The Euclidean Algorithm

Alexander Speigle

August 28, 2024

Outline

Rings and Ring Norms

Define $(R, +, \cdot)$ as a ring

Rings and Ring Norms

Define $(R, +, \cdot)$ as a ring

- (R, +) is a abelian group and
- a$\cdot b \in R$
- a$\cdot(b + c) = a \cdot b + a \cdot c$
- (a + b)$\cdot c = a \cdot c + b \cdot c$

Rings and Ring Norms

Define $(R, +, \cdot)$ as a ring

- (R, +) is a abelian group and
- a$\cdot b \in R$
- a$\cdot(b + c) = a \cdot b + a \cdot c$
- (a + b)$\cdot c = a \cdot c + b \cdot c$

Define $N : R \to \mathbb{Z}^+ \cup \{0\}$ such that $N(0) = 0$ as a ring norm

Rings and Ring Norms

Define $(R, +, \cdot)$ as a ring

- (R, +) is a abelian group and
- a$\cdot b \in R$
- a$\cdot(b + c) = a \cdot b + a \cdot c$
- (a + b)$\cdot c = a \cdot c + b \cdot c$

Define $N : R \to \mathbb{Z}^+ \cup \{0\}$ such that $N(0) = 0$ as a ring norm

$$\begin{aligned} N : \mathbb{Z} &\to \mathbb{Z}^+ \cup \{0\} \\ n &\mapsto |n| \end{aligned}$$

Rings and Ring Norms

Define $(R, +, \cdot)$ as a ring

- (R, +) is a abelian group and
- a$\cdot b \in R$
- a$\cdot(b + c) = a \cdot b + a \cdot c$
- (a + b)$\cdot c = a \cdot c + b \cdot c$

Define $N : R \to \mathbb{Z}^+ \cup \{0\}$ such that $N(0) = 0$ as a ring norm

$$\begin{aligned} N : \mathbb{Z} &\to \mathbb{Z}^+ \cup \{0\} \\ n &\mapsto |n| \end{aligned}$$

$$\begin{aligned} N : \mathbb{Z} &\to \mathbb{Z}^+ \cup \{0\} \\ n &\mapsto \begin{cases} 0 & n = 2k \\ 1 & n = 2k + 1 \end{cases} \end{aligned}$$

Greatest Common Divisor

Given two elements of a ring a and b define the GCD of a and b to be the element d such that

Greatest Common Divisor

Given two elements of a ring a and b define the GCD of a and b to be the element d such that

$$\begin{aligned} d|a \quad &\text{and} \quad d|b \\ d'|a \quad &\text{and} \quad d'|b \implies d'|d \end{aligned}$$

Greatest Common Divisor

Given two elements of a ring a and b define the GCD of a and b to be the element d such that

$$\begin{aligned} d|a \quad &\text{and} \quad d|b \\ d'|a \quad &\text{and} \quad d'|b \implies d'|d \end{aligned}$$

$$60 : \{1, 2, 3, 4, 5, 6, 10, 15, 20, 30\}$$

$$45 : \{1, 3, 5, 9, 15\}$$

Greatest Common Divisor

Given two elements of a ring a and b define the GCD of a and b to be the element d such that

$$
\begin{aligned}
&d|a \quad \text{and} \quad d|b \\
&d'|a \quad \text{and} \quad d'|b \implies d'|d
\end{aligned}
$$

$$60 : \{1, 2, 3, 4, 5, 6, 10, 15, 20, 30\}$$

$$45 : \{1, 3, 5, 9, 15\}$$

$$\gcd(60, 45) = 15$$

Euclidean Domains

Define $(R, +, \cdot)$ as a Euclidean domain

Euclidean Domains

Define $(R, +, \cdot)$ as a Euclidean domain

- $(R, +, \cdot)$ is a ring with norm N

Euclidean Domains

Define $(R, +, \cdot)$ as a Euclidean domain

- $(R, +, \cdot)$ is a ring with norm N
- $\forall a, b \in R, \exists q, r \in R$ such that

Euclidean Domains

Define $(R, +, \cdot)$ as a Euclidean domain

- $(R, +, \cdot)$ is a ring with norm N
- $\forall a, b \in R, \exists q, r \in R$ such that
- $a = q \cdot b + r$ with $r = 0$ or $N(r) < N(b)$

Example Euclidean Domains

$\mathbb{Z}, \mathbb{Z}[\mathrm{i}], \mathbb{Z}[x]$ are examples of rings with a division algorithm

$$\mathbb{Z}[\mathrm{i}] = \{a + b\mathrm{i} : a, b \in \mathbb{Z}\}$$

$$\mathbb{Z}[x] = \{\sum_0^n a_n x^n : a_n \in \mathbb{Z}, n \in \mathbb{Z}^+\}$$

