r/2}+1, N)$ is a non-trivial factor of N.

Continued Fractions

- C.D. Olds

Solve the quadratic equation:

$$x^2 - 3x - 1 = 0$$

$$x^2 = 3x + 1 \implies x = 3 + \frac{1}{x}$$

$$x = 3 + \frac{1}{x} = 3 + \frac{1}{3 + \frac{1}{x}}$$

$$\implies x = 3 + \cfrac{1}{3 + \cfrac{1}{3 + \cfrac{1}{3 + \cfrac{1}{3 + \frac{1}{x}}}}}$$

The right side of the equation contains a succession of fractions, obtained by stopping at consecutive stages as:

$$3,\ 3+\frac{1}{3},\ 3+\frac{1}{3+\frac{1}{3}},\ 3+\frac{1}{3+\frac{1}{3+\frac{1}{3}}},\ \ldots$$

These numbers when converted into fractions and then into decimals, give in turn the numbers:

$$3,\ \frac{10}{3}=3.333\ldots,\ \frac{33}{10}=3.3,\ \frac{109}{33}=3.30303\ldots,$$

⇒ These numbers (or convergents) give better and better approximations to the +ve square root of the given quadratic equation.

The quadratic formula $x^2-3x-1=0$ shows that this root is equal to:

$$x=\frac{3+\sqrt{13}}{2}=3.302775\ldots$$

which when rounded to 3.303

An expression of the form

$$a_1 + \cfrac{b_1}{a_2 + \cfrac{b_2}{a_3 + \cfrac{b_3}{a_4 + \cfrac{b_4}{\ddots}}}}$$

is called a continuous fraction.

In general, the numbers $a_1, a_2, a_3, \ldots$, $b_1, b_2, b_3, \ldots$ may be any real or complex numbers, and the # of terms may be finite or infinite. Usually they are required to be integers. If $b_i = 1$ for all i the expression is called a simple continued fraction. If the expression contains finitely many terms, it is called a finite continuous fraction. If the expression contains infinitely many terms, it is called an infinite continuous fraction.

Simple continued fractions have the form

$$a_1 + \cfrac{1}{a_2 + \cfrac{1}{a_3 + \cfrac{1}{a_4 + \cfrac{1}{\ddots}}}}$$

where the 1st term a_1 is usually +ve or -ve integer (but could be zero), and where the terms $a_2, a_3, a_4, \ldots$ are +ve integers.

Finite simple continued fractions have the form:

$$a_1 + \cfrac{1}{a_2 + \cfrac{1}{a_3 + \cfrac{1}{a_4 + \ddots + \cfrac{1}{a_{n-1} + \cfrac{1}{a_n}}}}}$$

with only a finite # of terms $a_1, a_2, \ldots, a_n$. Such a fraction is called a terminating continued fraction.

The continued fraction can be denoted as:

$$[a_1, a_2, \cdots a_n] = a_1 + \frac{1}{a_2 + a_3 + \cdots + a_n}$$

The terms $a_1, a_2, \cdots, a_n$ are called the partial quotients of the continued fraction.

Examples

Ex: $$\frac{67}{29} = 2 + \cfrac{1}{3 + \cfrac{1}{4 + \frac{1}{2}}} = 2 + \frac{1}{3} + \frac{1}{4} + \frac{1}{2}$$

$$= [2, 3, 4, 2]$$

Euclid's algorithm for gcd.

$$\gcd(a, b) = \gcd(b, a \bmod b) \quad \text{or} \quad \gcd(b, r_1)$$

$$= \gcd(r_1, r_2) \cdots = \gcd(r_m, 0).$$

$67 = 2 \times 29 + 9$

$29 = 3 \times 9 + 2$

$9 = 4 \times 2 + 1$

$2 = 2 \times 1 + 0$

$$1 \overline{)2} \quad 2$$

$$29 \overline{)67} \quad 2, \ 58, \ 9$$

$$9 \overline{)29} \quad 3, \ 27, \ 2$$

$$2 \overline{)9} \quad 4, \ 8, \ 1$$

$$\frac{67}{29} = [2, 3, 4, 2] = 2 + \cfrac{1}{3 + \cfrac{1}{4 + \frac{1}{2}}}$$

$$29 \overline{)67}\ 2 = q_1$$
$$\underline{58}$$
$$9 \overline{)29}\ 3 = q_2$$
$$\underline{27}$$
$$2 \overline{)9}\ 4 = q_3$$
$$\underline{8}$$
$$1 \overline{)2}\ 2 = q_4$$
$$\underline{2}$$
$$0$$

$$\frac{67}{29} = [2, 3, 4, 2] = [q_1, q_2, q_3, q_4]$$

Ex: $\frac{29}{67} = 0 + \cfrac{1}{2 + \cfrac{1}{3 + \cfrac{1}{4 + \frac{1}{2}}}} = [0, 2, 3, 4, 2]$

