

MATH 135 - Algebra for Honours Mathematics

Andy Zhang

Winter 2014

Contents

Chapter 1

Congruence and Modular Arithmetic

1.1 Congruence

1.1.1 Definition

Congruence: Let m be a fixed positive integer. If $a, b \in \mathbb{Z}$ we say that a is congruent to b modulo m , and write

$$a \equiv b \pmod{m}$$

if $m|(a - b)$. If $m \nmid (a - b)$, we write $a \not\equiv b \pmod{m}$

1.1.2 Propositions

Properties of Congruence(PC): Let $a, a', b, b' \in \mathbb{Z}$. If $a \equiv a' \pmod{m}$ and $b \equiv b' \pmod{m}$, then:

1. $a + b \equiv a' + b' \pmod{m}$

2. $a - b \equiv a' - b' \pmod{m}$

3. $ab \equiv a'b' \pmod{m}$

Congruences and Division(CD): If $ac \equiv bc \pmod{m}$ and $\gcd(c, m) = 1$, then $a \equiv b \pmod{m}$

1.2 Modular Arithmetic

1.2.1 Definition

Congruence Class: The congruence class modulo m of the integer a is the set of integers

$$[a] = \{x \in \mathbb{Z} | x \equiv a \pmod{m}\}$$

\mathbb{Z}_m : We define \mathbb{Z}_m to be the set of m congruence classes

$$\mathbb{Z}_m = \{[0], [1], [2], \dots, [m-1]\}$$

and we define addition/subtraction and multiplication/division as follows:

$$\begin{aligned}[a] + [b] &= [a + b] \\ [a] \cdot [b] &= [a \cdot b]\end{aligned}$$

1.2.2 Identities and Inverses in \mathbb{Z}_m

Identity: Given a set S and an operation designated by \circ , an identity is an element $e \in S$ so that

$$\forall a \in S, a \circ e = a$$

Inverse: The element $b \in S$ is an inverse of $a \in S$ if $a \circ b = b \circ a = e$

1.3 Fermat's Little Theorem

1.3.1 Theorem

Fermat's Little Theorem (FLT): If p is a prime number that does not divide the integer a , then

$$a^{p-1} \equiv 1 \pmod{p}$$

Corollary: For any integer a and any prime p ,

$$a^p \equiv a \pmod{p}$$

Existence of Inverses in \mathbb{Z}_p (INV \mathbb{Z}_p): Let p be a prime number. If $[a]$ is any non-zero element in \mathbb{Z}_p , then there exists an element $[b] \in \mathbb{Z}_p$ so that $[a] \cdot [b] = 1$

1.3.2 Proof

1. If $p \nmid a$, we first show that all of the integers

$$a, 2a, 3a, \dots, (p-1)a$$

are all distinct modulo p

2. Suppose that $ra \equiv sa \pmod{p}$ where $1 \leq r < s \leq p-1$

3. Since $\gcd(a, p) = 1$, Congruences and Division tells us that $r \equiv s \pmod{p}$, but this is not possible when $1 \leq r < s \leq p-1$.

4. Because $a, 2a, 3a, \dots, (p-1)a$ are all distinct mod p , it must be the case that these integers are equivalent to the integers $1, 2, 3, \dots, p-1$ in some order.

5. Multiplying these integers together gives

$$\begin{aligned}a \cdot 2a \cdot 3a \dots (p-1)a &\equiv 1 \cdot 2 \cdot 3 \dots (p-1) \pmod{p} \\ (p-1)!a^{p-1} &\equiv (p-1)! \pmod{p}\end{aligned}$$

6. Since $\gcd(p, (p-1)!) = 1$, Congruences and Division tells us that

$$a^{p-1} \equiv 1 \pmod{p}$$

1.4 Linear Congruences

1.4.1 Definition

Linear Congruence: A relation of the form

$$ax \equiv c \pmod{m}$$

is called a linear congruence in the variable x . A solution to such a linear congruence is an integer x_0 so that

$$ax_0 \equiv c \pmod{m}$$

1.4.2 Theorems

Linear Diophantine Equation Theorem, Part 2(LDET 2): Let $\gcd(a, m) = d \neq 0$.