Euclidean Algorithm

Theorem

The greatest common divisor between two ring elements is the last nonzero remainder of the following

Euclidean Algorithm

Theorem

The greatest common divisor between two ring elements is the last nonzero remainder of the following

- $a = q_1 b + r_1$

Euclidean Algorithm

Theorem

The greatest common divisor between two ring elements is the last nonzero remainder of the following

- $a = q_1 b + r_1$
- $b = q_2 r_1 + r_2$

Euclidean Algorithm

Theorem

The greatest common divisor between two ring elements is the last nonzero remainder of the following

- $a = q_1 b + r_1$
- $b = q_2 r_1 + r_2$
- $\vdots$
- $r_{n-1} = r_n$

This sequence of r_n terminates after finite iterations

Euclidean Algorithm

Theorem

The greatest common divisor between two ring elements is the last nonzero remainder of the following

- $a = q_1 b + r_1$
- $b = q_2 r_1 + r_2$
- $\vdots$
- $r_{n-1} = r_n$

This sequence of r_n terminates after finite iterations

$$(a, b) = (b, r_1) = (r_1, r_2) = \cdots = (r_{n-1}, r_n)$$

GCD in $\mathbb{Z}$

$\mathbb{Z}$ equipped with the ring norm $N : \mathbb{Z} \to \mathbb{Z}^+ \cup \{0\}$ defined as $N(m) = |m|$

Find the GCD of 35 and 21

GCD in $\mathbb{Z}$

$\mathbb{Z}$ equipped with the ring norm $N : \mathbb{Z} \to \mathbb{Z}^+ \cup \{0\}$ defined as $N(m) = |m|$

Find the GCD of 35 and 21

$$35 = 1 \cdot 21 + 14$$
$$21 = 1 \cdot 14 + 7$$
$$14 = 2 \cdot 7 + 0$$

GCD in $\mathbb{Z}$

$\mathbb{Z}$ equipped with the ring norm $N : \mathbb{Z} \to \mathbb{Z}^+ \cup \{0\}$ defined as $N(m) = |m|$

Find the GCD of 35 and 21

$$35 = 1 \cdot 21 + 14$$
$$21 = 1 \cdot 14 + 7$$
$$14 = 2 \cdot 7 + 0$$

$$35 = 2 \cdot 21 - 7$$
$$21 = -3 \cdot -7 + 0$$

GCD in $\mathbb{Z}[\mathrm{i}]$

$\mathbb{Z}[\mathrm{i}]$ equipped with the ring norm $N : \mathbb{Z}[\mathrm{i}] \to \mathbb{Z}^{+} \cup \{0\}$ defined as $N(a + b\mathrm{i}) = a^2 + b^2$

Find the GCD of $2 + 3\mathrm{i}$ and $8 + 6\mathrm{i}$

GCD in $\mathbb{Z}[\mathrm{i}]$

$\mathbb{Z}[\mathrm{i}]$ equipped with the ring norm $N : \mathbb{Z}[\mathrm{i}] \to \mathbb{Z}^+ \cup \{0\}$ defined as $N(a + b\mathrm{i}) = a^2 + b^2$

Find the GCD of $2 + 3\mathrm{i}$ and $8 + 6\mathrm{i}$

$$\begin{aligned} 8 + 6\mathrm{i} &= (3 - \mathrm{i}) \cdot (2 + 3\mathrm{i}) - 1 - \mathrm{i} \\ 2 + 3\mathrm{i} &= -2 \cdot (-1 - \mathrm{i}) + \mathrm{i} \\ -1 - \mathrm{i} &= (-1 + \mathrm{i}) \cdot \mathrm{i} + 0 \end{aligned}$$

Topological Relationships and Minimal Norms

Let R be a ring and $N : R \to \mathbb{Z}^+ \cup \{0\}$ be a ring norm with the added condition that it defines distance. The ring R is a Euclidean domain if

$$\forall a, b \in R, \exists q, r \in R \text{ such that}$$
$$a = q \cdot b + r \text{ with } r = 0 \text{ or } N(r) < N(b)$$

