MATH 415

Modern Algebra I

Lecture 24: Euclidean algorithm. Chinese remainder theorem.

Generators of an ideal

Let R be an integral domain.

Theorem 1 Suppose I_α, $\alpha \in A$ is a nonempty collection of ideals in R. Then the intersection $\bigcap_\alpha I_\alpha$ is also an ideal in R.

Let S be a set (or a list) of some elements of R. The **ideal generated by** S, denoted (S) or $\langle S \rangle$, is the smallest ideal in R that contains S.

Theorem 2 The ideal (S) is well defined. Indeed, it is the intersection of all ideals that contain S.

Theorem 3 If $S = \{a_1, a_2, \dots, a_k\}$ then the ideal (S) consists of all elements of the form $r_1 a_1 + r_2 a_2 + \cdots + r_k a_k$, where $r_1, r_2, \dots, r_k \in R$.

An ideal $(a) = aR$ generated by a single element is called **principal**. The ring R is called a **principal ideal domain (PID)** if every ideal is principal.

Greatest common divisor

Definition. Let R be an integral domain. Given nonzero elements $a_1, a_2, \ldots, a_k \in R$, their **greatest common divisor** $\gcd(a_1, a_2, \ldots, a_k)$ is an element $c \in R$ such that

- c is a common divisor of $a_1, a_2, \ldots, a_k$, i.e., $a_i = cq_i$ for some $q_i \in R$, $1 \leq i \leq k$,
- any common divisor of $a_1, a_2, \ldots, a_k$ is a divisor of c as well.

If $\gcd(a_1, a_2, \ldots, a_k)$ exists then it is unique up to multiplication by a unit.

Note that an element $c \in R$ is a common divisor of the elements $a_1, a_2, \ldots, a_k$ if and only if all these elements belong to the principal ideal cR. Another common divisor d is a divisor of c if and only if $cR \subset dR$. Therefore $\gcd(a_1, a_2, \ldots, a_k)$, if it exists, is a generator of the smallest principal ideal containing $a_1, a_2, \ldots, a_k$.

Theorem If R is a principal ideal domain, then

(i) the greatest common divisor $\gcd(a_1, a_2, \ldots, a_k)$ exists for any nonzero elements $a_1, a_2, \ldots, a_k \in R$;

(ii) $\gcd(a_1, a_2, \ldots, a_k) = r_1 a_1 + r_2 a_2 + \cdots + r_k a_k$ for some $r_1, r_2, \ldots, r_k \in R$.

Proof. Consider an ideal $I = (a_1, a_2, \ldots, a_k)$ generated by the elements $a_1, a_2, \ldots, a_k$. Since the ring R is a principal ideal domain, we have $I = cR$ for some $c \in R$. It follows that $c = \gcd(a_1, a_2, \ldots, a_k)$. Moreover, since $c \in I$, we have $c = r_1 a_1 + r_2 a_2 + \cdots + r_k a_k$ for some $r_1, r_2, \ldots, r_k \in R$.

Relatively prime elements

Definition. Let R be an integral domain. Nonzero elements $a, b \in R$ are called **relatively prime** (or **coprime**) if $\gcd(a, b) = 1$.

Theorem Suppose R is a principal ideal domain. If a nonzero element $c \in R$ is divisible by two coprime elements a and b, then it is divisible by their product ab.

Proof: By assumption, $c = aq_1$ and $c = bq_2$ for some $q_1, q_2 \in R$. Since $\gcd(a, b) = 1$ and R is a principal ideal domain, it follows that $r_1 a + r_2 b = 1$ for some $r_1, r_2 \in R$. Then $c = c(r_1 a + r_2 b) = r_1 ca + r_2 cb = r_1 q_2 ab + r_2 q_1 ab$ $= (r_1 q_2 + r_2 q_1) ab$, which implies that c is divisible by ab.

Corollary Suppose R is a principal ideal domain. If a nonzero element $c \in R$ is divisible by pairwise coprime elements $a_1, a_2, \dots, a_k$, then it is divisible by their product $a_1 a_2 \dots a_k$.

Euclidean rings

Let R be an integral domain. A function $E : R \setminus \{0\} \to \mathbb{Z}_+$ is called a **Euclidean function** on R if for any $x, y \in R \setminus \{0\}$ we have $x = qy + r$ for some $q, r \in R$ such that $r = 0$ or $E(r) < E(y)$.

The ring R is called a **Euclidean ring** (or **Euclidean domain**) if it admits a Euclidean function.

In a Euclidean ring, division with remainder is well defined.

Theorem Any Euclidean ring is a principal ideal domain.

Euclidean algorithm

Lemma 1 If b divides a then $\gcd(a, b) = b$.

Lemma 2 Suppose R is a Euclidean ring. If b does not divide a and r is the remainder of a when divided by b, then $\gcd(a, b) = \gcd(b, r)$.