If $x = x_0$ and $y = y_0$ is one particular integer solution to the linear Diophantine equation $ax + my = c$, then the complete integer solution is

$$x = x_0 + \frac{m}{d}n, y = y_0 - \frac{a}{d}n, \forall n \in \mathbb{Z}$$

The complete solution if x_0 is a solution is

$$x \equiv x_0 \pmod{\frac{m}{d}} \text{ where } d = \gcd(a, m)$$

Linear Congruence Theorem, Version 1(LCT 1): Let $\gcd(a, m) = d \neq 0$.

The linear congruence $ax \equiv c \pmod{m}$ has a solution iff $d|c$.

1.5 Chinese Remainder Theorem

1.5.1 Definition

Chinese Remainder Theorem(CRT): Let $a_1, a_2 \in \mathbb{Z}$. If $\gcd(m_1, m_2) = 1$, then the simultaneous linear congruences

$$n \equiv a_1 \pmod{m_1}$$

$$n \equiv a_2 \pmod{m_2}$$

has a unique solution modulo m_1m_2 . Thus if $n = n_0$ is one integer solution, then the complete solution is

$$n \equiv n_0 \pmod{m_1m_2}$$

Moreover, this could be generalized with many congruences. If $n = n_0$ is a solution, then the complete solution would be

$$n \equiv n_0 \pmod{m_1m_2\dots m_k}$$

Chapter 2

The RSA Scheme

2.1 RSA

2.1.1 Setting up RSA

1. Choose two large, distinct primes p and q and let $n = pq$.
2. Select an integer e so that $\gcd(e, (p-1)(q-1)) = 1$ and $1 < e < (p-1)(q-1)$.
3. Solve
$$ed \equiv 1 \pmod{(p-1)(q-1)}$$
for an integer d where $1 < d < (p-1)(q-1)$.
4. Publish the public encryption key (e, n) .
5. Keep the private decryption key secure (d, n) .

2.1.2 Sending a Message

To send a message:

1. Look up the recipient's public key (e, n) .
2. Generate the integer message M so that $0 \leq M < n$.
3. Compute the ciphertext C as follows:
$$M^e \equiv C \pmod{n} \text{ where } 0 \leq C < n$$
4. Send C

2.1.3 Receiving a Message

To decrypt a message:

1. Use your private key (d, n) .
2. Compute the message text R from the ciphertext C as follows:
$$C^d \equiv R \pmod{n} \text{ where } 0 \leq R < n$$
3. R is the original message.

Chapter 3

Injective, Surjective and Bijections

3.1 Injective(One-to-One)

3.1.1 Definition

Injective: Let S and T be two sets. A function $f : S \rightarrow T$ is **one-to-one**(or **injective**) iff for every $x_1 \in S$, $f(x_1) = f(x_2)$ implies that $x_1 = x_2$ and $|S| \leq |T|$. When trying to prove that a function is one-to-one, start off with $f(x_1) = f(x_2)$ and try to use algebraic manipulation to obtain $x_1 = x_2$.

3.1.2 Simple Example

Proposition: Let $m \neq 0$ and b be fixed real numbers. The function $f : \mathbb{R} \rightarrow \mathbb{R}$ defined by $f(x) = mx + b$ is one to one

Proof: Let $x_1, x_2 \in S$. Suppose that $f(x_1) = f(x_2)$. Now we show that $x_1 = x_2$. Since $f(x_1) = f(x_2)$, $mx_1 + b = mx_2 + b$. Subtracting b from both sides and dividing by m gives $x_1 = x_2$ as required.

3.1.3 Hard Example

Proposition: Let $f : T \rightarrow U$ and $g : S \rightarrow T$ be one-to-one functions. Then $f \circ g$ is a one-to-one function.

Proof: Let $x_1, x_2 \in S$. Suppose that $(f \circ g)(x_1) = (f \circ g)(x_2)$. Since $(f \circ g)(x_1) = (f \circ g)(x_2)$, we know that $f(g(x_1)) = f(g(x_2))$. Since f is one-to-one, we know that $g(x_1) = g(x_2)$. And since g is one-to-one, $x_1 = x_2$ as required.

3.2 Surjective

3.2.1 Definition

Surjective: A function $f : S \rightarrow T$ is **surjective**(or **onto**) if and only if for every $y \in T$ there exists an $x \in S$ so that $f(x) = y$. This implies that $|S| \geq |T|$.

When trying to prove that a function is onto, try to find a function $g(x)$ such that $f(g(x)) = y$ to prove that each y in the codomain is mapped to.

3.3 Bijections

3.3.1 Definition

Bijection: A function $f : S \rightarrow T$ is **bijjective** iff f is both surjective and injective.

