Euclidean Rings and Diophantine Equations

Duc Van Huynh

January 18, 2012
Gaussian says hello.
Integral Domain

An integral domain is a commutative ring $R$ with identity in which for any two elements $a$ and $b$, the equality $ab = 0$ implies either $a = 0$ or $b = 0$. 
Integral Domain

An integral domain is a commutative ring $R$ with identity in which for any two elements $a$ and $b$, the equality $ab = 0$ implies either $a = 0$ or $b = 0$.

Units, associates, and irreducibles

1. Any divisor of 1 is called a unit.
Integral Domain

An integral domain is a commutative ring $R$ with identity in which for any two elements $a$ and $b$, the equality $ab = 0$ implies either $a = 0$ or $b = 0$.

Units, associates, and irreducibles

1. Any divisor of 1 is called a *unit*.
2. We say $a$ and $b$ are *associates* if there exists a unit $u \in R$ such that $a = bu$. 
Integral Domain

An integral domain is a commutative ring $R$ with identity in which for any two elements $a$ and $b$, the equality $ab = 0$ implies either $a = 0$ or $b = 0$.

Units, associates, and irreducibles

1. Any divisor of 1 is called a *unit*.
2. We say $a$ and $b$ are *associates* if there exists a unit $u \in R$ such that $a = bu$.
3. We say that $a \in R$ is *irreducible* if for any factorization of $a = bc$, one of $b$ or $c$ is a unit.
Integral Domain

Norm on $\mathbb{R}$

A norm on $\mathbb{R}$ is a map $N : \mathbb{R} \rightarrow \mathbb{N}$ such that:

1. $N(ab) = N(a)N(b)$ $\forall a, b \in \mathbb{R}$; and

Example 1

Let $D$ be squarefree. Consider $\mathbb{R} = \mathbb{Z}[\sqrt{D}]$. The map $N$ on $\mathbb{R}$ defined by $N(a + b\sqrt{D}) = |a^2 - Db^2|$.

is a norm.
Integral Domain

**Norm on \( R \)**

A norm on \( R \) is a map \( N : R \to \mathbb{N} \) such that:

1. \( N(ab) = N(a)N(b) \ \forall a, b \in R \); and
2. \( N(a) = 1 \) if and only if \( a \) is a unit.
Integral Domain

Norm on $R$

A norm on $R$ is a map $N : R \to \mathbb{N}$ such that:

1. $N(ab) = N(a)N(b) \forall a, b \in R$; and
2. $N(a) = 1$ if and only if $a$ is a unit.

Example 1

Let $D$ be squarefree. Consider $R = \mathbb{Z}[\sqrt{D}]$. The map $N$ on $R$ defined by

$$N(a + b\sqrt{D}) = |a^2 - Db^2|.$$ 

is a norm.
Theorem 1

If $R$ has a norm map, then every elements of $R$ can be written as a product of irreducibles.
Theorem 1

If $R$ has a norm map, then every elements of $R$ can be written as a product of irreducibles.

Example 1 continue

The ring $R = \mathbb{Z}[\sqrt{D}]$ from example 1 has the norm $N$ defined by

$$N(a + b\sqrt{D}) = |a^2 - Db^2|$$

By Theorem 1, every elements of $R$ can be written as a product of irreducibles. Is this factorization unique?
Example 2

Consider $R = \mathbb{Z}[\sqrt{-5}]$. It has the norm $N(a + b\sqrt{-5}) = a^2 + 5b^2$.

1. What are the units of $R$?
   
   By definition of a norm, we know that $u$ is a unit if and only if $N(u) = a^2 + 5b^2 = 1$. But this is only possible iff $a = \pm 1$. 
Example 2

Consider $R = \mathbb{Z}[\sqrt{-5}]$. It has the norm $N(a + b\sqrt{-5}) = a^2 + 5b^2$.

1. What are the units of $R$?
   
   By definition of a norm, we know that $u$ is a unit if and only if $N(u) = a^2 + 5b^2 = 1$. But this is only possible iff $a = \pm 1$.

2. Does there exists $x \in R$ such that $N(x) = 2$? Well, then $N(x) = a^2 + 5b^2 = 2$, which clearly has no solutions in $\mathbb{Z}$.
Example 2

Consider $R = \mathbb{Z}[\sqrt{-5}]$. It has the norm $N(a + b\sqrt{-5}) = a^2 + 5b^2$.

