CRYPTOGRAPHY AND ENCRYPTION: EUCLID'S GCD ALGORITHM

ADESHOLA, A. D.
ALIU, T.

Abstract

There is a strong need to devise new encryption mechanisms (algorithms) that offer enhanced security assurance, and guarantee the security of information transmitted over computer networks. This has generated a lot of interest, and has made cryptography an area of interest in research all over the world today. In this study, we study Cryptography through the Euclid's GCD Algorithm Principle.

Keywords: Cryptography, encryption, divisor and algorithm..

INTRODUCTION

Cryptography is the "study of ways to disguise messages so as to avert unauthorized interception". This arises from the desire for private communication, a trait which has been in humans from earlier times. Both in times of war and in moments of peace, Cryptograph and Encryption play strategic role in the operations of the military and civilian intelligence formations. Today, because of the pervasive influence of the internet and the general preponderance of global comport and communication networks as the major infrastructure for information dissemination in the network (knowledge) society, concern for the security of data and information transmitted over various networks has increased tremendously.

PRELIMINARIES

Division: Let d and a be integers. We say that d divides a if there exists an integer k such that $a = kd$ In this case, we also say that d is a divisor of a and that a is a multiple of d. The notation $d \mid a$ is used to denote that d divides a. If $d \mid a$, then so does $(-d) \mid a$. A divisor of a is at least 1 and at most $|a|$.

ADESHOLA, A. D. and **ALIU, T.** are Lecturers at the Department of Mathematics, Kwara State University, Malete, Nigeria.

International Journal of Engineering and Technical Mathematics Vol.3, No.1 & 2
© 2010 by The Development Universal Consortia. All Rights Reserved.

Example: The divisors of 24 are 1, 2, 3, 4, 6, 8, 12, and 24.

An integer is $p = z$ called a prime if it is divisible only by 1 and itself (that is it has no factors). For two integers a and b and for any positive integer n, if $n \mid (a-b)$ (that is, $a \bmod n = b \bmod n$, which means that a and b have the same residue modulo n), then we say that a is congruent to b modulo n, and we write $a = b \pmod{n}$. For any positive integer n, the integers can be divided into n equivalence classes according to their residues modulo n:

$$[a]_n = \{a + kn : k \in Z\}$$

While the collection of all the n equivalence classes of the residues modulo n is called Z_n:

$$Z_n = \{[a]_n : 0 \le a \le n\text{-}1\}.$$

Common Divisors

If d is a divisor of a and d is also a divisor of b, then d is called a common divisor of a and b. The greatest common divisor of two integers a and b, not both zero, is the largest of the common divisors of a and b, and it is denoted by $\gcd(a,b)$.

Examples : $\gcd(24, 30) = 6$
$\gcd(15, 7) = 1$
$\gcd(81, 18) = 9$

GCD Characterization Theorem

If a and b are any integers, not both zero, then $\gcd(a, b)$ is the smallest positive element of the set $LC(a, b) = \{ax + by: x, y \in Z\}$ of linear combinations of a and b.

Proof

Let s be the smallest positive element of the set $LC(a, b)$. Also let $s = ax + by$ for some x, y $\in$ Z and let the unique residual representation of a modulo s be $a = qs + r$,

Then,

$$\begin{aligned} a \bmod s &= r \\ &= a - qs \\ &= a - q(ax + by) \\ &= a(1 - qx) + b(-qy) \end{aligned}$$

so - $(a \bmod s)$

Is also in the set $LC(a, b)$.

However, since $(a \bmod s) < s$, we must have $(a \bmod s) = 0$

Therefore $-s \mid a$.

Similarly $-s \mid b$.

Therefore, s is a common divisor of a and b.

Therefore, we must have $s \leq \gcd(a, b)$.

However, in general – since $\gcd(a, b) \mid b$ -we must have that $\gcd(a, b) \mid a$ (since a is a linear combination of a and b).

Now, if $\gcd(a, b) \mid s$ and $s > 0$, then we must have that $\gcd(a, b) \leq s$. We now have $s \leq \gcd(a, b)$ and $s \leq \gcd(a, b) \leq s$. This implies that $\gcd(a, b) - s$. Therefore, the greatest common divisor of a and b is the smallest positive linear combination of a and b.

