Rings & Arithmetic 7: Arithmetic in euclidean rings

Monday, 24 October 2005

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

- Simple properties of euclidean rings
- The principal ideal property
- Important corollaries
- Uniqueness of factorisation
- The euclidean algorithm

Simple facts about euclidean rings R

Let R be a euclidean ring with "valuation" $v : R \setminus \{0\} \to \mathbb{N} \cup \{0\}$.

Fact 1: *For $x, y \in R \setminus \{0\}$, $v(x) = v(xy)$ if and only if $y \in U(R)$.*

Proof.

Fact 2: $v(1) \leqslant v(x)$ *for all $x \in R \setminus \{0\}$ with equality if and only if $x \in U(R)$.*

Proof.

Fact 3: *Let $a \in R \setminus \{0\}$. There exist $k \geqslant 0$, irreducible elements $a_1, a_2, \ldots, a_k$ in R, and $u \in U(R)$ such that $a = u\, a_1\, a_2 \cdots a_k$.*

Proof.

Ideals in euclidean rings

Recall: a principal ideal is an ideal generated by a single element.
If the generator is a then the ideal is denoted Ra or (a).
Principal ideals mirror divisibility: $a|b \iff (b) \subseteq (a)$.

Theorem: *Every ideal in a euclidean ring is principal.*

Proof.

Note: an integral domain in which every ideal is principal is known as a principal ideal domain (PID).

Important corollaries

Theorem: *In a principal ideal domain R, and, in particular, in a euclidean ring R, highest common factors exist. Moreover, if $d = \mathsf{hcf}(a, b)$ then there exist $u, v \in R$ such that $d = ua + vb$.*

Proof.

Theorem: *In a principal ideal domain R, and, in particular, in a euclidean ring R, irreducible elements are prime.*

Proof.

Uniqueness of factorisation, I

Definition: Let $a \in R$ where R is an integral domain. We'll say that factorisations

$$a = u\, p_1 \cdots p_k = v\, q_1 \cdots q_m\,,$$

where $u, v \in U(R)$ and $p_1, \ldots, p_k$, $q_1, \ldots, q_m$ are irreducible elements of R, are essentially the same if $k = m$ and the elements q_i can be re-labelled so that $q_i \sim p_i$ for $1 \leqslant i \leqslant k$. We'll say that an element a of a commutative ring R with 1 is uniquely factorisable into irreducibles if there exists such a factorisation and all factorisations into irreducibles are essentially the same.

Definition: A unique factorisation domain (UFD) is an integral domain in which every non-zero element is uniquely factorisable into irreducibles.

Uniqueness of factorisation, II

Theorem. *A euclidean ring is a unique factorisation domain.*

Proof.

Commentary

Note: As a special case we get the "Fundamental Theorem of Arithmetic"—uniqueness of factorisation in $\mathbb{Z}$ or in $\mathbb{N}$.

Note: As another special case we get uniqueness of factorisation in the polynomial ring $F[x]$ where F is a field.

Note: Factorising is difficult.

Note: In fact every PID is a UFD. Proof of existence of a factorisation is non-trivial (at the level of a Mars-bar Challenge). Proof of uniqueness, however, is exactly the same as in the case of euclidean rings.

The euclidean algorithm, I

Question: How can one **find** highest common factors? Factorisation is often impracticable.

Notation: If $a = qb + r$ where $r = 0$ or $v(r) < v(b)$ we write $a \div b$ for q and $\text{res}\, a \pmod{b}$ for r.

Observation: Given a, b, division of a by b (when $b \neq 0$) to **find** $a \div b$ and $\text{res}\, a \pmod{b}$ is done by a Division Algorithm.

Observation: If $a = qb + r$ then $\text{hcf}(a, b) = \text{hcf}(b, r)$.

The euclidean algorithm, II

Assume a Division Algorithm in R.

Input: elements a, b of euclidean ring R;

Output: hcf(a, b) .

Begin: while $b \neq 0$ do

$r := \text{res } a \pmod b$ [use Division Algorithm];

$a := b$;

$b := r$;

endwhile;

return a;

End.

Proof of correctness.

The extended euclidean algorithm

Input: elements a, b of euclidean ring R;

Output: $\mathrm{hcf}(a, b)$
and elements $u, v \in R$ such that $\mathrm{hcf}(a, b) = ua + vb$.

This is an interesting exercise for you.