Idea of the proof: Since $a = bq + r$ for some $q \in R$, the pairs a, b and b, r have the same common divisors.

Theorem Suppose R is a Euclidean ring. Given two nonzero elements $a, b \in R$, there is a sequence $r_1, r_2, \dots, r_k$ such that $r_1 = a$, $r_2 = b$, r_i is the remainder of r_{i-2} when divided by r_{i-1} for $3 \le i \le k$, and r_k divides r_{k-1}. Then $\gcd(a, b) = r_k$.

Example. $R = \mathbb{Z}$, $a = 1356$, $b = 744$.
$\gcd(a, b) = ?$

We obtain

$$
\begin{aligned}
&1356 = 744 \cdot 1 + 612,\\
&744 = 612 \cdot 1 + 132,\\
&612 = 132 \cdot 4 + 84,\\
&132 = 84 \cdot 1 + 48,\\
&84 = 48 \cdot 1 + 36,\\
&48 = 36 \cdot 1 + 12,\\
&36 = 12 \cdot 3.
\end{aligned}
$$

Thus $\gcd(1356, 744) = 12$.

Problem. Find an integer solution of the equation $1356m + 744n = 12$.

Let us use calculations done for the Euclidean algorithm applied to 1356 and 744.

$1356 = 744 \cdot 1 + 612$
$\implies 612 = 1 \cdot 1356 - 1 \cdot 744$

$744 = 612 \cdot 1 + 132$
$\implies 132 = 744 - 612 = -1 \cdot 1356 + 2 \cdot 744$

$612 = 132 \cdot 4 + 84$
$\implies 84 = 612 - 4 \cdot 132 = 5 \cdot 1356 - 9 \cdot 744$

$132 = 84 \cdot 1 + 48$
$\implies 48 = 132 - 84 = -6 \cdot 1356 + 11 \cdot 744$

$84 = 48 \cdot 1 + 36$
$\implies 36 = 84 - 48 = 11 \cdot 1356 - 20 \cdot 744$

$48 = 36 \cdot 1 + 12$
$\implies 12 = 48 - 36 = -17 \cdot 1356 + 31 \cdot 744$

Thus $m = -17$, $n = 31$ is a solution.

Alternative solution. Consider a matrix $\left(\begin{array}{cc|c} 1 & 0 & 1356 \\ 0 & 1 & 744 \end{array}\right)$,

which is the augmented matrix of a system $\begin{cases} x = 1356, \\ y = 744. \end{cases}$

We are going to apply elementary row operations to this matrix until we get 12 in the rightmost column.

$$\left(\begin{array}{cc|c} 1 & 0 & 1356 \\ 0 & 1 & 744 \end{array}\right) \to \left(\begin{array}{cc|c} 1 & -1 & 612 \\ 0 & 1 & 744 \end{array}\right) \to \left(\begin{array}{cc|c} 1 & -1 & 612 \\ -1 & 2 & 132 \end{array}\right)$$

$$\to \left(\begin{array}{cc|c} 5 & -9 & 84 \\ -1 & 2 & 132 \end{array}\right) \to \left(\begin{array}{cc|c} 5 & -9 & 84 \\ -6 & 11 & 48 \end{array}\right) \to \left(\begin{array}{cc|c} 11 & -20 & 36 \\ -6 & 11 & 48 \end{array}\right)$$

$$\to \left(\begin{array}{cc|c} 11 & -20 & 36 \\ -17 & 31 & 12 \end{array}\right) \to \left(\begin{array}{cc|c} 62 & -113 & 0 \\ -17 & 31 & 12 \end{array}\right)$$

Hence the above system is equivalent to

$$\begin{cases} 62x - 113y = 0, \\ -17x + 31y = 12. \end{cases}$$

Thus $m = -17$, $n = 31$ is a solution to $1356m + 744n = 12$.

Problem. Find all common roots of real polynomials $p(x) = x^4 + 2x^3 - x^2 - 2x + 1$ and $q(x) = x^4 + x^3 + x - 1$.

Common roots of p and q are exactly roots of their greatest common divisor $\gcd(p, q)$. We can find $\gcd(p, q)$ using the Euclidean algorithm.

First we divide p by q: $x^4 + 2x^3 - x^2 - 2x + 1 =$
$= (x^4 + x^3 + x - 1)(1) + x^3 - x^2 - 3x + 2.$

Next we divide q by the remainder $r_1(x) = x^3 - x^2 - 3x + 2$:
$x^4 + x^3 + x - 1 = (x^3 - x^2 - 3x + 2)(x + 2) + 5x^2 + 5x - 5.$

Next we divide r_1 by the remainder $r_2(x) = 5x^2 + 5x - 5$:
$x^3 - x^2 - 3x + 2 = (5x^2 + 5x - 5)(\frac{1}{5}x - \frac{2}{5}).$

Since r_2 divides r_1, it follows that

$$\gcd(p, q) = \gcd(q, r_1) = \gcd(r_1, r_2) = r_2.$$

The polynomial $r_2(x) = 5x^2 + 5x - 5$ has roots
$(-1 - \sqrt{5})/2$ and $(-1 + \sqrt{5})/2$.