1. What are the units of $R$?
   By definition of a norm, we know that $u$ is a unit if and only if $N(u) = a^2 + 5b^2 = 1$. But this is only possible iff $a = \pm 1$.

2. Does there exist $x \in R$ such that $N(x) = 2$? Well, then $N(x) = a^2 + 5b^2 = 2$, which clearly has no solutions in $\mathbb{Z}$.

3. Is 2 irreducible? Suppose not. Suppose $2 = xy$ such that neither $x$ or $y$ is a unit. Then $N(x) = 2$, which is not possible. Hence, 2 is irreducible. Similarly, 3 is irreducible.
Example 2

Consider $R = \mathbb{Z}[\sqrt{-5}]$. It has the norm $N(a + b\sqrt{-5}) = a^2 + 5b^2$.

1. What are the units of $R$?
   By definition of a norm, we know that $u$ is a unit if and only if $N(u) = a^2 + 5b^2 = 1$. But this is only possible iff $a = \pm 1$.

2. Does there exist $x \in R$ such that $N(x) = 2$? Well, then $N(x) = a^2 + 5b^2 = 2$, which clearly has no solutions in $\mathbb{Z}$.

3. Is 2 irreducible? Suppose not. Suppose $2 = xy$ such that neither $x$ or $y$ is a unit. Then $N(x) = 2$, which is not possible. Hence, 2 is irreducible. Similarly, 3 is irreducible.

4. Is $1 + \sqrt{-5}$ irreducible? Suppose not. Suppose $1 + \sqrt{-5} = xy$ such that neither $x$ or $y$ is a unit. Then $N(x) = 2$ or 3; either way, it is not possible. Hence, $1 + \sqrt{-5}$ is irreducible.
Example 2 continue

1. We have shown that $2, 3, 1 \pm \sqrt{-5}$ are irreducibles. Since 2 and 3 have different norms, they are not associates.
Example 2 continue

1. We have shown that 2, 3, $1 \pm \sqrt{-5}$ are irreducibles. Since 2 and 3 have different norms, they are not associates.

2. If $N(x) = N(y)$, are $x$ and $y$ associates? We see that $N(1 \pm \sqrt{-5}) = 6$. Are $1 \pm \sqrt{-5}$ associates?
Example 2 continue

1. We have shown that 2, 3, $1 \pm \sqrt{-5}$ are irreducibles. Since 2 and 3 have different norms, they are not associates.

2. If $N(x) = N(y)$, are $x$ and $y$ associates? We see that $N(1 \pm \sqrt{-5}) = 6$. Are $1 \pm \sqrt{-5}$ associates?

3. Suppose $1 \pm \sqrt{-5}$ are associates. Then $1 + \sqrt{-5} = u(1 - \sqrt{-5})$ for some unit $u$. But the only units of $R$ are $\pm 1$. Hence, $1 \pm \sqrt{-5}$ are not associates.
Example 2 continue

1. We have shown that 2, 3, 1 ± \( \sqrt{-5} \) are irreducibles. Since 2 and 3 have different norms, they are not associates.

2. If \( N(x) = N(y) \), are \( x \) and \( y \) associates? We see that \( N(1 \pm \sqrt{-5}) = 6 \). Are \( 1 \pm \sqrt{-5} \) associates?

3. Suppose \( 1 \pm \sqrt{-5} \) are associates. Then \( 1 + \sqrt{-5} = u(1 - \sqrt{-5}) \) for some unit \( u \). But the only units of \( R \) are \( \pm 1 \). Hence, \( 1 \pm \sqrt{-5} \) are not associates.

4. 2, 3, \( 1 \pm \sqrt{-5} \) are irreducibles and not associates.
Example 2 continue

By *Theorem 1*, we know that every elements of $R = \mathbb{Z}[\sqrt{-5}]$ can be expressed as the product of irreducibles. Is the expression unique?

Note that $2 \times 3 = (1 + \sqrt{-5})(1 - \sqrt{-5}) = 6$. Hence, we do not have uniqueness in $R$.
By Theorem 1, we know that every element of $R = \mathbb{Z}[\sqrt{-5}]$ can be expressed as the product of irreducibles. Is the expression unique?

Note that $2 \times 3 = (1 + \sqrt{-5})(1 - \sqrt{-5}) = 6$. Hence, we do not have uniqueness in $R$. 
Example 2 continue

1. By Theorem 1, we know that every element of $R = \mathbb{Z}[\sqrt{-5}]$ can be expressed as the product of irreducibles. Is the expression unique?

