Lecture 9

7.6

A numeric version of the Chinese Remainder Theorem was known to the ancient Chinese - pre-common era - and used for computing troop supplies. It is useful for all sorts of problems.

Suppose we want to solve the pair of congruences $x \equiv 4 \pmod 7$ and $x \equiv 14 \pmod{30}$ for x. (This could be asking to find a day of the week and a time of the month in terms of the entire year.) Is there a solution? What is a good way to find it? The ancient Chinese worked out a method that is still computationally viable.

Theorem (Chinese Remainder Theorem)

Every system of congruences

$$\begin{aligned} x &\equiv a_1 \pmod{m_1} \\ x &\equiv a_2 \pmod{m_2} \\ &\vdots \\ x &\equiv a_k \pmod{m_k}, \end{aligned}$$

where the m_i are pairwise relatively prime, has a solution. Furthermore, every two solutions are congruent $\mod M$, where $M = m_1 m_2 \ldots m_k$.

We prove the Chinese Remainder Theorem constructively as follows.

1. If $M_i = M/m_i$, then the $\gcd(M_i, m_i) = 1$ since the m_i are pairwise relatively prime.

2. We need to find a way to determine c_i so that $c_i M_i \equiv 1 \pmod{m_i}$. But we already know that, for each i, we can use the Euclidean algorithm to find integers c_i and f_i such that $c_i M_i + f_i m_i = 1$. Then $c_i M_i \equiv 1 \pmod{m_i}$. For small numbers, it is often easier to use guess and check, but the Euclidean algorithm always works and this is a proof.

3. We can use the a_i, c_i, and M_i to get a formula for a solution x_0, namely, set
$$x_0 = a_1c_1M_1 + a_2c_2M_2 + \cdots + a_kc_kM_k.$$
Since $M_j \equiv 0 \pmod{m_i}$ when $i \neq j$, and $a_ic_iM_i \equiv a_i \pmod{m_i}$ by the choice of c_i, we have $x_0 \equiv a_i \pmod{m_i}$ for all i.

4. Now we need to show that if $x_1 \equiv a_i \pmod{m_i}$ for all i, then $x_1 \equiv x_0 \pmod{M}$. Let x_1 be any other solution to the system of congruences. Then $x_1 \equiv a_i \equiv x_0 \pmod{m_i}$ for every i, which means that $x_0 - x_1$ is divisible by m_i for each i. Since the m_i are pairwise relatively prime, $M = m_1m_2 \ldots m_k$ divides $x_0 - x_1$. Therefore, $x_1 \equiv x_0 \pmod{M}$.

Let's see how this works out in practice. Let's use the Chinese Remainder Theorem to solve the following pair of congruences for x.
$$\begin{aligned} x &\equiv 4 \pmod{7} \\ x &\equiv 14 \pmod{30} \end{aligned}$$

We use the procedure of the Theorem with $m_1 = 7$ and $m_2 = 30$. Then $M = 210$, $M_1 = 30$, and $M_2 = 7$. We use the Euclidean algorithm to write 1 as a linear combination of 7 and 30:
$$\begin{aligned} 30 &= 4 \cdot 7 + 2 \qquad & 1 &= 7 - 3 \cdot 2 \\ 7 &= 3 \cdot 2 + 1 & &= 7 - 3 \cdot (30 - 4 \cdot 7) \\ & & &= 13 \cdot 7 - 3 \cdot 30. \end{aligned}$$

Therefore $c_1 = -3$ and $c_2 = 13$. Hence $x_0 = 4 \cdot (-3) \cdot 30 + 14 \cdot 13 \cdot 7 = -360 + 1274 = 914$ is a solution. For a smaller solution, we may take $x_0 \pmod{210}$ to get $x' = 74$.

Notice that this version of the Chinese Remainder Theorem has $R = \mathbb{Z}$ and the $A_j = n_j\mathbb{Z}$. This completes 7.6.5a and b. I'm leaving part c for you to practice on.

7.6.1: Let R be a ring with identity $1 \neq 0$. An element $e \in R$ is called idempotent if $e^2 = e$. Assume that e is an idempotent in R and the $er = re$ for all $r \in R$. Then Re and $R(1-e)$ are left ideals by definition. If $r, s \in R$, then $(re)s = r(es) = r(se) = (rs)e \in Re$. Similarly, $r(1-e)s = r(s - es) =$

$r(s - se) = rs(1 - e) \in R(1 - e)$. Therefore both Re and $R(1 - e)$ are two-sided ideals.

