MATH H113: Honors Introduction to Abstract Algebra

2016-04-15

- Chinese Remainder Theorem
- Euclidean domains

Homework 4/22:
Sect. 7.6: 1, 3, 5c, 7
Sect. 8.1: 3, 7, 11
Sect. 8.2: 8 (Assume $D \neq \emptyset$ and $0 \notin D$)

Chinese Remainder Theorem

Theorem (Chinese Remainder Theorem): Let R be a commutative ring with 1, and let $A_1, \ldots, A_k$ be ideals in R.

a. The map $\phi : R \to (R/A_1) \times \cdots \times (R/A_k)$ is a ring homomorphism and its kernel is $A_1 \cap \ldots \cap A_k$.
b. Assume that A_i and A_j are comaximal $\forall i \neq j$. Then $A_1 \cap \ldots \cap A_k = A_1 A_2 \ldots A_k$, and ϕ induces an isomorphism $R/A_1A_2 \ldots A_k = R/(A_1 \cap \ldots \cap A_k) \cong (R/A_1) \times \cdots \times (R/A_k)$.

(Non-)Proof: We proved the $k = 2$ case already. The cases $k > 2$ are proved by induction (see the book). It's also true for $k = 1$ (easy), and for $k = 0$ ($A_1 \ldots A_k = A_1 \cap \ldots A_k = R$ and $(R/A_1) \times \ldots \times (R/A_k) = (0)$).
Example: Find all residue classes $x \mod 21$ that satisfy $x^2 \equiv 4 \pmod{21}$.
We have $\mathbb{Z}/21\mathbb{Z} \cong (\mathbb{Z}/3\mathbb{Z}) \times (\mathbb{Z}/7\mathbb{Z})$.
If $n \in \mathbb{Z}$ and $n^2 \equiv 4 \pmod{21}$) then $x^2 \equiv 4 \pmod 3$ and $x^2 \equiv 4 \pmod 7$.
And conversely if $n^2 \equiv 4 \pmod 3$ and $n^2 \equiv 4 \pmod 7$ then $a = (\bar{n}, \bar{n}) \in (\mathbb{Z}/3\mathbb{Z}) \times (\mathbb{Z}/7\mathbb{Z})$ satisfies $a^2 = (\bar{4}, \bar{4})$
$\therefore$ (applying ϕ^{-1}): $b = \bar{n} \in \mathbb{Z}/21\mathbb{Z}$ satisfies $b^2 = \bar{4} \in \mathbb{Z}/21\mathbb{Z}$.
Solve $x^2 \equiv 4 \pmod 3$
$0^2 = 0 \not\equiv 4$
$1^2 = 1 \equiv 4$
$2^2 = 4 \equiv 4$
Solutions are $1, 2 \pmod 3$
Solve $x^2 \equiv 4 \pmod 7$

n	0	1	2	3	4	5	6
$n^2 \mod 7$	0	1	4	2	2	4	1

Solutions are $2, 5 \pmod 7$

$x \mod 3$	$x \mod 7$	$x \mod 21$
1	2	16
1	5	19
2	2	2
2	5	5

Slightly bigger example (part of Ex. 4 p. 248):
Solve for $x^2 \equiv x \pmod{30}$
$\mathbb{Z}/30\mathbb{Z} \cong (\mathbb{Z}/2\mathbb{Z}) \times (\mathbb{Z}/3\mathbb{Z}) \times (\mathbb{Z}/5\mathbb{Z})$
all with solutions (0, 1) of $x^2 \equiv x \pmod{2, 3, 5}$
(If p is prime then $\mathbb{Z}/p\mathbb{Z}$ is a field, $\therefore$ it's an integral domain.
So $x^2 = x$ in $\mathbb{Z}/p\mathbb{Z} \iff x(x-1) = 0 \iff x = 0 \vee x = 1$

$n \mod 2$	$n \mod 3$	$n \mod 5$	$n \mod 30$
0	0	0	0
0	0	1	6
0	1	0	10
0	1	1	16
1	0	0	15
1	0	1	21
1	1	0	25
1	1	1	1

General idea: to solve a given polynomial equation with integer coefficients mod $n = p_1^{a_1} \cdots p_r^{a_r}$ it's equivalent to solving it $\mod p_i^{a_i}$ $\forall i$ (assuming the p_i are all distinct).