2. Note that $2 \times 3 = (1 + \sqrt{-5})(1 - \sqrt{-5}) = 6$. Hence, we do not have uniqueness in $R$.

3. When can we have uniqueness?
An integral domain $R$ is a *unique factorization domain* if

1. every element of $R$ can be written as a product of irreducibles; and
An integral domain $R$ is a *unique factorization domain* if

1. every element of $R$ can be written as a product of irreducibles; and
2. this factorization is essentially unique in the sense that if $a = \pi_1 \pi_2 \ldots \pi_r = \tau_1 \tau_2 \ldots \tau_s$, then $r = s$ and after suitable permutation, $\pi_i$ and $\tau_i$ are associates.
An integral domain $R$ is a \textit{unique factorization domain} if

1. every element of $R$ can be written as a product of irreducibles; and

2. this factorization is essentially unique in the sense that if $a = \pi_1 \pi_2 \ldots \pi_r = \tau_1 \tau_2 \ldots \tau_s$, then $r = s$ and after suitable permutation, $\pi_i$ and $\tau_i$ are associates.

\textbf{Theorem 2}

(2) of the definition above is equivalent to: if $\pi$ is irreducible and $\pi$ divides $ab$, then $\pi | a$ or $\pi | b$. 
Principal Ideal

An ideal $I \subset R$ is called principal if it can be generated by a single element of $R$. A domain $R$ is then called a principal ideal domain if every ideal of $R$ is principal.
Unique Factorization Domain

Principal Ideal

An ideal \( I \subset R \) is called *principal* if it can be generated by a single element of \( R \). A domain \( R \) is then called a *principal ideal domain* if every ideal of \( R \) is principal.

Theorem 3

If \( \pi \) is an irreducible element of a principal ideal domain, then \((\pi)\), the ideal generated by \( \pi \), is a maximal ideal.
Unique Factorization Domain

Principal Ideal

An ideal \( I \subset R \) is called *principal* if it can be generated by a single element of \( R \). A domain \( R \) is then called a *principal ideal domain* if every ideal of \( R \) is principal.

Theorem 3

If \( \pi \) is an irreducible element of a principal ideal domain, then \((\pi)\), the ideal generated by \( \pi \), is a maximal ideal.

Theorem 4

If \( R \) is a principal ideal domain, then \( R \) is a unique factorization domain.
Euclidean Domain

Theorem 5

If $R$ is an integral domain with norm map $N$, and given $a, b \in R$, $\exists q, r \in R$ such that $a = bq + r$ with $r = 0$ or $N(r) < N(b)$, we say that $R$ is Euclidean. Furthermore, it is also a principal ideal domain.

Theorem 6

If $F$ is a field, then $F[x]$ is Euclidean.

Theorem 7 (Gauss Lemma)

Let $R$ be a unique factorization domain and $F$ its field of fractions. If a polynomial $p(x)$ is reducible in $F[x]$, then it is reducible in $R[x]$. 
Euclidean Domain

Theorem 5
If $R$ is an integral domain with norm map $N$, and given $a, b \in R$, $\exists q, r \in R$ such that $a = bq + r$ with $r = 0$ or $N(r) < N(b)$, we say that $R$ is Euclidean. Furthermore, it is also a principal ideal domain.

Theorem 6
If $F$ is a field, then $F[x]$ is Euclidean.
Euclidean Domain

Theorem 5
If $R$ is an integral domain with norm map $N$, and given $a, b \in R$, $\exists q, r \in R$ such that $a = bq + r$ with $r = 0$ or $N(r) < N(b)$, we say that $R$ is Euclidean. Furthermore, it is also a principal ideal domain.

Theorem 6
If $F$ is a field, then $F[x]$ is Euclidean.

Theorem 7 (Gauss Lemma)
Let $R$ be a unique factorization domain and $F$ its field of fractions. If a polynomial $p(x)$ is reducible in $F[x]$, then it is reducible in $R[x]$.
Theorem 8

If $R$ is a unique factorization domain, then $R[x]$ is a unique factorization domain.
The fun begins.

**$R = \mathbb{Z}[i]$ is Euclidean**

$R$ has the norm $N(a + bi) = a^2 + b^2$. Given any two elements of $R$, say $\alpha = a + bi$ and $\gamma = c + di$, we would like to find $q, r \in \mathbb{Z}$ such that $a + bi = q(c + di) + r$, where $r = 0$ or $N(r) < N(c + di)$. We will work in $\mathbb{Q}[i]$. 
Duc Van Huynh  Euclidean Rings and Diophantine Equations

The fun begins.

