MINI PROJECT

18th May 2020

Damayanti R Sambhe(180123010)
Shivam Kumaar Arya(180123044)
Indian Institute of Technology, Guwahati
Department of Mathematics

AIM

To analyze the conditions for the existence of the Euclidean Algorithm, explore the uniqueness of the Greatest Common Divisors including the study of the examples for the related.

BACKGROUND

Euclid's algorithm is an efficient method for computing the greatest common divisor (GCD) of two integers. Euclid first described the algorithm in his Elements (c. 300 BC). The algorithm never takes more steps than five times the number of digits (base 10) of the smaller integer. This was proven by Gabriel Lamé in 1844 and is, in fact, one of the first results in computational complexity theory.

This algorithm has many theoretical and practical applications. It is frequently used in everyday algebra for reducing fractions and division in modular arithmetic. Computations using this algorithm form part of the cryptographic protocols used in secure internet communication, and in methods for breaking these cryptosystems by factoring large composite numbers.

In this report, we will explore the generalization of Euclid's algorithm to integral domains. Specifically, we will look at the conditions for the existence of such a procedure within the domain, if it exists then, the properties of the results, and, finally, look at some concrete examples.

1. Introduction

Definition 1. An integral domain R is called ***Euclidean*** if there is a function $|\cdot| : R-\{0\} \to N$ such that R has division with the remainder with respect to $|\cdot|$ for all a and b in R with $b \neq 0$, *i.e.* we can find q and r in R such that,

$$a = bq+r, \qquad r = 0 \text{ or } |r| < |b|$$

Examples of Euclidean domains are Z (with $|n| = |n|$, The usual modulus), F[x] for a field F (with $|f| = \deg(f)$, and Z[i] ($|\alpha| = N(\alpha)$, The square of the norm in ***C***).

The Euclidean Algorithm is as follows:-

Input: *a, b ∈ Q, b≠0*

Output: *The GCD of a and b.*

Pseudocode:

```
while b≠0
    a=b
    b=a mod b
return a
```

We now show that such an algorithm will always terminate and return (one of) the correct GCD(s) in a Euclidean Domain.

Consider Q a Euclidean Domain with $|\cdot| : Q^* \rightarrow N$ such that for $a \in Q, b \in Q^*$ there exists $q, r \in Q$ such that,

$$a = bq+r, \qquad r = 0 \text{ or } |r| < |b|$$

Clearly since $|r|$ keeps on decreasing it means that termination is guaranteed in atmost b steps.

Now, consider $< a, b >= \{ax + by | x, y \in Q\}$. It is obvious that if $c, d \in < a, b >$ then $< c, d > \subseteq < a, b >$.

Lemma: If $b \neq 0$ *then* $< a, b > \ = \ < b, a \bmod b >$.

Proof: We know that $\exists \ q, r$ *such that,*

$$a = bq+r, \qquad r = 0 \text{ or } |r| < |b|$$

$$\Rightarrow r = a - qb \Rightarrow r \in \ < a, b > \ \Rightarrow \ < r, b > \ \subseteq \ < a, b > \qquad 4.1$$

Also,

$$a = bq + r \Rightarrow a \in \ < r, b > \ \Rightarrow \ < a, b > \ \subseteq \ < r, b > \qquad 4.2$$

From 4.1 and 4.2, it follows,

$$< a, b > \ = \ < r, b >$$

Therefore, the ideal formed by *a* and *b* in each iteration is invariant over each loop iteration.

Now, suppose the algorithm returns g,

$$\Rightarrow \ <a,b> \ = \ <g,0>$$

$\Rightarrow$ *a and b* are multiples of *g, i.e g* is a common divisor.

Also,

$$g \in \ <a,b> \ \Rightarrow g = ax + by$$

$\Rightarrow g$ is divided by all other common divisors of *a* and *b.*

$$\Rightarrow g = gcd(a,b).$$

Hence we prove that if an Integral Domain is Euclidean then there exists a corresponding Euclidean Algorithm to it. Note that it is possible that multiple GCDs exist, we will see such examples.

2.CONSTRUCTION

In this section we will look at the necessary and sufficient condition for an integral domain to be Euclidean. Briefly, we will look at a method to construct the

For any $S \subset Q$,

$$\text{B} = \{b \mid \exists \ a{\in}Q, \ s.t \ \ a + bQ \ \subseteq S \ , \ b{\in}Q\}$$

Then B is the total derived set of S, and we denote $B \cap S \ = \ S'$.

Let Q be an Integral Domain such that P $\subset Q^*$ and P is ideal in Q.

Further, suppose that Q is Euclidean which means that there exists some function $|\cdot| : Q^* \rightarrow \mathbb{N}$ such that,

b | a $\Rightarrow$ $|b| \leq |a|$ *and if b does not divide a* $\Rightarrow \exists q,r \in Q \ st \ a = bq + r, |r|$ <|b|.

Now consider, $P_i = \{b \mid |b| \geq i\}$, clearly P_i *is an ideal of* Q.

