Rings & Arithmetic 5: Some important points

Thursday, 20 October 2005

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

- Example: a number theoretic fact
- The Chinese Remainder Theorem
- Examples
- Highest common factors

Example: a number-theoretic fact

Theorem. If p is an odd prime number then there exists $a \in \mathbb{N}$ such that $a^2 \equiv -1 \pmod{p}$ if and only if $p \equiv 1 \pmod{4}$.

Proof. (1) The case $p \equiv 3 \pmod{4}$.

The proof continued

(2) The case $p \equiv 1 \pmod 4$: suppose $p = 4m+1$, let $M := \mathbb{Z}_p^\times$, a multiplicative group of order $4m$.

- If $k \in M$ and $\operatorname{ord} k = 2$ then $k = -1$.
- If $\varphi : M \to M$ is given by $\varphi(x) = x^2$ then φ is a group homomorphism. Also $\operatorname{Ker}\varphi = \{\pm 1\}$, and so $|\operatorname{Im}\varphi| = 2m$.
- There exists $k \in \operatorname{Im}\varphi$ with $\operatorname{ord} k = 2$.
- Thus -1 is a square.

Note: There are many other proofs.

The Chinese Remainder Theorem I

Definition: Ideals A, B of a ring R are said to be co-prime if $A + B = R$.

Example: Ideals $12\mathbb{Z}$, $7\mathbb{Z}$ are co-prime in $\mathbb{Z}$. Generally, if m, n are co-prime integers then $m\mathbb{Z}$, $n\mathbb{Z}$ are co-prime ideals in $\mathbb{Z}$.

Theorem: *Let R, S_1, S_2 be rings (commutative, with 1) and let $\varphi_1 : R \to S_1$, $\varphi_2 : R \to S_2$ be homomorphisms. Then*

(1) *there is a natural homomorphism $\varphi : R \to S_1 \times S_2$ with* $\mathrm{Ker}\,\varphi = \mathrm{Ker}\,\varphi_1 \cap \mathrm{Ker}\,\varphi_2$;

(2) *if φ_1, φ_2 are surjective and* $\mathrm{Ker}\,\varphi_1$, $\mathrm{Ker}\,\varphi_2$ *are co-prime then φ is surjective.*

Proof.

The Chinese Remainder Theorem, II

Corollary [Chinese Remainder Theorem, abstract form]: *If A, B are co-prime ideals in a ring R then $R/(A \cap B) \cong R/A \times R/B$.*

Example: if m, n are co-prime integers then $\mathbb{Z}_{mn} \cong \mathbb{Z}_m \times \mathbb{Z}_n$.

More generally: if $m_1, m_2, \ldots, m_k$ are pairwise co-prime integers and $n = m_1 m_2 \cdots m_k$ then $\mathbb{Z}_n \cong \mathbb{Z}_{m_1} \times \mathbb{Z}_{m_2} \times \cdots \times \mathbb{Z}_{m_k}$.

In particular: if $n = p_1^{\alpha_1} \cdots p_k^{\alpha_k}$, where $p_1, \ldots, p_k$ are distinct prime numbers then $\mathbb{Z}_n \cong \mathbb{Z}_{q_1} \times \cdots \times \mathbb{Z}_{m_k}$, where $q_i := p_i^{\alpha_i}$.

The Chinese Remainder Theorem, III

Corollary [Chinese Remainder Theorem, classical form]:
If $m_1, m_2, \ldots, m_k$ are pairwise co-prime integers and $c_1, c_2, \ldots, c_k \in \mathbb{Z}$ then there exists $x \in \mathbb{Z}$ such that $x \equiv c_i \pmod{m_i}$ for $1 \leqslant i \leqslant k$.

Moreover, x is unique up to addition of multiples of $m_1 m_2 \cdots m_k$.

An example from Hardy and Wright

Example. Six professors begin courses of lectures on Monday, Tuesday, Wednesday, Thursday, Friday, and Saturday, and announce their intentions of lecturing at intervals of two, three, four, one, six and five days respectively. The regulations of the university forbid Sunday lectures (so that a Sunday lecture must be omitted). When first will all six professors find themselves compelled to omit a lecture?

Highest common factors, I

Definition. Element b divides element a in R (and we write $b|a$) if $\exists c \in R : a = bc$.

Definition. Elements a, b are said to be associates (and we write $a \sim b$) if $\exists u \in U(R) : a = ub$.

Note: $a \sim b$ if and only if $a|b$ & $b|a$.
Also $a \sim b$ if and only if $(a) = (b)$.

Definition: A highest common factor (also known as greatest common divisor) of elements a, b of R is an element d with the properties:

(1) $d|a$ & $d|b$ and (2) $c|a$ & $c|b \Rightarrow c|d$.

Highest common factors, II

Note: This general definition is different from the classical definition in $\mathbb{N}$. You should think why they come to essentially the same thing in $\mathbb{N}$.

Note: Highest common factor of a, b is not unique. If d is a highest common factor of a, b then so is any associate of d; conversely, if d_1, d_2 are highest common factors of a, b then $d_1 \sim d_2$.

Note: Nevertheless, we write $d = \mathrm{hcf}(a, b)$.

Note: Highest common factor of a, b does not necessarily exist. Example: If $R = \mathbb{Z}[\sqrt{-5}] = \{a + b\sqrt{-5} \mid a, b \in \mathbb{Z}\} \leqslant \mathbb{C}$ then $\mathrm{hcf}(6, 2 + 2\sqrt{-5})$ does not exist.