3.3.2 Simple Example

We have already shown that for $m \neq 0$ and b a fixed real number, the function $f : \mathbb{R} \rightarrow \mathbb{R}$ defined by $f(x) = mx + b$ is both surjective and injective. Hence, f is bijective.

3.4 Summary

- $f : S \rightarrow T$ is a function iff $\forall s \in S \exists! t \in T, f(s) = t$ where $!$ means unique
- $f : S \rightarrow T$ is surjective iff $\forall t \in T \exists s \in S, f(s) = t$, meaning for each element $t \in T$, there is at least one element $s \in S$ so that $f(s) = t$
- $f : S \rightarrow T$ is injective iff $\forall x_1 \in S \forall x_2 \in S, f(x_1) = f(x_2) \Rightarrow x_1 = x_2$ or $x_1 \neq x_2 \Rightarrow f(x_1) \neq f(x_2)$, meaning for each element $t \in T$, there is at most one element $s \in S$ so that $f(s) = t$

3.4.1 Frequently Asked Questions

Questions to be added

Chapter 4

Counting

4.1 Bijection and Cardinality

4.1.1 Definition

Cardinality: If there exists a bijection between the sets S and T , we say that the sets have the same and we write $|S| = |T|$.

Number of Elements, Finite, Infinite: If there exists a bijection between a set S and \mathbb{N}_n , we say that the **number of elements** in S is n and we write $|S| = n$. Moreover, we also say that S is a **finite set**. If no bijection exists between a set S and \mathbb{N}_n for any n , we say that S is an **infinite set**.

Countable: A set S is **countable** if there exists an injective function f from S to the natural numbers \mathbb{N}

4.1.2 Guidelines

Proposition: Let $S = \dots$ Let $T = \dots$ Then there exists a bijection $f : S \rightarrow T$. Hence, $|S| = |T|$.

To do this, we must prove that f is both surjective and injective.

Consider the function $f : S \rightarrow T$ defined by $f(s) = \dots$. We show that f is surjective. Let $t \in T$. Consider $s = \dots$. We show that $s \in S$. Now we show that $f(s) = t$.

We then show that f is injective. Let $s_1, s_2 \in S$ and suppose that $f(s_1) = f(s_2)$. Now we show that $s_1 = s_2$.

Hence, $f : S \rightarrow T$ is a bijection and $|S| = |T|$.

4.2 Finite Sets

4.2.1 Definitions

Disjoint: Set S and T are **disjoint** if $S \cap T = \emptyset$

4.2.2 Propositions

Cardinality of Intersecting Sets(CIS): If S and T are any finite sets, then

$$|S \cup T| = |S| + |T| - |S \cap T|$$

Cardinality of Disjoint Sets(CDS): If S and T are disjoint finite sets, then

$$|S \cup T| = |S| + |T|$$

4.2.3 Example

Proof of CDS:

1. Since S is a finite set, there exists a bijection $f : S \rightarrow \mathbb{N}_m$ for some non negative integer m , and $|S| = m$
2. Since T is a finite set, there exists a bijection $g : T \rightarrow \mathbb{N}_n$ for some non negative integer n , and $|T| = n$
3. Construct function $h : S \cup T \rightarrow \mathbb{N}_{m+n}$ as follows:
 $h(x) = f(x)$ if $x \in S$ else $g(x) + m$ if $x \in T$
4. To show that h is surjective, let $y \in \mathbb{N}_{m+n}$. If $y \leq m$, then because f is surjective there exists an element $x \in S$ so that $f(x) = y$, hence $h(x) = y$. If $m + 1 \leq y \leq m + n$, then because g is surjective, there exists an element $x \in T$ so that $g(x) = y - m$ and so $h(x) = (y - m) + m = y$.
5. To show that h is injective, let $x_1, x_2 \in S \cup T$ and suppose that $h(x_1) = h(x_2)$. If $h(x) \leq m$ then $h(x) = f(x)$ so if $h(x_1) \leq m$ we have
$$h(x_1) = h(x_2) \Rightarrow f(x_1) = f(x_2)$$
But since f is a bijection $f(x_1) = f(x_2)$ implies $x_1 = x_2$ as needed. If $h(x) > m$ then $h(x) = g(x)$ so if $h(x_1) > m$ we have
$$h(x_1) = h(x_2) \Rightarrow g(x_1) + m = g(x_2) + m \Rightarrow g(x_1) = g(x_2)$$
But since g is a bijection $g(x_1) = g(x_2)$ implies $x_1 = x_2$ as needed. Since h is a function which is both injective and surjective, h is bijective.