$67 \overline{)29} \; 0 = q_1$

0

$29 \overline{)67} \; 2 = q_2$

58

$9 \overline{)29} \; 3 = q_3$

27

$2 \overline{)9} \; 4 = q_4$

8

$1 \overline{)2} \; 2 = q_5$

2

0

* If $p > q$ and $\frac{p}{q} = [a_1, a_2, \ldots, a_n]$

then, $\frac{q}{p} = [0, a_1, a_2, \ldots, a_n]$

Is the expansion, $\frac{67}{29} = [2,3,4,2] = [a_1, a_2, a_3, a_4]$

the only expansion of $\frac{67}{29}$ as a simple finite continued fraction ?

$$\frac{1}{a_4} = \frac{1}{2} = \frac{1}{1+\frac{1}{1}}$$

$$\therefore \quad \frac{67}{29} = [2,3,4,1,1]$$

* Every finite continued fraction ending with $a_n > 1$ has 2 forms:

(i) CF ending with $a_n > 1$, i.e., $[\ldots, a_n]$

(ii) CF ending 1, i.e., replace the final a_n by $(a_n - 1) + \frac{1}{1}$,

i.e., $[\ldots, a_n - 1, 1]$

⇒ Any rational # p/q can be expressed as a finite simple continued fraction in which the last term can be modified so as to make the # of terms in the expansion either even or odd.

Ex:- $\frac{-37}{44} = [-1, 6, 3, 2] = [-1, 6, 3, 1, 1] = [a_1, a_2, a_3, a_4, a_5]$

$$
\begin{array}{r|l}
44 & -37 \;|\; -1 \\
 & -44 \\
\hline
7 & 44 \;|\; 6 \\
 & 42 \\
\hline
2 & 7 \;|\; 3 \\
 & 6 \\
\hline
1 & 2 \;|\; 2 \\
 & 2 \\
\hline
 & 0
\end{array}
$$

Ex:- $\frac{67 \times 3}{29 \times 3} = \frac{201}{87} = \frac{67}{29} = [2, 3, 4, 2]$

$$
\begin{array}{r|l|l}
27 & 201 & 2 \\
 & 174 & \\
\hline
 & 27 & 27 \mid 3 \\
 & & 81 \\
\hline
 & & 6 \mid 27 \mid 4 \\
 & & 24 \\
\hline
 & & 3 \mid 6 \mid 2 \\
 & & 6 \\
\hline
 & & 0
\end{array}
$$

Note: If we calculated $[2, 3, 4, 2] = 2 + \frac{1}{3} + \frac{1}{4} + \frac{1}{2}$

we would get back to $\frac{67}{29}$, not to $\frac{201}{87}$.

We always obtain a rational fraction P/q in its lowest form.

* Any finite simple continued fraction represents a rational number.

Conversely,

any rational number p/q can be represented as a finite simple continued fraction.

*

Convergents & their properties

Any rational fraction P/q could be expanded into a finite simple continued fraction

$$P/q = [a_1, a_2, \ldots, a_{n-1}, a_n]$$

where a_1 is a +ve or -ve integer or zero,

where, $a_2, a_3, \ldots, a_n$ are +ve integers.

The numbers $a_1, a_2, \ldots, a_n$ are called the partial quotients or quotients of the continued fraction.

From these we can form the fractions,

$$c_1 = \frac{a_1}{1}, \quad c_2 = a_1 + \frac{1}{a_2}, \quad c_3 = a_1 + \frac{1}{a_2 + \frac{1}{a_3}}, \ldots$$

obtained, in succession, by cutting off the expansion process after the $1^{st}, 2^{nd}, 3^{rd} \ldots$ steps. These fractions are called the first, second, third, ..., convergents, respectively, of the continued fraction.