**$R = \mathbb{Z}[i]$** is Euclidean

$R$ has the norm $N(a + bi) = a^2 + b^2$. Given any two elements of $R$, say $\alpha = a + bi$ and $\gamma = c + di$, we would like to find $q, r \in \mathbb{Z}$ such that $a + bi = q(c + di) + r$, where $r = 0$ or $N(r) < N(c + di)$. We will work in $\mathbb{Q}[i]$.

$$\frac{\alpha}{\gamma} = \frac{a + bi}{c + di} = x + yi, \text{ where } x, y \in \mathbb{Q}$$
The fun begins.

**$R = \mathbb{Z}[i]$ is Euclidean**

$R$ has the norm $N(a + bi) = a^2 + b^2$. Given any two elements of $R$, say $\alpha = a + bi$ and $\gamma = c + di$, we would like to find $q, r \in \mathbb{Z}$ such that $a + bi = q(c + di) + r$, where $r = 0$ or $N(r) < N(c + di)$. We will work in $\mathbb{Q}[i]$.

\[
\frac{\alpha}{\gamma} = \frac{a + bi}{c + di} = x + yi, \text{ where } x, y \in \mathbb{Q}
\]

Choose $m, n \in \mathbb{Z}$ such that $|x - m| \leq 1/2$, and $|s - n| \leq 1/2$. Set $q = m + ni$. Then $q \in R$ and $\alpha = q\gamma + r$ for some suitable $r$, with
The fun begins.

\[ R = \mathbb{Z}[i] \text{ is Euclidean} \]

\( R \) has the norm \( N(a + bi) = a^2 + b^2 \). Given any two elements of \( R \), say \( \alpha = a + bi \) and \( \gamma = c + di \), we would like to find \( q, r \in \mathbb{Z} \) such that \( a + bi = q(c + di) + r \), where \( r = 0 \) or \( N(r) < N(c + di) \). We will work in \( \mathbb{Q}[i] \).

\[
\frac{\alpha}{\gamma} = \frac{a + bi}{c + di} = x + yi, \text{ where } x, y \in \mathbb{Q}
\]

Choose \( m, n \in \mathbb{Z} \) such that \( |x - m| \leq 1/2 \), and \( |s - n| \leq 1/2 \). Set \( q = m + ni \). Then \( q \in R \) and \( \alpha = q \gamma + r \) for some suitable \( r \), with

\[
N(r) = N(\alpha - q \gamma) = N(\alpha/\gamma - q)N(\gamma) < N(\gamma)
\]
Gaussian Integers
Find all integer solutions to $y^2 + 1 = x^3$ with $x, y \neq 0$.

1. $x$ is even $\Rightarrow$ $y$ is odd. $y$ is odd $\Rightarrow$ $y^2 \equiv 1 \pmod{8}$. $x$ even $\Rightarrow$ $y^2 \equiv 7 \pmod{8}$. So, $x$ is odd and $y$ is even.
Find all integer solutions to $y^2 + 1 = x^3$ with $x, y \neq 0$.

1. $x$ is even $\Rightarrow$ $y$ is odd. $y$ is odd $\Rightarrow$ $y^2 \equiv 1 \pmod{8}$. $x$ even $\Rightarrow$ $y^2 \equiv 7 \pmod{8}$. So, $x$ is odd and $y$ is even.

2. $y^2 + 1 = (y + i)(y - i) = x^3$. We work in $R = \mathbb{Z}[i]$. 
Diophantine Equations

Find all integer solutions to $y^2 + 1 = x^3$ with $x, y \neq 0$.

1. $x$ is even $\Rightarrow$ $y$ is odd. $y$ is odd $\Rightarrow$ $y^2 \equiv 1 \pmod{8}$. $x$ even $\Rightarrow$ $y^2 \equiv 7 \pmod{8}$. So, $x$ is odd and $y$ is even.

2. $y^2 + 1 = (y + i)(y - i) = x^3$. We work in $R = \mathbb{Z}[i]$.

3. If a non-unit $\delta$ divides both $y + i$ and $y - i$, then $\delta | 2i$, which implies $\delta | 2$. So, $N(\delta)$ is even, but $N(y + i)$ is odd.

4. $y + i$ and $y - i$ are each a product of perfect cube and a unit. Write $y + i = u(a + bi)^3$. 