Topological Relationships and Minimal Norms

Let R be a ring and $N : R \to \mathbb{Z}^+ \cup \{0\}$ be a ring norm with the added condition that it defines distance. The ring R is a Euclidean domain if

$$\forall a, b \in R, \exists q, r \in R \text{ such that}$$
$$a = q \cdot b + r \text{ with } r = 0 \text{ or } N(r) < N(b)$$

$$a - q \cdot b = r$$

Topological Relationships and Minimal Norms

Let R be a ring and $N : R \to \mathbb{Z}^+ \cup \{0\}$ be a ring norm with the added condition that it defines distance. The ring R is a Euclidean domain if

$$\begin{aligned}&\forall a, b \in R, \exists q, r \in R \text{ such that}\\ &a = q \cdot b + r \text{ with } r = 0 \text{ or } N(r) < N(b)\end{aligned}$$

$$a - q \cdot b = r$$

$$\|r\| < \|b\|$$

Topological Relationships and Minimal Norms

Let R be a ring and $N : R \to \mathbb{Z}^+ \cup \{0\}$ be a ring norm with the added condition that it defines distance. The ring R is a Euclidean domain if

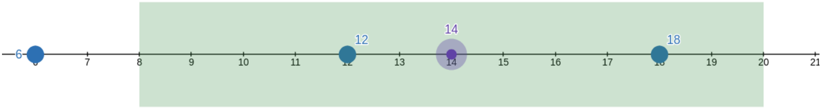
$$\forall a, b \in R, \exists q, r \in R \text{ such that}$$
$$a = q \cdot b + r \text{ with } r = 0 \text{ or } N(r) < N(b)$$

$$a - q \cdot b = r$$

$$\|r\| < \|b\|$$

$$\|q \cdot b - a\| < \|b\|$$

Topological Relationships and Minimal Norms



Integer Worst Case

For any $b < a \in \mathbb{Z}$ there are one or two choices for q, r

Integer Worst Case

For any $b < a \in \mathbb{Z}$ there are one or two choices for q, r

$$\begin{aligned} |r_1| + |r_2| &= |b| \\ \min\{|r_1|, |r_2|\} &\leq \frac{|b|}{2} \end{aligned}$$

Integer Worst Case

The remainders get halved in every iteration

Integer Worst Case

The remainders get halved in every iteration

$$
\begin{aligned}
a &= q_1 b + r_1 \quad |r_1| \leq \frac{|b|}{2} \\
b &= q_2 r_1 + r_2 \quad |r_2| \leq \frac{|r_1|}{2} \\
r_1 &= q_3 r_2 + r_3 \quad |r_3| \leq \frac{|r_2|}{2} \\
&\vdots \\
r_{n-1} &= q_{n+1} r_n + r_{n+1} \quad |r_{n+1}| \leq \frac{|r_n|}{2}
\end{aligned}
$$

Integer Worst Case

$$f_n = f_{n-1} + f_{n-2}$$

Integer Worst Case

$$f_n = f_{n-1} + f_{n-2}$$

$$\begin{aligned}
f_{n+1} &= f_n + f_{n-1} \\
f_n &= f_{n-1} + f_{n-2} \\
&\vdots \\
5 &= 1 \cdot 3 + 2 \\
3 &= 1 \cdot 2 + 1 \\
2 &= 2 \cdot 1 + 0
\end{aligned}$$

Integer Worst Case

$$f_n = f_{n-1} + f_{n-2}$$

$$\begin{aligned}
f_{n+1} &= f_n + f_{n-1} \\
f_n &= f_{n-1} + f_{n-2} \\
&\vdots \\
5 &= 1 \cdot 3 + 2 \\
3 &= 1 \cdot 2 + 1 \\
2 &= 2 \cdot 1 + 0
\end{aligned}$$

$$\frac{f_n}{f_{n-1}} \to \phi \approx 1.61$$

Integer Worst Case

$$f_n = f_{n-1} + f_{n-2}$$

$$f_n = 2f_{n-1} - f_{n-3}$$

$$\begin{aligned}
f_{n+1} &= f_n + f_{n-1} \\
f_n &= f_{n-1} + f_{n-2} \\
&\vdots \\
5 &= 1 \cdot 3 + 2 \\
3 &= 1 \cdot 2 + 1 \\
2 &= 2 \cdot 1 + 0
\end{aligned}$$

$$\frac{f_n}{f_{n-1}} \to \phi \approx 1.61$$

Integer Worst Case

$$f_n = f_{n-1} + f_{n-2}$$

$$f_n = 2f_{n-1} - f_{n-3}$$

$$\begin{aligned} f_{n+1} &= f_n + f_{n-1} \\ f_n &= f_{n-1} + f_{n-2} \\ &\vdots \\ 5 &= 1 \cdot 3 + 2 \\ 3 &= 1 \cdot 2 + 1 \\ 2 &= 2 \cdot 1 + 0 \end{aligned}$$

$$\begin{aligned} f_{n+1} &= 2f_n - f_{n-2} \\ f_n &= -3 \cdot -f_{n-2} - f_{n-4} \\ -f_{n-2} &= 3 \cdot -f_{n-4} + f_{n-6} \\ &\vdots \\ (-1)^n 5 &= (-1)^n 3 \cdot 2 - 1 \text{ or } (-1)^n 8 = (-1)^n 3 \\ 2 &= -2 \cdot -1 \quad \text{or} \quad 3 = -3 \cdot -1 \end{aligned}$$