The n^{th} convergent,

$$C_n = a_1 + \frac{1}{a_2} + \frac{1}{a_3} + \cdots + \frac{1}{a_n} = [a_1, a_2, \ldots, a_n]$$

is equal to the continued fraction itself.

$$C_1 = \frac{a_1}{1} = \frac{P_1}{q_1} \quad \text{where} \quad P_1 = a_1, \; q_1 = 1.$$

$$C_2 = a_1 + \frac{1}{a_2} = \frac{a_1 a_2 + 1}{a_2} = \frac{P_2}{q_2}$$

where $P_2 = a_1 a_2 + 1$ and $q_2 = a_2$.

$$C_3 = a_1 + \frac{1}{a_2} + \frac{1}{a_3} = a_1 + \frac{a_3}{a_2 a_3 + 1}$$

$$= \frac{a_1 a_2 a_3 + a_1 + a_3}{a_2 a_3 + 1} = \frac{P_3}{q_3}$$

$$C_4 = a_1 + \frac{1}{a_2} + \frac{1}{a_3} + \frac{1}{a_4}$$

$$= \frac{a_1 a_2 a_3 a_4 + a_1 a_2 + a_1 a_4 + a_3 a_4 + 1}{a_2 a_3 a_4 + a_2 + a_4} = \frac{P_4}{q_4}$$

and so on.

Look at the convergent C_3.

$$C_3 = \frac{a_1 a_2 a_3 + a_1 + a_3}{a_2 a_3 + 1} = \frac{a_3(a_1 a_2 + 1) + a_1}{a_3(a_2) + 1}$$

$$= \frac{a_3 P_2 + P_1}{a_3 q_2 + q_1} = \frac{P_3}{q_3}$$

$\therefore$

$$P_3 = a_3 P_2 + P_1$$

$$q_3 = a_3 q_2 + q_1$$

Similarly,

$$C_4 = \frac{a_4(a_1 a_2 a_3 + a_1 + a_3) + (a_1 a_2 + 1)}{a_4(a_2 a_3 + 1) + (a_2)}$$

$$= \frac{a_4 P_3 + P_2}{a_4 q_3 + q_2} = \frac{P_4}{q_4}$$

$\therefore$

$$P_4 = a_4 P_3 + P_2$$

$$q_4 = a_4 q_3 + q_2$$

In general,

$$C_i = [a_1, a_2, \cdots, a_i] = \frac{P_i}{q_i}$$

where, $P_i = a_i P_{i-1} + P_{i-2}$

$$q_i = a_i q_{i-1} + q_{i-2}$$

Theorem 1.3

* The numerators P_i and the denominators q_i of the i^{th} convergent C_i of the continued fraction $[a_1, a_2, \ldots, a_n]$ satisfy the equations:

$$P_i = a_i P_{i-1} + P_{i-2} \qquad (i = 3, 4, 5, \ldots, n) \qquad \text{(Eq. 1.28)}$$

$$q_i = a_i q_{i-1} + q_{i-2}$$

with the initial values $P_1 = a_1$, $P_2 = a_2 a_1 + 1$, $q_1 = 1$, $q_2 = a_2$.

Proof The result is easily checked directly for the cases $i = 0, 1, 2$.

Assume that the theorem is true, or has been verified by direct calculation, for the integers $3, 4, 5 \ldots$ up to some integer k; i.e.,

$$C_j = [a_1, a_2, \ldots, a_{j-1}, a_j] = \frac{P_j}{q_j} = \frac{a_j P_{j-1} + P_{j-2}}{a_j q_{j-1} + q_{j-2}} \qquad (1.30)$$

for $j = 3, 4, \ldots, k-1, k$.