Duc Van Huynh
Diophantine Equations

Find all integer solutions to $y^2 + 1 = x^3$ with $x, y \neq 0$.

1. $x$ is even $\Rightarrow$ $y$ is odd. $y$ is odd $\Rightarrow$ $y^2 \equiv 1 \pmod{8}$. $x$ even $\Rightarrow$ $y^2 \equiv 7 \pmod{8}$. So, $x$ is odd and $y$ is even.

2. $y^2 + 1 = (y + i)(y - i) = x^3$. We work in $R = \mathbb{Z}[i]$.

3. If a non-unit $\delta$ divides both $y + i$ and $y - i$, then $\delta|2i$, which implies $\delta|2$. So, $N(\delta)$ is even, but $N(y + i)$ is odd.

4. $y + i$ and $y - i$ are each a product of perfect cube and a unit. Write $y + i = u(a + bi)^3$.

5. The only units of $R$ are $\pm 1$ and $\pm i$. 
Find all integer solutions to \( y^2 + 1 = x^3 \) with \( x, y \neq 0 \).

1. \( x \) is even \( \Rightarrow \) \( y \) is odd. \( y \) is odd \( \Rightarrow \) \( y^2 \equiv 1 \pmod{8} \). \( x \) even \( \Rightarrow \) \( y^2 \equiv 7 \pmod{8} \). So, \( x \) is odd and \( y \) is even.

2. \( y^2 + 1 = (y + i)(y - i) = x^3 \). We work in \( R = \mathbb{Z}[i] \).

3. If a non-unit \( \delta \) divides both \( y + i \) and \( y - i \), then \( \delta \mid 2i \), which implies \( \delta \mid 2 \). So, \( N(\delta) \) is even, but \( N(y + i) \) is odd.

4. \( y + i \) and \( y - i \) are each a product of perfect cube and a unit. Write \( y + i = u(a + bi)^3 \).

5. The only units of \( R \) are \( \pm 1 \) and \( \pm i \).

6. All units are perfect cubes.
Find all integer solutions to $y^2 + 1 = x^3$ with $x, y \neq 0$, continue.

We may assume that $y + i = (a + bi)^3$. 
Find all integer solutions to $y^2 + 1 = x^3$ with $x, y \neq 0$, continue.

1. We may assume that $y + i = (a + bi)^3$.
2. $y + i = a^3 + 3a^2 bi - 3ab^2 - b^3 i = a^3 - 3ab^2 + (3a^2 b - b^3) i$. 
Find all integer solutions to \( y^2 + 1 = x^3 \) with \( x, y \neq 0 \), continue.

1. We may assume that \( y + i = (a + bi)^3 \).

2. \( y + i = a^3 + 3a^2 bi - 3ab^2 - b^3 i = a^3 - 3ab^2 + (3a^2 b - b^3)i \).

3. Comparing imaginary parts, we have \( 1 = 3a^2 b - b^3 = b(3a^2 - b^2) \).
Find all integer solutions to \( y^2 + 1 = x^3 \) with \( x, y \neq 0 \), continue.

1. We may assume that \( y + i = (a + bi)^3 \).
2. \( y + i = a^3 + 3a^2 bi - 3ab^2 - b^3 i = a^3 - 3ab^2 + (3a^2 b - b^3)i \).
3. Comparing imaginary parts, we have \( 1 = 3a^2 b - b^3 = b(3a^2 - b^2) \).
4. No solution.
\[ R = \mathbb{Z}[\sqrt{-2}] \text{ is Euclidean.} \]

1. Let \( \alpha, \beta \in R \). Then \( \alpha/\beta = \alpha\beta/\beta\bar{\beta} = c + d\sqrt{-2} \).
Diophantine Equations

\( R = \mathbb{Z}[\sqrt{-2}] \) is Euclidean.

1. Let \( \alpha, \beta \in R \). Then \( \alpha/\beta = \alpha\beta/\beta\bar{\beta} = c + d\sqrt{-2} \).

2. Choose \( m, n \in \mathbb{Z} \) such that \( |m - c| \leq 1/2 \) and \( |n - d| \leq 1/2 \).
Diophantine Equations

$R = \mathbb{Z}[\sqrt{-2}]$ is Euclidean.