$(re)e = re^2 = re$ and $ere = e^2r = er$. Therefore e is the identity of Re. Note that $(1-e)^2 = 1-2e+e^2 = 1-2e+e = 1-e$, so $1-e$ is also idempotent. Then, $(r(1-e))(1-e) = r(1-e)^2 = r(1-e)$ and $(1-e)r(1-e) = (1-e)(r-re) = (1-e)(r-er) = (1-e)^2r = (1-e)r$. Therefore $(1-e)$ is the identity of $R(1-e)$.

Overview

We have now studied the basic algebraic objects and connections between them. The rest of the course will be on special topics.

Chapter 8 We know from high school and undergraduate studies that the integers have many special properties. For example, there is the Euclidean algorithm by which we can find the greatest common divisor of two integers and write it as a linear combination of the original integers. We learned in this class that every ideal of the integers is principal, namely, $n\mathbb{Z} = (n)$. Lastly, we have the Fundamental Theorem of Arithmetic that every positive integer at least 2 can be written uniquely as $p_1^{n_1} \cdots p_s^{n_s}$ where $p_1 < \cdots < p_s$. In chapter 8 we investigate these properties for other rings and discover that fields are a proper subset of Euclidean Rings, i.e., rings with a Euclidean algorithm, that Euclidean Rings are a proper subset of Principal Ideal Domains, i.e., integral domains in which every ideal is principal. And lastly, that Principal Ideal Domains are a proper subset of Unique Factorization Domains in which every element can be written as a unit times a product of irreducible elements.

Mostly we need the concepts and some of the computational parts of this chapter, so we will do a quick overview with a few homework problems to set the concepts and computational aspects. We'd skip the chapter except that we need the concepts to make sense of the next big topic.

Information on Chapter 8

In Chapter 8, all rings are commutative and integral domains. One basic measure of size is a generalization of the usual absolute value on the integers. You need to read the section to understand the rest of the chapter. I'll hit the high points.

Definition: Any function $N : R \to \mathbb{Z}^+ \cup \{0\}$ with $N(0) = 0$ is called a norm on R. Mostly we work with positive norms, namely, that, if $a \neq 0$, then $N(a) > 0$, i.e. 0 is the only element whose norm is 0.

8.1 An integral domain R is said to be a Euclidean Domain if there is a norm N on R such that, for any two elements $a, b \in R$ with $b \neq 0$, there exist $q, r \in R$ such that $a = qb + r$ with $r = 0$ or $N(r) < N(b)$. As usual q is called the quotient and r the remainder.

This definition is enough to produce the Euclidean Algorithm in any Euclidean domain (see page 271) and is the generalization of the Euclidean Algorithm on the integers (page 5). The proof that the last non-zero remainder in the Euclidean Algorithm is the greatest common divisor and can be written as a linear combination of the original a, b is again identical to the proof for the integers.

One consequence is that every ideal in a Euclidean Domain is principal, i.e., $I = (d)$ for some $d \in R$. We will see that there are rings in which every ideal is principal but are not Euclidean domains.

Just as there is a generalization of gcd, we can define the least common multiple (lcm) of a, b to be $e \in R$ such that $a|e$, $b|e$ and if $a|e'$, $b|e'$, then $e|e'$ where $a|e$ is notation for a divides e. In a Euclidean domain, any two elements $a, b \in R$, $b \neq 0$ have a $\text{lcm}(a, b) = ab/(a, b)$ just as in the integers.

An important example of a Euclidean domain that is not the integers is $F[x]$, polynomials over a field F where the norm is the degree of the polynomial. Notice that this norm is not positive since the norm of any constant is 0. In this book, the degree of 0 is 0 but in many others it is undefined or $-\infty$.

8.2 A Principal Ideal Domain (PID) is an integral domain in which every ideal is principal. In section 8.1, it was shown that every Euclidean domain is a PID. In particular, $F[x]$ is a PID. Note that $\mathbb{Z}[x]$ is not a PID because $(2, x)$ is not principal but requires the two generators. To see this, suppose $(2, x) = (f(x))$. Then $2 = f(x)g(x)$. Since $\mathbb{Z}$ is an integral domain, $\deg(fg) = \deg(f) + \deg(g) = 0$. Therefore, $\deg(f) = \deg(g) = 0$, so $f = c \in \mathbb{Z}$. By unique factorization, $f = 2$ or $f = -2$. Then $x = 2g(x)$, when $g = x/2 \notin \mathbb{Z}[x]$. Therefore, $(2, x)$ is not principal. We will see in 8.3 that $\mathbb{Z}[x]$ is a unique factorization domain (UFD).

A PID still has greatest common divisors which are linear combinations of the original elements and least common multiples, but there isn't a Euclidean algorithm so they are harder to find.

