Rings & Arithmetic 9: The Gaussian integers

Friday, 28 October 2005

Lectures for Part A of Oxford FHS in Mathematics and Joint Schools

- The ring of Gaussian integers
- Division with remainder
- Gaussian units
- Gaussian primes
- Sums of two squares
- Concluding remarks

The Gaussian integers

Definition. A Gaussian integer is a complex number of the form $a + b\mathrm{i}$ where $a, b \in \mathbb{Z}$. We define

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

Observe that $\mathbb{Z}[\mathrm{i}] \leqslant \mathbb{C}$ and therefore $\mathbb{Z}[\mathrm{i}]$ is an integral domain.

The norm of a Gaussian integer

Define $N : \mathbb{Z}[\mathrm{i}] \to \{0\} \cup \mathbb{N}$ by $N(x) := |x|^2$ for all $x \in \mathbb{Z}[\mathrm{i}]$.
Thus if $x = a + b\mathrm{i}$ then $N(x) = a^2 + b^2$.

Note: $N(x)$ is often called the norm of x; and N the norm function. Note that it is defined on all of $\mathbb{Z}[\mathrm{i}]$, even on 0.

Note: The norm is multiplicative: $N(xy) = N(x)N(y)$ for all $x, y \in \mathbb{Z}[\mathrm{i}]$.

Division in the ring of Gaussian integers

Theorem. *If* $x, y \in \mathbb{Z}[\mathrm{i}]$ *and* $y \neq 0$ *then*

(1) $N(xy) \geqslant N(x)$,

(2) *there exist* $q, r \in \mathbb{Z}[\mathrm{i}]$ *such that* $x = qy + r$ *and* $N(r) < N(y)$.

Thus the ring of Gaussian integers is euclidean.

Proof.

The Gaussian units

Theorem. $U(\mathbb{Z}[\mathrm{i}]) = \{1,\ -1,\ \mathrm{i},\ -\mathrm{i}\}\,.$

Proof.

Gaussian primes, I

Lemma. *Let x be a prime in $\mathbb{Z}[\mathrm{i}]$. Then there is a prime p in $\mathbb{N}$ such that $x|p$ in $\mathbb{Z}[\mathrm{i}]$. Moreover, either $N(x) = p$ or $x = up$ for some $u \in U(\mathbb{Z}[\mathrm{i}])$.*

Proof.

Lemma. *Let p be an ordinary prime number in $\mathbb{N}$. Then p is reducible (prime) in $\mathbb{Z}[\mathrm{i}]$ if and only if $\exists\, a, b \in \mathbb{Z} : p = a^2 + b^2$.*

Proof.

Gaussian primes, II

Lemma. *Let p be an ordinary prime number in $\mathbb{N}$.*

- *If $p = 2$ then $p = (-\mathrm{i})(1 + \mathrm{i})^2$.*
- *If $p \equiv 3 \pmod 4$ then p remains prime in $\mathbb{Z}[\mathrm{i}]$.*
- *If $p \equiv 1 \pmod 4$ then p becomes reducible in $\mathbb{Z}[\mathrm{i}]$—in fact p factorises as a product of two distinct primes in $\mathbb{Z}[\mathrm{i}]$.*

Proof.

Gaussian primes, III

Corollary of these lemmas:

Theorem. *The primes in* $\mathbb{Z}[\mathrm{i}]$ *are (associates of):*

- $1 + i$;
- *primes* p *of* $\mathbb{N}$ *of the form* $4m + 3$; *and*
- *numbers* $a + b\mathrm{i}$ *where* $a, b \in \mathbb{N}$ *and* $a^2 + b^2$ *is prime.*

Examples: $1 + i$, 3, $2 + \mathrm{i}$, $2 - \mathrm{i}$, 7, 11, $3 + 2\mathrm{i}$, $3 - 2\mathrm{i}$, $4 + \mathrm{i}$, $4 - \mathrm{i}$, 19, 23, ... are primes in $\mathbb{Z}[\mathrm{i}]$.

Application to sums of two squares

Theorem. *Every ordinary prime of the form* $4m+1$ *is a sum of two squares.* [Fermat's Two Squares Theorem.]

Theorem. *Let* $n \in \mathbb{N}$. *Factorise* n *as* $p_1^{m_1} p_2^{m_2} \cdots p_k^{m_k}$ *where* $p_1, \ldots, p_k$ *are distinct prime numbers. There exist* $a, b \in \mathbb{N} \cup \{0\}$ *such that* $n = a^2 + b^2$ *if and only if* $p_i \equiv 3 \pmod 4 \Rightarrow m_i$ *is even.*

Summary of the Rings & Arithmetic course

- Definitions: commutative rings with 1, integral domains, fields, etc.;
- Ideals, quotient rings (*e.g:* $\mathbb{Z}_n$; quotient by maximal ideal is a field), homomorphisms, Isomorphism Theorems;
- Arithmetic—units, irreducibles, primes, etc.;
- Euclidean rings:
  - ideals are principal;
  - hcf exists;
  - irreducibles are prime:
  - unique factorisation theorem holds.
- Rings $\mathbb{Z}$, $F[x]$, $\mathbb{Z}[\mathrm{i}]$, ... are euclidean so the theory applies.

The end

Farewell: we start with Linear Algebra on Monday.