Corollary: For any integers a and b, if $d \mid a$ and $d \mid b$ then $d \mid \gcd(a, b)$.

Proof

According to the GCD Characterization Theorem, $\gcd(a, b)$ is a linear combination of a and b. And – any common divisor d of a and b must also divide every linear combination of a and b.

Corollary: For any integers a and b and any nonnegative integer n, we have $\gcd(an, bn) = n \gcd(a, b)$.

If $n = 0$, the corollary is true. If $n > 0$, then $\gcd(an, bn)$ is the smallest positive element of the set $\{anx + bny\}$, which is n times the smallest positive element of the set $\{ax + by\}$.

Fundamental Theorem of Arithmetic

For all positive integers d, a, and b, if $d \mid ab$ and $\gcd(a, b) = 1$, then $(d \mid b)$.

Proof

Since $d \mid ab$, there exists integer k such that $ab = kd$. Also since $\gcd(a, b) = 1$, there exists integer x and y such that $ax + dy = 1$. By manipulating, we get $b = (kx + yb)d$, which implies that $d \mid b$.

Theorem

For any integers a, b, and p, for both $\gcd(a, p) = 1$ and $\gcd(b, p) = 1$, $\gcd(ab, p) = 1$.

Proof

By the GCD Characterization Theorem, there exist x, x', y, y', such $ax + py = 1$ and $bx' + py' = 1$. Also by multiplying, we $ab(xx') + p(ybx' + y'ax + pyy') = 1$. This linear combination of ab and p im that $\gcd(ab, p) = 1$.

Theorem

For all prime p and all integers a and b, if $p \mid ab$, then $p \mid a$ or $p \mid b$ (or both).

Proof

Assume that p divides ab, but p does not divide a and p does not divide b. Sir is prime, its only divisors are 1 and p. Thus, $\gcd(a, p) = 1$ and $\gcd(b, p) = 1$. by $\gcd(ab, p) = 1$, which contracts the assumption that p divides ab.

Euclid's GCD Algorithm

Greek Mathematician and author of one of the most famous text in whole of Mathematics, *Stoicheion or Elements.* In 13 books it cover the geom of the triangle, the circle, various quadrilaterals, Eudoxus' theory of propor elementary number theory, irrationals, and solid geometry. Important re established include the infinity of the primes (*IX*: 20), the fundamental theore arithmetic Pythagoras' theorem (*I* :47), the Euclidean algorithm (*Bk: VII*), existence of irrational numbers (*Bk* :X), and the construction of the five Plat solids (*Bk :VIII*).

Euclid's Algorithm

Euclid's (a, b)

```
1   if (b = 0)
2   then return a
3   else return Euclid (b, (a mod b))
```

Example:

Euclid (30, 21) =
Euclid (21, 9) =
Euclid (9, 3) =
Euclid (3, 0) =

Extended Euclid's Algorithm

Euclid's Algorithm can be extended to compute the coefficients x and y, such that $d = \gcd(a, b) = ax + by$.

Extended-Euclid (a, b)

1 **if** $(b = 0)$
2 **then return** $(a, 1, 0)$
3 $(d', x', y') \leftarrow$ Extended-Euclid $(b, (a \bmod b))$
4 $(d, x, y) \leftarrow (d', y', x' - \lfloor a/b \rfloor y')$
5 **Return** (d, x, y)

RESULTS AND DISCUSSION OF EXTENDED EUCLID'S GCD ALGORITHM

Table 1: Extended Euclid's Algorithm

a	b	$\lfloor a/b \rfloor$	d	x	y
99	78	1	3	-11	14
78	21	3	3	3	-11
21	15	1	3	-2	3
15	6	2	3	1	-2
6	3	2	3	0	1
3	0	-	3	1	0

Line 1 of Extended-Euclid is identical to line 1 of Euclid. If $b = 0$, then line 2 of Extended-Euclid returns the following values (which solve the linear combination $\gcd(a, b) = ax + by$):

a as the value of the $\gcd(a, b)$
1 as the value of the coefficient x, and
0 as the value of the coefficient y

If $b \neq 0$, then, in Line 3, Extended-Euclid first computes the values (d', x', y') of such that :

$d' = \gcd(b, (a \bmod b))$ and

$d' = bx' + (a \bmod b)y'$.