The biggest result of the section is that, in a PID, every non-zero prime ideal is maximal. As a corollary, we see that $R[x]$ is a PID implies that R is a field.

8.2.1: Let R be a PID. Then (a) and (b) are comaximal, i.e., $(a) + (b) = R$ if and only if $1 = xa + yb$ for some $x, y \in R$ if an only if $(a, b) = 1$.

8.2.2 Suppose R is a PID and a, b be non-zero elements in R. Let $(e) = (a) \cap (b)$. Then $e \in (a)$, so $a|e$ and, similarly, $b|e$. If $a|f$ and $b|f$, then $f \in (a) \cap (b) = (e)$, whence $e|f$. Therefore $e = lcm(a, b)$.

8.2.3: Suppose R is a PID and that (p) is a prime ideal. Then R/I is an integral domain. Let $\pi : R \to R/I$ be the usual projection surjective homomorphism. By exercise 7.3.24 $I = \pi^{-1}\overline{J}$ is an ideal for J an ideal of R/I. But R is a PID, so $I = (a)$ for some $a \in R$. Thus, since π is surjective, $J = \pi(I) = \pi((d)) = (\overline{d})$ is principal.

8.3 We are now ready for the third least restrictive integral domain, a unique factorization domain or UFD. To understand what is going on, we need to make a distinction between prime and irreducible as we are used to using prime for positive integers and irreducible for real polynomial such as $x^2 + 1$. Please note that these definitions hold in an integral domain.

A non-zero, non-unit element $r \in R$ is *irreducible* in R if, whenever $r = ab,\ a, b \in R$ at least one of a, b must be a unit in R. Otherwise r is said to be reducible. Please notice that this looks very like our definition of a prime number in the positive integers since 1 is the only unit in $\mathbb{Z}^+$. We will see why in a moment.

A nonzero element $p \in R$ is called *prime* in R if the ideal (p) generated by p is a prime ideal. In other words, a nonzero element p is a prime if it is not a unit and whenever $p|ab,\ p|a$ or $p|b$. In the positive integers, we used the definition for irreducible for prime and then proved the condition for prime listed here. The reason it doesn't matter is, that in a PID every non-zero element is prime if and only if it is irreducible and Z is a PID.

Please notice the theorem that says that prime implies irreducible. Also, note that it depends on the ring whether or not something is prime or irreducible. For example $x^2 + 1$ is irreducible in $\mathbb{R}[x]$ but reducible in $\mathbb{C}[x]$.

A last definition is that $a, b \in R$ are associates if and only if $a = ub$ for some unit $u \in R$.

We now can state that an integral domain R is a *Unique Factorization Domain* (UFD) if every nonzero element $r \in R$ which is not a unit can be written uniquely up to order of irreducibles and associates as $R = p_1 p_2 \cdots p_n$ where the p_i are irreducible in R.

For example, $\mathbb{Z}[x]$ is a UFD but we saw it was not a PID. However, in a UFD r is prime if and only if it is irreducible, just as was true for a PID. Since we will see in chapter 9 that, if R is a UFD, then $R[x]$ is a UFD, almost all the integral domains we know are UFDs, which is why the distinction between irreducible and prime seems so odd.

One nice thing about a UFD is that we can find the greatest common divisor and least common multiple the same way we do from the fundamental theorem of arithmetic, i.e., from the factorizations. See Proposition 13.

I leave it to you to read the rest of the chapter. I find the number theory theorems interesting.

8.3.3: Let $n = 2130797 = 17^2 \cdot 73 \cdot 101$. Then, in the notation of Corollary 19, $a_1 = 2, a_2 = 1, a_3 = 1$. So the number of ways of representing n as the sum of two squares is $4(2+1)(1+1)(1+1) = 48$, which is too many to list them all.

8.3.4: Suppose an integer n is the sum of two rational squares, i.e., $n = a^2/b^2 + c^2/d^2$ where $(a,b) = 1 = (c,d)$. Then $n = (a^2d^2 + c^2b^2)/b^2d^2$. Since n is an integer, if $p|b$ for p a prime, then $p^2|(a^2d^2 + c^2b^2)$, so $p^2|a^2d^2$. But $(a,b) = 1$ implies that $(a,p) = 1$, whence $p^2|d^2$ and $p|d$. It follows that $|b|||d|$. By reversing the roles of b and d, see that $b^2 = d^2$, so $n = (a^2 + c^2)/b^2$. Therefore, $nb^2 = a^2 + c^2$. Since all the exponents of the primes dividing b^2 are even, by Corollary 19 all the primes of n which are congruent to $3 \mod 4$ have even degree in the factorization of n. Thus, n can be written as the sum of two integer squares.