Math 4400
Week 5 - Thursday.
Quadratic numbers.

Note: In class I said we would discuss an application of the pattern in Pascal's triangle, but I'm going to delay that till later.

Definition:

- A complex number α is a <u>quadratic integer</u> if it is a root of a monic degree 2 polynomial $f(x) = x^2 + ax + b$ with $a, b \in \mathbb{Z}$.
- It is a quadratic rational if ... $a, b \in \mathbb{Q}$.

Examples:

- i is a quadratic integer — $f(x) = x^2 + 1$
  $i = \sqrt{-1}$
  $f(i) = i^2 + 1 = -1 + 1 = 0.$
- $\frac{i}{2}$ is a quadratic rational but <u>not</u> a quadratic

integer $\quad f(x) = x^2 + \frac{1}{4}$.

- If $D \in \mathbb{Z}$, $a, b \in \mathbb{Z}$, then $a + b\sqrt{D}$ is a quadratic integer.

Note $\sqrt{D}$ is a quadratic integer – root of $x^2 - D$.

→ Root of $x^2 - 2ax + (a^2 - b^2 D)$.
(get this by completing the square).

- If $D \in \mathbb{Z}$, $a, b \in \mathbb{Q}$, then $a + b\sqrt{D}$ is a quadratic rational.

Important fact: If α is a quadratic rational but not rational, then there is <u>exactly one</u> $f(x) = x^2 + ax + b$ with $a, b \in \mathbb{Q}$ such that $f(\alpha) = 0$.

Observation: $(a + b\sqrt{D})(c + d\sqrt{D})$

$= ac + bc\sqrt{D} + ad\sqrt{D} + bd(\sqrt{D})(\sqrt{D})$

$= ac + bdD + (ad + bc)\sqrt{D}$

Definition: Let $D \in \mathbb{Z}$ be a non-square integer.

$\mathbb{Z}[\sqrt{D}]$ = all complex numbers $a + b\sqrt{D}$, $a, b \in \mathbb{Z}$

$\mathbb{Q}[\sqrt{D}]$ = all complex numbers $a + b\sqrt{D}$, $a, b \in \mathbb{Q}$.

Theorem.

1. $\mathbb{Z}[\sqrt{D}]$ and $\mathbb{Q}[\sqrt{D}]$ are rings
2. $\mathbb{Q}[\sqrt{D}]$ is a field.

Example: $\frac{1}{2+\sqrt{3}} = \frac{1}{2+\sqrt{3}} \frac{(2-\sqrt{3})}{(2-\sqrt{3})}$

$= \frac{2-\sqrt{3}}{4-(\sqrt{3})^2} = \frac{2-\sqrt{3}}{1}$

$= 2-\sqrt{3}$.

In general $\frac{1}{a+b\sqrt{D}} = \frac{a-b\sqrt{D}}{a^2-b^2D} = \frac{a}{a^2-b^2D} + \frac{b}{a^2-b^2D}\sqrt{D}$

Back to modular arithmetic...

We can do modular arithmetic in $\mathbb{Z}[\sqrt{D}]$!

E.g., if n is an integer, can consider

$\mathbb{Z}[\sqrt{D}]/(n)$

$\uparrow$

Elements can be represented as

$a + b\sqrt{D}$, $a, b \in \mathbb{Z}/n\mathbb{Z}$.

(so n^2 elements total!).

Example: Which elements are invertible in $\mathbb{Z}[\sqrt{3}]/(7)$? ← All nonzero are invertible, so this a field.

$a + b\sqrt{3}$ $\quad a, b$ in $\mathbb{Z}/7\mathbb{Z} = \mathbb{F}_7$.

$$\frac{1}{a+b\sqrt{3}} \overset{\text{if it exists}}{=} \frac{a-b\sqrt{3}}{a^2-3b^2} = \frac{1}{a^2-3b^2}(a-b\sqrt{3})$$

multiply by $1 = \frac{a-b\sqrt{3}}{a-b\sqrt{3}}$

$a^2 - 3b^2 \in \mathbb{Z}/7\mathbb{Z}$ so it has an inverse $\Leftrightarrow a^2 - 3b^2 \neq 0$.

all have inverses.

	a^2-3b^2	
$1+1\sqrt{3}$	→	$1-3=-2\neq 0$ ✓
$1+2\sqrt{3}$	→	$1-12=-11=3\neq 0$. ✓
$1+3\sqrt{3}$	→	$1-27=-26\neq 0$. ✓
$1+4\sqrt{3}$	→	$1-3\cdot 16=-47\neq 0$ ✓
$1+5\sqrt{3}$		$1-3\cdot 25=-74\neq 0$ ✓
$1+6\sqrt{3}$		$1-3\cdot 36=-107\neq 0$. ✓

Definition: The norm of $a+b\sqrt{D} \in \mathbb{Q}(\sqrt{D})$ is $N(a+b\sqrt{D}) = (a+b\sqrt{D})(a-b\sqrt{D}) = a^2 - b^2D$.

Theorem: $a+b\sqrt{D}$ in $\mathbb{Z}[\sqrt{D}]/(n)$ is invertible if and only if $N(a+b\sqrt{d}) = a^2 - b^2D$

is coprime to n
(i.e. $\gcd(a^2 - b^2 D, n) = 1$).

Corollary: Let $R = \mathbb{Z}[\sqrt{D}]$. Let p be an odd prime not dividing D.

1. If D is not a square mod p then $(R/(p))^\times$ has $p^2 - 1$ elements, thus $R/(p)$ is a field.
2. If D is a square mod p, then $(R/(p))^\times$ has $(p-1)^2$ elements, so is not a field.

Example: $D = -1$, $\sqrt{D} = \sqrt{-1} = i$ "Gaussian integers"

$\mathbb{Z}[\sqrt{D}] = \mathbb{Z}[i]$. $a + bi$, $a, b \in \mathbb{Z}$

-1 is not a square mod 3, so

$\mathbb{Z}[i]/(3)$ is a field with 9 elements!

$a + bi$ $a, b \in \mathbb{Z}/3\mathbb{Z} = \mathbb{F}_3$.

See book – Ch. 3, §3 for more examples / discussion.