In Line 4, after returning from the recursive call, 3, Extended-Euclid set:

$d = \gcd(a, b) = \gcd(b, (a \bmod b)) = d'$

To obtain x and y such that $d = ax + by$, we notice that

$$\begin{aligned} d = d' &= bx' + (a \bmod b)y' \\ &= bx' + (a - \lfloor a/b \rfloor b)y' \\ &= ay' + b(x' - \lfloor a/b \rfloor y') \end{aligned}$$

Now, the selection of $x = y'$ and $y = x' - \lfloor a/b \rfloor y'$, satisfies the equation $d = ax + by$.

Line 5 of Extended-Euclid returns the values computed for d, x, and y. The running time of Extended-Euclid is the same order of magnitude as the Euclid.

CONCLUSION

Encryption/decryption is especially important in wireless communications. This is because wireless circuits are easier to tap than their hard – wired counterparts. Nevertheless, encryption/decryption is a good idea when carrying out any kind of sensitive transaction, such as a credit – card purchase online, or the discussion of a company secret between different departments in the organization.

REFERENCES

Adeshola, A. D.; Makanjuola, S. O. & Kehinde, R. (2008). Semigroups in Automata. *International Journal of Engineering and Technical Mathematics, Vol. I : 208-213.*

Adeshola, A. D. (2007). *Syntax Recognition in Formal Languages and Automata Theory using Free Semigroups.* M.Sc. Dissertation, Unilorin.

Bruce, S. (1996). *Applied Cryptography: Protocols, Algorithms, and Source Code in C*, 2-nd edition, John Wiley & Sons.

Charlie, K., Radia, P. & Mike, S. (2002). *Network Security: Private Communication in a Public World,* (2nd edition) Prentice Hall.

David, N. (1998). *Penguin Dictionary of Mathematics.* England: Penguin Books Ltd.,

Douglas, R. S. (2003). *Cryptography: Theory and Practice*. Chapman and Hall.

Falaki, S. O. & Alese, B. K. (2007). *Research Oriented Course in Cryptography and Encryption Algorithms.* Abuja: National Mathematical Centre.

Howie, J. M. (1991). *Automata & Languages.* Oxford: Oxford University Press.

William, S. (2004). *Computer Networking with Internet Protocols and Technology.* 550pp.

William, S. (2003). *Cryptography and Network Security: Principles and Practice,* (3rd edition) Prentice Hall.

BANDWIDTH SELECTION AND DENSITY ESTIMATION B REGULATION MATRIX

JIMOH KILANI

Abstract

This study continues Golubev and Hardle. (2001) concentrating on data driven choice of smoothing parameters for penalized least-square estimators. Our consideration is based on the so-called orthogonal approach. The corner stone idea of this approach is to parameterize the functional class $W_\beta^2(L)$. *We do this by constructing an orthonormal system in the Hilbert space* $L_q^2[0,1]$ *which is equipped with the norm* $\square.\square_q$ *and with the inner product* $<.,.>_q$.

INTRODUCTION

There is a vast mathematical literature on data driven choice of smooth parameters (see Efriomovich and Pinsker (1984), Lepski (1991), Lepski (19 Golubev and Nussbaun (1992), Kneip (1994), Lepski and Spokiony (19 Nemirovskii (1998), Tsybakov (1998) among others). Thus we see that the opti regularization matrix strongly depends on the functional class $W_\beta^2(L)$. In prac the parameter L is hardly known. Therefore there is need to construct a practic feasible data-driven method for adaptive penalization. The goal of matrix base the observation is to choose the regulation to minimize the covariance matrix. In this paper we will deal with partial linear model.

$$Y_i = \theta^T Z_i + m(X_i) + \xi_i, \quad i = 1,2,...,n \qquad \text{---------- (1)}$$

Where $\theta \in R^d$ is a vector of unknown parameters, ξ_i are random variables w zero mean and the finite variance $\delta^2 = E\xi_i^2$. The regressors $X_i \in [0,1]$ assumed to be random variables with a strictly positive density $q(x)$ on $[0,$ We shall also make an assumption that they do not depend on ξ_i. The nuisanc

JIMOH KILANI *is a former Lecturer at the Department of Mathematics, Adeyemi College of Educa Ondo, Nigeria.*

International Journal of Engineering and Technical Mathematics Vol.3, No.1
© 2010 by The Development Universal Consortia. All Rights Reserved.