C_{k+1} differs from C_k only in having $(a_k + 1/a_{k+1})$ in place of a_k.

i.e.,

$$C_k = a_1 + \frac{1}{a_2} + \frac{1}{a_3} + \cdots + \frac{1}{a_{k-1}} + \frac{1}{a_k}$$

with

$$C_{k+1} = a_1 + \frac{1}{a_2} + \frac{1}{a_3} + \cdots + \frac{1}{\left(a_k + \frac{1}{a_{k+1}}\right)}$$

From (1.30),

$$C_k = [a_1, a_2, \ldots, a_{k-1}, a_k] = \frac{P_k}{q_k} = \frac{a_k P_{k-1} + P_{k-2}}{a_k q_{k-1} + q_{k-2}} \quad \text{— (1.32)}$$

$$P_k = a_k P_{k-1} + P_{k-2}$$

$$q_k = a_k q_{k-1} + q_{k-2}$$

The numbers P_{k-1}, q_{k-1} depend only upon the number a_{k-1} and the numbers $P_{k-2}, q_{k-2}, P_{k-3}, q_{k-3}$, all of which in turn depend upon preceding a's, p's and q's.

$\therefore$ The numbers $P_{k-2}, q_{k-2}, P_{k-1}, q_{k-1}$ depend only upon the first $k-1$ quotients $a_1, a_2, \ldots a_{k-1}$ and hence are independent of a_k.

$\Rightarrow P_{k-2}, q_{k-2}, P_{k-1}, q_{k-1}$ will not change when a_k is replaced by $\left(a_k + \frac{1}{a_{k+1}}\right)$.

$$C_{k+1} = \left[a_1, a_2, \ldots, a_{k-1}, a_k + \frac{1}{a_{k+1}}\right]$$

$$= \frac{\left(a_k + \frac{1}{a_{k+1}}\right) P_{k-1} + P_{k-2}}{\left(a_k + \frac{1}{a_{k+1}}\right) q_{k-1} + q_{k-2}}$$

Xing by q_{k+1},

$$c_{k+1} = \frac{(a_k q_{k+1} + 1) p_{k-1} + q_{k+1} p_{k-2}}{(a_k q_{k+1} + 1) q_{k-1} + q_{k+1} q_{k-2}} = \frac{a_{k+1}(a_k p_{k-1} + p_{k-2}) + p_{k-1}}{a_{k+1}(a_k q_{k-1} + q_{k-2}) + q_{k-1}}$$

From [1.32] $\quad p_k = a_k p_{k-1} + p_{k-2}$

$$q_k = a_k q_{k-1} + q_{k-2}$$

$\therefore$

$$c_{k+1} = \frac{a_{k+1} p_k + p_{k-1}}{a_{k+1} q_k + q_{k-1}} = \frac{p_{k+1}}{q_{k+1}}$$

Note: Nowhere in the proof we have used the fact that the quotients a_i are integers, although each a_i is an integer. the # $a_k + \frac{1}{a_k}$ need not be one.

Nevertheless its substitution for a_k in the proof causes no breakdown of the arguments.

$$P_i = a_i P_{i-1} + P_{i-2}$$

$$q_i = a_i q_{i-1} + q_{i-2}$$

$P_1 = a_1, q_1 = 1$; $P_2 = a_1 a_2 + 1, q_2 = a_2$

$P_2 = a_2 P_1 + P_0$ & $q_2 = a_2 q_1 + q_0$

$a_1 a_2 + 1 = a_2 a_1 + P_0$ $\quad a_2 = a_2 \cdot 1 + q_0$

$\Longrightarrow$ $P_0 = 1$ $\quad q_0 = 0$

$P_1 = a_1 P_0 + P_{-1}$ & $q_1 = a_1 q_0 + q_{-1}$

$a_1 = a_1 \cdot 1 + P_{-1}$ $\quad 1 = a_1 \cdot 0 + q_{-1}$

$P_{-1} = 0$ $\quad q_{-1} = 1$

$\therefore$ $P_0 = 1, q_0 = 0$

$P_{-1} = 0, q_{-1} = 1$

* If $P_i = a_i P_{i-1} + P_{i-2}$ and $q_i = a_i q_{i-1} + q_{i-2}$ are defined as such,

then,

$$P_i q_{i-1} - P_{i-1} q_i = (-1)^i$$

Proof.

Direct calculations show that the theorem is true for $i = 0, 1, 2$.