$$\frac{f_n}{f_{n-1}} \to \phi \approx 1.61$$

Integer Worst Case

$$f_n = f_{n-1} + f_{n-2}$$

$$f_n = 2f_{n-1} - f_{n-3}$$

$$\begin{aligned}
f_{n+1} &= f_n + f_{n-1} \\
f_n &= f_{n-1} + f_{n-2} \\
&\vdots \\
5 &= 1 \cdot 3 + 2 \\
3 &= 1 \cdot 2 + 1 \\
2 &= 2 \cdot 1 + 0
\end{aligned}$$

$$\begin{aligned}
f_{n+1} &= 2f_n - f_{n-2} \\
f_n &= -3 \cdot -f_{n-2} - f_{n-4} \\
-f_{n-2} &= 3 \cdot -f_{n-4} + f_{n-6} \\
&\vdots \\
(-1)^n 5 &= (-1)^n 3 \cdot 2 - 1 \text{ or } (-1)^n 8 = (-1)^n 3 \\
2 &= -2 \cdot -1 \quad \text{or} \quad 3 = -3 \cdot -1
\end{aligned}$$

$$\frac{f_n}{f_{n-1}} \to \phi \approx 1.61$$

$$\frac{f_n}{f_{n-2}} = \frac{f_n}{f_{n-1}} \frac{f_{n-1}}{f_{n-2}} \to \phi^2 \approx 2.61$$

Gaussian Algorithm

Actual quotient of two Guassian integers will be inside some square and want to choose the quotient to be closest to one of the corners

Gaussian Algorithm

Actual quotient of two Guassian integers will be inside some square and want to choose the quotient to be closest to one of the corners

For $a, b \in \mathbb{Z}[i]$ the first step in calculating (a, b) is $a - qb = r$

$$\|q \cdot b - a\| < \|b\|$$

Gaussian Algorithm

Actual quotient of two Guassian integers will be inside some square and want to choose the quotient to be closest to one of the corners

For $a, b \in \mathbb{Z}[i]$ the first step in calculating (a, b) is $a - qb = r$

$$\|q \cdot b - a\| < \|b\|$$

$6 + 7\mathrm{i} = (2 + \mathrm{i}) \cdot (3 + 2\mathrm{i}) + 2$

Gaussian Algorithm

Actual quotient of two Guassian integers will be inside some square and want to choose the quotient to be closest to one of the corners

For $a, b \in \mathbb{Z}[i]$ the first step in calculating (a, b) is $a - qb = r$

$$\|q \cdot b - a\| < \|b\|$$

$$6 + 7\mathrm{i} = (2 + \mathrm{i}) \cdot (3 + 2\mathrm{i}) + 2 \qquad 6 + 7\mathrm{i} = (3 + \mathrm{i}) \cdot (3 + 2\mathrm{i}) - 1 - 2\mathrm{i}$$

Conclusions

Conclusions

$\mathbb{Z}$ Worst Case is

$$\log_\phi(3-\phi)N$$

$\mathbb{Z}$ Average Case is

$$\frac{12}{\pi^2}\ln(2N)$$

Conclusions

$\mathbb{Z}$ Worst Case is

$$\log_\phi (3-\phi) N$$

$\mathbb{Z}$ Average Case is

$$\frac{12}{\pi^2} \ln(2N)$$

$\mathbb{Z}[i]$ Worst Case is

$$\log_{2+\sqrt{3}}(6N^2+3)$$

Conclusions

$\mathbb{Z}$ Worst Case is

$$\log_\phi (3-\phi) N$$

$\mathbb{Z}$ Average Case is

$$\frac{12}{\pi^2} \ln(2N)$$

$\mathbb{Z}[i]$ Worst Case is

$$\log_{2+\sqrt{3}} (6N^2+3)$$

$\mathbb{Z}[x]$ Worst Case has steps and calculations at each step being

$$N = \deg\ p(x) \qquad N^2$$

$$N^3$$

Sources

Abstract Algebra - Dummit and Foote (Book)

The Art of Computer Programming Vol II: Seminumerical Algorithms - Donald Knuth (Book)

The Euclidean Algorithm for Gaussian Integers - Heinrich Rolletschek (Paper)

Prove that the Gaussian Integer's ring is a Euclidean domain (StackExchange)

$\mathbb{Z}[i]$ is a Principal Ideal Domain (StackExchange)

Integer Remainders (Desmos)

Gaussian Remainders (Desmos)