Chinese Remainder Theorem

Theorem Let $n, m \geq 2$ be relatively prime integers and a, b be any integers. Then the system

$$\begin{cases} x \equiv a \bmod n, \\ x \equiv b \bmod m \end{cases}$$

of congruences has a solution. Moreover, this solution is unique modulo nm.

Proof: Since $\gcd(n, m) = 1$, we have $sn + tm = 1$ for some integers s, t. Let $c = bsn + atm$. Then

$$c = bsn + a(1 - sn) = a + (b - a)sn \equiv a \pmod{n},$$
$$c = b(1 - tm) + atm = b + (a - b)tm \equiv b \pmod{m}.$$

Therefore c is a solution. Also, any element of $[c]_{nm}$ is a solution. Conversely, if x is a solution, then $n|(x - c)$ and $m|(x - c)$, which implies that $nm|(x - c)$, i.e., $x \in [c]_{nm}$.

Problem. Solve simultaneous congruences $\begin{cases} x \equiv 3 \bmod 12, \\ x \equiv 2 \bmod 29. \end{cases}$

The moduli 12 and 29 are coprime. First we use the Euclidean algorithm to represent 1 as an integral linear combination of 12 and 29:

$$\left(\begin{array}{cc|c} 1 & 0 & 12 \\ 0 & 1 & 29 \end{array}\right) \to \left(\begin{array}{cc|c} 1 & 0 & 12 \\ -2 & 1 & 5 \end{array}\right) \to \left(\begin{array}{cc|c} 5 & -2 & 2 \\ -2 & 1 & 5 \end{array}\right)$$

$$\to \left(\begin{array}{cc|c} 5 & -2 & 2 \\ -12 & 5 & 1 \end{array}\right) \to \left(\begin{array}{cc|c} 29 & -12 & 0 \\ -12 & 5 & 1 \end{array}\right).$$

Hence $(-12) \cdot 12 + 5 \cdot 29 = 1$. Let $x_1 = 5 \cdot 29 = 145$, $x_2 = (-12) \cdot 12 = -144$. Then

$$\begin{cases} x_1 \equiv 1 \bmod 12, \\ x_1 \equiv 0 \bmod 29. \end{cases} \qquad \begin{cases} x_2 \equiv 0 \bmod 12, \\ x_2 \equiv 1 \bmod 29. \end{cases}$$

It follows that one solution is $x = 3x_1 + 2x_2 = 147$. The other solutions form the congruence class of 147 modulo $12 \cdot 29 = 348$.

Chinese Remainder Theorem (generalized)

Theorem Let $n_1, n_2, \dots, n_k \geq 2$ be pairwise coprime integers and $a_1, a_2, \dots, a_k$ be any integers. Then the system of congruences

$$\begin{cases} x \equiv a_1 \bmod n_1, \\ x \equiv a_2 \bmod n_2, \\ \dots\dots\dots \\ x \equiv a_k \bmod n_k \end{cases}$$

has a solution which is unique modulo $n_1 n_2 \dots n_k$.

Idea of the proof: The theorem is proved by induction on k. The base case $k = 1$ is trivial. The induction step uses the usual Chinese Remainder Theorem.

Problem. Solve simultaneous congruences

$$\begin{cases} x \equiv 1 \bmod 3, \\ x \equiv 2 \bmod 4, \\ x \equiv 3 \bmod 5. \end{cases}$$

First we solve the first two congruences. Let $x_1 = 4$, $x_2 = -3$. Then $x_1 \equiv 1 \bmod 3$, $x_1 \equiv 0 \bmod 4$ and $x_2 \equiv 0 \bmod 3$, $x_2 \equiv 1 \bmod 4$. It follows that $x_1 + 2x_2 = -2$ is a solution. The general solution is $x \equiv -2 \bmod 12$.

Now it remains to solve the system

$$\begin{cases} x \equiv -2 \bmod 12, \\ x \equiv 3 \bmod 5. \end{cases}$$

We need to represent 1 as an integral linear combination of 12 and 5: $1 = (-2) \cdot 12 + 5 \cdot 5$. Then a particular solution is $x = 3 \cdot (-2) \cdot 12 + (-2) \cdot 5 \cdot 5 = -122$. The general solution is $x \equiv -122 \bmod 60$, which is the same as $x \equiv -2 \bmod 60$.