$i=0$: $P_0 q_{-1} - P_{-1} q_0 = 1 \cdot 1 - 0 \cdot 0 = 1 = (-1)^0$

$i=1$: $P_1 q_0 - P_0 q_1 = a_1 \cdot 0 - 1 \cdot 1 = (-1)^1$

$i=2$: $P_2 q_1 - P_1 q_2 = (a_2 a_1 + 1) \cdot 1 - a_1 a_2 = 1 = (-1)^2$

From theorem 1.3, for $i = k+1$

$P_{k+1} = a_{k+1} P_k + P_{k-1}$ & $q_{k+1} = a_{k+1} q_k + q_{k-1}$

Hence,

$$P_{k+1}q_k - P_k q_{k+1} = (a_{k+1}P_k + P_{k-1})q_k - P_k(a_{k+1}q_k + q_{k-1})$$

$$= \cancel{a_{k+1}P_k q_k} + P_{k-1}q_k - \cancel{a_{k+1}P_k q_k} - P_k q_{k-1}$$

$$= (-1)(P_k q_{k-1} - P_{k-1}q_k)$$

Assume that the theorem holds for $i=k$, i.e.,

$$P_k q_{k-1} - P_{k-1}q_k = (-1)^k.$$

$$\therefore P_{k+1}q_k - P_k q_{k+1} = (-1)(-1)^k = (-1)^{k+1}$$

$\Rightarrow$ the theorem holds for $i=k+1$ if it hold for $i=k$.

* Every convergent $c_i = \frac{P_i}{q_i}$, $i \geq 1$, of a simple continued fraction is in its lowest terms.

i.e., $\boxed{\gcd(P_i, q_i) = 1}$

Proof

$$P_i q_{i-1} - P_{i-1} q_i = (-1)^i$$

$\Rightarrow$ Any # which divides both P_i and q_i must be a divisor of $(-1)^i$.

Only divisors of $(-1)^i$ are $+1$ and -1.

$\therefore$ $+1$ and -1 are the only common divisors of P_i and q_i.

$\Longrightarrow$ $\gcd(P_i, q_i) = 1$

Dirichlet's Approximation Theorem

For each real number x and natural number n, there exists integers p and q such that $1 \leq q \leq n$ with

$$\left| x - \frac{p}{q} \right| < \frac{1}{nq} \leq \frac{1}{q^2}$$

In particular, $|qx - p| < \frac{1}{n}$

* In number theory, Dirichlet's theorem on Diophantine approximation, also called Dirichlet's approximation theorem, attempts to show that any real # has a sequence of good rational approximations.

Proof

Let x be any real # and n be a +ve integer.

Define α_k so that $kx = \alpha_k \pmod 1$

$\therefore$ $kx = m_k + \alpha_k$ $\forall$ $k = 0, 1, 1, \ldots, n$

such that $m_k \in \mathbb{Z}$ and $\alpha_k \in [0, 1)$

One can divide the interval $[0, 1)$ into n smaller intervals of measure $1/n$.

$\therefore$ We have $n+1$ number of α_k and n intervals.

The Pigeonhole principle $\Rightarrow$ At least two of x_k's are in the same interval. say x_i and x_j with $i<j$.

$\Leftrightarrow$

$\therefore$ There are distinct i & j in the range $0, 1, \ldots, n$ such that $|x_j - x_i| < 1/n$

$$|(j-i)\alpha - (m_j - m_i)| = |j\alpha - m_j - (i\alpha - m_i)| = |x_j - x_i| < \frac{1}{n}$$

Dividing both sides by $j-i$ will result in :

$$\left|\alpha - \frac{m_j - m_i}{j-i}\right| < \frac{1}{(j-i)n} \leq \frac{1}{(j-i)^2}$$

* For each real number x and natural number n, there exists integers p and q with $1 \leq q \leq n$ and $\gcd(p, q) = 1$ such that,

$$|qx - p| \leq \frac{1}{n} \quad \text{(or)} \quad \left|x - \frac{p}{q}\right| \leq \frac{1}{nq}$$

Proof.

Last theorem proves that there exists p & q such that $\left|x - \frac{p}{q}\right| < \frac{1}{nq}$.

Once such are p, q have been found, then a coprime pair can be found by dividing numerator and denominator of p/q by $\gcd(p, q)$.

say, $p' = p/\gcd(p,q)$ and $q' = \frac{q}{\gcd(p,q)}$

$\gcd(ma, mb) = m \gcd(a,b)$

$\therefore \gcd(p', q') = \frac{1}{\gcd(p,q)} \gcd(p,q) = 1$