6. Thus

$$|S \cup T| = |\mathbb{N}_{m+n}| = m + n = |\mathbb{N}_m| + |\mathbb{N}_n| = |S| + |T|$$

If it wasn't clear, $f(x)$ is mapped to $1, 2, \dots, m$ and $g(x) + m$ is mapped to $m + 1, m + 2, \dots, m + n$.

4.3 Infinite Sets

4.3.1 Propositions

Cardinality of Subsets of Finite Sets(CSFS): If S and T are finite sets, and $S \subset T$, then $|S| < |T|$

$|\mathbb{N}| = |2\mathbb{N}|$: Let $2\mathbb{N}$ be the set of positive even natural numbers. Then $|\mathbb{N}| = |2\mathbb{N}|$
 $|\mathbb{N}x\mathbb{N}| = |\mathbb{N}|$

Even-Odd Factorization of Natural Numbers(EOFNN): Any natural number n can be written uniquely as $n = 2^i q$ where i is a non-negative integer and q is an odd natural number. Note: use EOFNN to prove $|\mathbb{N} \times \mathbb{N}| = |\mathbb{N}|$.
Note: Not all infinite sets have the same size

4.3.2 Example

Proof of $|\mathbb{N}| = |2\mathbb{N}|$

We want to prove that there's a bijection between both sets

1. Consider the function $f : \mathbb{N} \rightarrow 2\mathbb{N}$ defined by $f(s) = 2s$
2. We show that f is surjective. Let $t \in 2\mathbb{N}$. Consider $s = \frac{1}{2}t$. We show that $s \in \mathbb{N}$ since $f(\frac{1}{2}t) = t$ and therefore is surjective
3. We show that f is injective. Let $s_1, s_2 \in \mathbb{N}$ and suppose that $f(s_1) = f(s_2)$. Now we show that $s_1 = s_2$. Since $f(s_1) = 2s_1$ and $f(s_2) = 2s_2$, $s_1 = s_2$.
4. Hence, $f : \mathbb{N} \rightarrow 2\mathbb{N}$ is a bijection and $|\mathbb{N}| = |2\mathbb{N}|$.

Chapter 5

Complex Numbers

5.1 Complex Numbers

5.1.1 Definition

Complex Number: A complex number z in **standard form** is an expression of the form $x + yi$ where $x, y \in \mathbb{R}$. The set of all complex numbers is denoted by

$$\mathbb{C} = \{x + yi | x, y \in \mathbb{R}\}$$

Real part and Imaginary part: For a complex number $z = x + yi$, the real number x is called the **real part** and is written $\Re(z)$ and the real number y is called the **imaginary part** and is written $\Im(z)$.

5.1.2 Properties

Complex Conjugate: The complex conjugate of $z = x + yi$ is

$$\bar{z} = x - yi$$

This implies that:

- $z + \bar{w} = \bar{z} + w$
- $z\bar{w} = \bar{z}w$
- $\bar{\bar{z}} = z$
- $z + \bar{z} = 2\Re(z)$
- $z - \bar{z} = 2\Im(z)$

Modulus: The modulus of the complex number $z = x + yi$ is the non-negative real number:

$$|z| = |x + yi| = \sqrt{x^2 + y^2}$$

5.2 Polar Form

5.2.1 Definition

Polar Form: The polar form of a complex number z is

$$z = r(\cos \theta + i \sin \theta)$$

where r is the modulus of z and the angle θ is called an argument of z

Complex Exponential: By analogy, we define the complex exponential function by

$$e^{i\theta} = \cos \theta + i \sin \theta$$

5.2.2 Properties

Polar Multiplication of Complex Numbers(PMCN): If $z_1 = r_1(\cos \theta_1 + i \sin \theta_1)$ and $z_2 = r_2(\cos \theta_2 + i \sin \theta_2)$ are two complex numbers in polar form, then

$$z_1 z_2 = r_1 r_2 (\cos(\theta_1 + \theta_2) + i \sin(\theta_1 + \theta_2))$$

5.2.3 De Moivre's Theorem

De Moivre's Theorem(DMT): If $\theta \in \mathbb{R}$ and $n \in \mathbb{Z}$ then

$$(\cos \theta + i \sin \theta)^n = \cos n\theta + i \sin n\theta$$

5.3 Roots of Complex Numbers

5.3.1 Definition

Complex Roots: If a is a complex number, then the complex numbers that solve

$$z^n = a$$

are called the complex n th roots. De Moivre's Theorem gives us a straightforward way to find complex n th roots of a .