1. Let $\alpha, \beta \in R$. Then $\alpha/\beta = \alpha\beta/\beta\bar{\beta} = c + d\sqrt{-2}$.

2. Choose $m, n \in \mathbb{Z}$ such that $|m - c| \leq 1/2$ and $|n - d| \leq 1/2$.

3. Take $q = m + b\sqrt{-2}$ and $r = \alpha - q\beta$. 
Diophantine Equations

\[ R = \mathbb{Z}[\sqrt{-2}] \text{ is Euclidean.} \]

1. Let \( \alpha, \beta \in R \). Then \( \alpha/\beta = \alpha \beta / (\beta \bar{\beta}) = c + d \sqrt{-2} \).
2. Choose \( m, n \in \mathbb{Z} \) such that \( |m - c| \leq 1/2 \) and \( |n - d| \leq 1/2 \).
3. Take \( q = m + b \sqrt{-2} \) and \( r = \alpha - q \beta \).
4. \( N(\alpha/\beta - q) = (m - c)^2 + 2(n - d)^2 \)
Diophantine Equations

\[ R = \mathbb{Z}[\sqrt{-2}] \text{ is Euclidean.} \]

1. Let \( \alpha, \beta \in R \). Then \( \alpha/\beta = \alpha\beta/\beta\bar{\beta} = c + d\sqrt{-2} \).
2. Choose \( m, n \in \mathbb{Z} \) such that \( |m - c| \leq 1/2 \) and \( |n - d| \leq 1/2 \).
3. Take \( q = m + b\sqrt{-2} \) and \( r = \alpha - q\beta \).
4. \( N(\alpha/\beta - q) = (m - c)^2 + 2(n - d)^2 \)
5. \( N(r) = N(\beta)N(\alpha/\beta - q) < N(\beta)(1/2 + 2(1/4)) < N(\beta) \).
Diophantine Equations

Solve $y^2 + 2 = x^3$ for $x, y \in \mathbb{Z}$ with $x, y \neq 0$.

1. $x$ and $y$ are both odd.
Diophantine Equations

Solve $y^2 + 2 = x^3$ for $x, y \in \mathbb{Z}$ with $x, y \neq 0$.

1. $x$ and $y$ are both odd.
2. $y^2 + 2 = (y + \sqrt{-2})(y - \sqrt{-2}) = x^3$. We work in $\mathbb{Z}[\sqrt{-2}]$. 
Diophantine Equations

Solve $y^2 + 2 = x^3$ for $x, y \in \mathbb{Z}$ with $x, y \neq 0$.

1. $x$ and $y$ are both odd.
2. $y^2 + 2 = (y + \sqrt{-2})(y - \sqrt{-2}) = x^3$. We work in $\mathbb{Z}[\sqrt{-2}]$.
3. If a non-unit $\delta$ divides both $y + \sqrt{-2}$ and $y - \sqrt{-2}$, then $\delta | 2\sqrt{-2}$, which implies that $N(\delta)$ is even. Not possible.
Diophantine Equations

Solve $y^2 + 2 = x^3$ for $x, y \in \mathbb{Z}$ with $x, y \neq 0$.

1. $x$ and $y$ are both odd.
2. $y^2 + 2 = (y + \sqrt{-2})(y - \sqrt{-2}) = x^3$. We work in $\mathbb{Z}[\sqrt{-2}]$.
3. If a non-unit $\delta$ divides both $y + \sqrt{-2}$ and $y - \sqrt{-2}$, then $\delta | 2\sqrt{-2}$, which implies that $N(\delta)$ is even. Not possible.
4. The only units of $R$ are $\pm 1$. 
Diophantine Equations

Solve \( y^2 + 2 = x^3 \) for \( x, y \in \mathbb{Z} \) with \( x, y \neq 0 \).

1. \( x \) and \( y \) are both odd.
2. \( y^2 + 2 = (y + \sqrt{-2})(y - \sqrt{-2}) = x^3 \). We work in \( \mathbb{Z}[\sqrt{-2}] \).
3. If a non-unit \( \delta \) divides both \( y + \sqrt{-2} \) and \( y - \sqrt{-2} \), then \( \delta | 2\sqrt{-2} \), which implies that \( N(\delta) \) is even. Not possible.
4. The only units of \( R \) are \( \pm 1 \).
5. We may write
\[
y + \sqrt{-2} = (a + b\sqrt{-2})^3 = a^3 - 6ab^2 + (3a^2b - 2b^3)\sqrt{-2}.
\]
Diophantine Equations

Solve $y^2 + 2 = x^3$ for $x, y \in \mathbb{Z}$ with $x, y \neq 0$.