Euclidean Domains

We'lls see that you can do the Euclidean algorithm in ring's other than $\mathbb{Z}$. Especially: $F[x]$, where F is any field. *For the rest of today's lecture, all rings are assumed to be commutative.*

Definition: Let R be an integral domain. Then:

a. A *norm* on R is a function $N : R \to \mathbb{N}$ such that $N(0) = 0$.
b. A norm N on R is *positive* if $N(r) > 0$ for all $r \neq 0$.
c. A norm N on R is *Euclidean* if for all $a, b \in R$ with $b \neq 0$ there are $q, r \in R$ such that $a = qb + r$ and $r = 0$ or $N(r) < N(b)$.

Example: $R = \mathbb{Z}$, $N(n) = |n|$
$7 = 2 \cdot 3 + 1$ $N(1) = 1 < 3 = N(3)$
or
$7 = 3 \cdot 3 - 2$ $N(-2) = 2 < 3 = N(3)$
(So we're dropping uniqueness)
Definition: A *Euclidean domain* is an integral domain with a Euclidean norm.
Examples:

1. $\mathbb{Z}$ is a Euclidean domain with $N(n) = |n|$
2. Similarly for $N(n) = \begin{cases} 0 & n = 0 \\ |n| - 1 & n \neq 0 \end{cases}$
3. Similarly for $N(n) = 2^{|n|} - 1$
4. $R = \{x + iy : x, y \in \mathbb{Z}\}$ (subring in $\mathbb{C}$)
   This is called the ring of Gaussian integers, $\mathbb{Z}[i]$.
   Let $N(x + iy) = x^2 + y^2 = |x + iy|^2$.
   This is a Euclidean norm on $\mathbb{Z}[i]$.
   Proof: N maps $\mathbb{Z}[i]$ to $\mathbb{N}$ and $N(0) = 0$. easy.
   In the complex plane, $\mathbb{Z}[i]$ looks like:
   Let $\alpha, \beta \in \mathbb{Z}[i], \beta \neq 0$.
   $\mathbb{Z}[i]$ is ($\cdot$ or $\star$)
   $\beta\mathbb{Z}[i] \subseteq \mathbb{Z}[i]$ is $\star$
   $\beta = 2 + i$
   $i\beta = -1 + 2i$

You can cover the plane with squares with vertices $(n + mi)\beta$, $(n + 1 + mi)\beta$, $n + (m + 1)\beta$, $(n + 1 + (m + 1)i)\beta$\$. In each square, for any point inside that square, the distance to the nearest vertex is at most $\frac{|\beta|}{\sqrt{2}}$
So given α, $\exists q \in \mathbb{Z}[i]$ such that $|q\beta - \alpha| \leq \frac{\beta}{\sqrt{2}}$ so $N(q\beta - \alpha) = N(\alpha + q\beta) \leq (\frac{|\beta|^2}{2} < |\beta|^2 = N(\beta)$.
That's the "division algorithm" for $\mathbb{Z}[i]$.

See picture

5. Let F be any field, and let $R = F[x]$.
   Define $N(f(x)) = \begin{cases} \deg f & f(x) \neq 0 \\ 0 & f(x) = 0 \end{cases}$.
   Then N is a Euclidean norm, so $F[x]$ is a Euclidean domain. (See Ex. 8.4.14)
6. Let F be any field and let $N : F \to \mathbb{N}$ be *any* norm. Then N is a Euclidean norm.
   Given $a, b \in F$ with $b \neq 0$, let $q = \frac{d}{b}$ and $r = 0$ $(a = qb + r)$.
   Let R be an integral domain in which $N(r) = 0$ $\forall r$ is a Euclidean norm.
   Then R must be a field. Take any $b \in R$, $b \neq 0$, and let $a = 1$. Then

$1 = qb + r$ with $q, r \in R$ and $r = 0$ or $N(r) < N(b) = 0$ (can't happen)
$\therefore 1 - qb$, so b is a unit $\forall$ nonzero $b \in R$.
R is a field

($R[x, y]$ is not a Euclidean domain)