Nth root of unity: z is an n th root of unity if $z^n = 1$.

5.3.2 Technique

Complex nth Roots Theorem(CNRT): If $r(\cos \theta + i \sin \theta)$ is the polar form of a complex number a , then the solutions to $z^n = a$ are:

$$\sqrt[n]{r} \left(\cos\left(\frac{\theta + 2k\pi}{n}\right) + i \sin\left(\frac{\theta + 2k\pi}{n}\right) \right)$$

where $k = 0, 1, 2, 3, \dots$

Finding coefficients of all x^k for $k \in \mathbb{N}$:

$$1, w = e^{i\frac{2\pi}{n}}, w = e^{i\frac{4\pi}{n}}$$

Let's let $n = 3$. $1 + w + w^2 = 0$. $\frac{f(1)+f(w)+f(w^2)}{3}$ is the sum we want.

Chapter 6

Polynomials

6.1 Polynomials

6.1.1 Definition

Polynomial: A polynomial in x over a field \mathbb{F} (eg $\mathbb{R}, \mathbb{C}, \mathbb{Q}, \mathbb{Z}_p$ for prime p , any number system that is closed under $+$ $-$ $*$ $/$) has the form

$$a_n x^n + a_{n-1} x^{n-1} + \dots + a_1 x + a_0$$

where $n \geq 0$ is an integer and $a_i \in \mathbb{F}$ for each i . The set of all polynomials in x over \mathbb{F} is denoted $\mathbb{F}[x]$

6.1.2 Proposition

Division Algorithm for Polynomials(DAP): If $f(x)$ and $g(x)$ are polynomials in $\mathbb{F}[x]$ and $g(x)$ is not the zero polynomial, then there exist unique polynomials $q(x)$ and $r(x)$ in $\mathbb{F}[x]$ such that

$$f(x) = q(x)g(x) + r(x)$$

where $\deg r(x) < \deg g(x)$ or $r(x) = 0$

$q(x)$ is the quotient polynomial and $r(x)$ is called the remainder polynomial. If $r(x) = 0$, then $g(x)|f(x)$

6.2 Factoring Polynomials

6.2.1 Definition

Root: An element $c \in \mathbb{F}$ is called a root or zero of the polynomial $f(x)$ if $f(c) = 0$.

6.2.2 Theorems

Fundamental Theorem of Algebra(FTA): For all complex polynomials $f(z)$ with $\deg(f(z)) \geq 1$, there exists a $z_0 \in \mathbb{C}$ so that $f(z_0) = 0$.

Remainder Theorem: The remainder when the polynomial $f(x)$ is divided by $(x - c)$ is $f(c)$.

Factor Theorem 1(FT 1): The linear polynomial $(x - c)$ is a factor of the

polynomial $f(x)$ iff $f(c) = 0$.

Factor Theorem 2 (FT 2): The linear polynomial $(x - c)$ is a factor of the polynomial $f(x)$ iff c is a root of the polynomial $f(x)$.

Complex Polynomials of Degree n Have n Roots (CPN): If $f(x)$ is a complex polynomial of degree $n \geq 1$, then $f(x)$ has n roots and can be written as the products of n linear factors. The n roots and factors may not be distinct.

Rational Roots Theorem (RRT): Let $f(x)$ be a polynomial of degree n . If $\frac{p}{q}$ is a rational root with $\gcd(p, q) = 1$, then $p|a_0$ and $q|a_n$.

Note: If asked for a rational root, find all divisors of a_n and a_0 and find all different combinations and evaluate whether they're roots.

Conjugate Roots Theorem (CJRT): Let $f(x)$ be a polynomial of degree n with real coefficients. If $c \in \mathbb{C}$ is a root of $f(x)$, then $\bar{c} \in \mathbb{C}$ is a root of $f(x)$.

Real Quadratic Factors (RQF): Let $f(x)$ be a polynomial of degree n with real coefficients. If $c \in \mathbb{C}$, $\Im(c) \neq 0$, is a root of $f(x)$, then there exists a real quadratic factor of $f(x)$ with c as a root.

Real Factors of Real Polynomials (RFRP): Let $f(x)$ be a polynomial of degree n with real coefficients. Then $f(x)$ can be written as a product of real linear and real quadratic factors.