1. $x$ and $y$ are both odd.
2. $y^2 + 2 = (y + \sqrt{-2})(y - \sqrt{-2}) = x^3$. We work in $\mathbb{Z}[-2]$.
3. If a non-unit $\delta$ divides both $y + \sqrt{-2}$ and $y - \sqrt{-2}$, then $\delta | 2\sqrt{-2}$, which implies that $N(\delta)$ is even. Not possible.
4. The only units of $R$ are $\pm 1$.
5. We may write
   
   $y + \sqrt{-2} = (a + b\sqrt{-2})^3 = a^3 - 6ab^2 + (3a^2b - 2b^3)\sqrt{-2}$.
6. Comparing real and imaginary parts, we have $y = a^3 - 6ab^2$ and $1 = b(3a^2 - 2b^2)$. 
## Diophantine Equations

Solve \( y^2 + 2 = x^3 \) for \( x, y \in \mathbb{Z} \) with \( x, y \neq 0 \).

1. \( x \) and \( y \) are both odd.
2. \( y^2 + 2 = (y + \sqrt{-2})(y - \sqrt{-2}) = x^3 \). We work in \( \mathbb{Z}[\sqrt{-2}] \).
3. If a non-unit \( \delta \) divides both \( y + \sqrt{-2} \) and \( y - \sqrt{-2} \), then \( \delta \mid 2\sqrt{-2} \), which implies that \( N(\delta) \) is even. Not possible.
4. The only units of \( R \) are \( \pm 1 \).
5. We may write \( y + \sqrt{-2} = (a + b\sqrt{-2})^3 = a^3 - 6ab^2 + (3a^2b - 2b^3)\sqrt{-2} \).
6. Comparing real and imaginary parts, we have \( y = a^3 - 6ab^2 \) and \( 1 = b(3a^2 - 2b^2) \).
7. We have \( x = 3, y = \pm 5 \).
Show that $R = \mathbb{Z}[(1 + \sqrt{-11})/2]$ is Euclidean.

1. Given $\alpha, \beta \in R$, we wish to find $\gamma \in R$ such that $N(\alpha/\beta - \gamma) < 1$. 

Given $\alpha, \beta \in R$, we wish to find $\gamma \in R$ such that $N(\alpha/\beta - \gamma) < 1$. 

Choose $v$ so that $|2y - v| \leq 1/2$ and $u$ with same parity as $v$.

So, $(2x - u)^2 + 11(2y - v)^2 \leq 1 + 11/4 = 15/4 < 4$.

Use this fact to find all integer solutions to the equation $x^2 + 11 = y^3$. 
Diophantine Equations

Show that \( R = \mathbb{Z}[(1 + \sqrt{-11})/2] \) is Euclidean.

1. Given \( \alpha, \beta \in R \), we wish to find \( \gamma \in R \) such that \( N(\alpha/\beta - \gamma) < 1 \).

2. Let \( \alpha/\beta = x + y\sqrt{-11}, x, y \in \mathbb{Q}, \) and \( \gamma = (u + v\sqrt{-11})/2 \) with \( u, v \in \mathbb{Z} \) and \( u \equiv v \pmod{2} \).
Show that $R = \mathbb{Z}[(1 + \sqrt{-11})/2]$ is Euclidean.

1. Given $\alpha, \beta \in R$, we wish to find $\gamma \in R$ such that $N(\alpha/\beta - \gamma) < 1$.

2. Let $\alpha/\beta = x + y\sqrt{-11}$, $x, y \in \mathbb{Q}$, and $\gamma = (u + v\sqrt{-11})/2$ with $u, v \in \mathbb{Z}$ and $u \equiv v \pmod{2}$.

3. We want $N \left( x + y\sqrt{-11} - \left( \frac{u + v\sqrt{-11}}{2} \right) \right) < 1$ or
### Diophantine Equations

**Show that** \( R = \mathbb{Z}[(1 + \sqrt{-11})/2] \) **is Euclidean.**

1. **Given** \( \alpha, \beta \in R \), we wish to find \( \gamma \in R \) such that \( N(\alpha/\beta - \gamma) < 1 \).

2. **Let** \( \alpha/\beta = x + y\sqrt{-11}, x, y \in \mathbb{Q} \), and \( \gamma = (u + v\sqrt{-11})/2 \) with \( u, v \in \mathbb{Z} \) and \( u \equiv v \pmod{2} \).