Consider some b in P_i', let $a \in Q$ be such that

$$a + bQ \subset P_i.$$

There must exist some $q,r \in Q$ such that $a = bq + r$, and $|r| < |b|$ but

$$r = a - bq \Rightarrow r \in P_i \Rightarrow |r| \geq i$$

Therefore,

$$|b| \geq i + 1 \Rightarrow b \in P_{i+1} \Rightarrow P_i' \subseteq P_{i+1}.$$

Conversely, if we are able to produce a sequence $Q^* = P_0 \supseteq P_1 \supseteq P_2 \ldots$ of product ideals of Q such that

i) $\cap P_i$ *is empty*

ii) $P_i^{'} \subseteq P_{i+1}$

Then the norm which is defined as |b| = i for every b in $P_i - P_{i+1}$ will be suitable to give a Euclidean Algorithm.

Therefore, there is a one-one correspondence between sequences of this kind and Euclidean Algorithms.

If for another Euclidean Algorithm, with the corresponding sequence $\overline{P}_i$, satisfying $P_i \subseteq \overline{P_i}$ we say that the first algorithm is faster (in the sense that it will take fewer steps to terminate).

If there exists a Euclidean Algorithm at all then there exists a *fastest* algorithm which corresponds to the sequence $Q^* = P_0 \supseteq P_0^{'} \supseteq P_0^{''} \ldots$

Therefore the emptiness of the intersection $\cap P_0^{(i)}$ is a *necessary and sufficient condition* for the existence of a Euclidean Algorithm within an integral domain.

3. UNIQUENESS IN EUCLID'S ALGORITHM

The following is the condition under which Euclid's algorithm will return a unique result. Note that Euclid's algorithm will return a unique answer iff division algorithm will return unique answers.

Theorem: Quotient and remainder are unique iff $|a+b| \leq max(|a|, |b|)$.

Proof:

If $a \neq 0 \neq b$ are such that $|a+b| > max(|a|, |b|)$,then

$$b = 0(a+b) + b \qquad |b| < |a+b|$$

$$b = 1(a+b) - a \qquad |a| < |a+b|$$

This contradicts uniqueness.

If the inequality holds and

$$a = bq + r, \qquad r = 0 \; or \; |r| < |b|$$

$$= bq' + r', \quad r' = 0 \text{ or } |r'| < g(b)$$

With $r \neq r'$ *and* $q \neq q'$,then

$$g(b) \leq g((q - q')b) = g(r' - r) < g(b).$$

Thus $r = r'$ *and* $q = q'$.

Since either of the ones implies other uniqueness holds iff the given condition holds true.

4.EXAMPLES

A] Integers:

The division algorithm for Z: If a, $b \in \mathbf{Z}$ with $b \neq 0$ then $\exists$ $q, r \in \mathbf{Z}$ such that $a = bq + r$ with $|r| < |b|$.The element q is called the *quotient* and r is the *remainder*.

The **greatest common divisor** (or **highest common factor**) of two integers a, $b \in \mathbf{Z}$ is an integer of largest modulus which divides them both. Note that GCD will be determined only upto multiplication with ±1. We can also check that $|a + b| \leq max(|a|, |b|)$ does not hold in this domain.

B] Polynomials:

The division algorithm for R[x]: If $a(x)$, $b(x) \in \mathbf{R}[x]$ with $b(x) \neq 0$ then $\exists$ $q(x)$, $r(x) \in \mathbf{R}[x]$ such that $a(x) = b(x)q(x) + r(x)$ with either $r(x) = 0$ or $deg(r(x)) < deg(b(x))$.

The **greatest common divisor** of two polynomials $a(x)$, $b(x) \in \mathbf{R}[x]$ is a polynomial of the highest degree which divides them both. The uniqueness condition holds which means that the result will be unique

C] Gaussian Integers:

The ring of **Gaussian integers** is the subring $\{a + bi \mid a, b \in \mathbf{Z}\}$ of $\mathbf{C}$. It is denoted $\mathbf{Z}[i]$.

The division algorithm for Z[i]: If $u, v \in \mathbf{Z}[i]$ with $v \neq 0$ then $\exists\ q, r \in \mathbf{Z}[i]$ such that $u = vq + r$ with $N(r) < N(v)$.

The **greatest common divisor** of two Gaussian integers $u, v \in \mathbf{Z}[i]$ is a Gaussian integer of the largest norm which divides them both. Note that the GCD will be determined only upto multiplication with ±1 and $\pm i$. It is immediately obvious that the condition for uniqueness will not hold.

References

[1]Jodeit, M. A. "Uniqueness in the Division Algorithm." The American Mathematical Monthly, vol. 74, no. 7, 1967, pp. 835–836. JSTOR, https://www.jstor.org/stable/i314988.
[2] Motzkin, Th. The Euclidean algorithm. Bull. Amer. Math. Soc. 55 (1949), no. 12, 1142--1146.,https://projecteuclid.org/euclid.bams/1183514381.
[3] Keith Conrad, "Remarks about Euclidean Domains", University of Connecticut, https://kconrad.math.uconn.edu/blurbs/ringtheory/euclideanrk.pdf.