3. **We want** \( N \left( x + y\sqrt{-11} - \left( \frac{u + v\sqrt{-11}}{2} \right) \right) < 1 \) or \( (2x - u)^2 + 11(2y - v)^2 < 4 \).
Show that $R = \mathbb{Z}[(1 + \sqrt{-11})/2]$ is Euclidean.

1. Given $\alpha, \beta \in R$, we wish to find $\gamma \in R$ such that $N(\alpha/\beta - \gamma) < 1$.

2. Let $\alpha/\beta = x + y\sqrt{-11}, x, y \in \mathbb{Q}$, and $\gamma = (u + v\sqrt{-11})/2$ with $u, v \in \mathbb{Z}$ and $u \equiv v \pmod{2}$.

3. We want $N\left(x + y\sqrt{-11} - \left(\frac{u+v\sqrt{-11}}{2}\right)\right) < 1$ or $(2x - u)^2 + 11(2y - v)^2 < 4$.

4. Choose $v$ so that $|2y - v| \leq 1/2$ and $u$ with same parity as $v$. 
Show that $R = \mathbb{Z}[(1 + \sqrt{-11})/2]$ is Euclidean.

1. Given $\alpha, \beta \in R$, we wish to find $\gamma \in R$ such that $N(\alpha/\beta - \gamma) < 1$.

2. Let $\alpha/\beta = x + y\sqrt{-11}$, $x, y \in \mathbb{Q}$, and $\gamma = (u + v\sqrt{-11})/2$ with $u, v \in \mathbb{Z}$ and $u \equiv v \pmod{2}$.

3. We want $N \left( x + y\sqrt{-11} - \left( \frac{u + v\sqrt{-11}}{2} \right) \right) < 1$ or $(2x - u)^2 + 11(2y - v)^2 < 4$.

4. Choose $v$ so that $|2y - v| \leq 1/2$ and $u$ with same parity as $v$.

5. So, $(2x - u)^2 + 11(2y - v)^2 \leq 1 + 11/4 = 15/4 < 4$. 
Show that $R = \mathbb{Z}[(1 + \sqrt{-11})/2]$ is Euclidean.

1. Given $\alpha, \beta \in R$, we wish to find $\gamma \in R$ such that $N(\alpha/\beta - \gamma) < 1$.
2. Let $\alpha/\beta = x + y\sqrt{-11}, x, y \in \mathbb{Q}$, and $\gamma = (u + v\sqrt{-11})/2$ with $u, v \in \mathbb{Z}$ and $u \equiv v \pmod{2}$.
3. We want $N \left( x + y\sqrt{-11} - \frac{u + v\sqrt{-11}}{2} \right) < 1$ or $(2x - u)^2 + 11(2y - v)^2 < 4$.
4. Choose $v$ so that $|2y - v| \leq 1/2$ and $u$ with same parity as $v$.
5. So, $(2x - u)^2 + 11(2y - v)^2 \leq 1 + 11/4 = 15/4 < 4$.
6. Use this fact to find all integer solutions to the equation $x^2 + 11 = y^3$. 
Example of non-Euclidean and more Diophantine equations

For January 23

1. \( \mathbb{Z}[(1 + \sqrt{-19})/2] \) is not Euclidean for the norm map.
Example of non-Euclidean and more Diophantine equations

For January 23

1. \( \mathbb{Z}[(1 + \sqrt{-19})/2] \) is not Euclidean for the norm map.
2. There are only finitely many rings \( \mathbb{Z}[\sqrt{d}] \) with \( d \equiv 2 \) or 3 (mod 4) which are norm Euclidean.
Example of non-Euclidean and more Diophantine equations

For January 23

1. $\mathbb{Z}[(1 + \sqrt{-19})/2]$ is not Euclidean for the norm map.
2. There are only finitely many rings $\mathbb{Z}[\sqrt{d}]$ with $d \equiv 2$ or 3 (mod 4) which are norm Euclidean.
3. Let $\rho$ be a nontrivial cube root of unity. Then $\mathbb{Z}[\rho]$ is Euclidean.
For January 23

1. \( \mathbb{Z}[(1 + \sqrt{-19})/2] \) is not Euclidean for the norm map.

2. There are only finitely many rings \( \mathbb{Z}[\sqrt{d}] \) with \( d \equiv 2 \) or \( 3 \) (mod 4) which are norm Euclidean.

3. Let \( \rho \) be a nontrivial cube root of unity. Then \( \mathbb{Z}[\rho] \) is Euclidean.

4. Using above, it can be shown that Fermat Last Theorem is true for \( n = 3 \).
Gaussian says bye.