246 REVIEW

MAT246 Review

Lemma 1.1.1
If m is a composite natural number, then there is a prime number that is a divisor of m.

Theorem 1.1.2
There is no largest prime number.

Definition 2.1.1 (The Principle of Mathematical Induction) If S is any set of natural numbers with the properties that:
A. 1 is in S, and
B. $k+1$ is in S whenever k is any number in S.
then S is the set of all natural numbers.

Proposition 2.1.2 (The well-ordering of the natural numbers).
Every set of natural numbers that contains at least one element has a smallest element in it.

Theorem 2.1.3 $1^2+2^2+3^2+\cdots+n^2 = \frac{n(n+1)(2n+1)}{6}$

Definition 2.1.4 (Generalized Principle of Mathematical Induction) Let m be a natural number. If S is a set of natural numbers with the properties that:
A. m is in S, and:
B. $k+1$ is in S, whenever k is in S and is greater than or equal to m. then S contains every natural number greater than or equal to m

Theorem 2.1.5 $n! > 2^n$ for $n \geq 4$.

Definition 2.2.1 (Principle of Complete Mathematical Induction) If S is any set of natural numbers with the properties that:
A. 1 is in S, and
B. $k+1$ is in S whenever k is a natural number and all of the natural

numbers from 1 through k are in S, then S is the set of all natural numbers.

Definition 2.2.2. (~~General~~ Generalized Principle of Complete Mathematical Induction).

...

Lemma 2.2.3 If n is a composite natural number, then there is a prime number that is a divisor of n.

~~The~~ Theorem 2.2.4 Every natural number other than 1 is a product of prime numbers.

Def. 3.1.1: For any fixed # $m > 1$, say a is congruent to $b \pmod{m}$ if $a-b$ is divisible by m.

Theorem 3.1.2 If $a \equiv b \pmod{m}$ and $b \equiv c \pmod{m}$, then $a \equiv c \pmod{m}$

~~Theorem 3.1.3.~~

Theorem 3.1.5 If $a \equiv b \bmod m$ & $c \equiv d \bmod n$. then

(i). $(a+c) \equiv (b+d) \bmod m$

(ii). $ac \equiv bd \bmod m$

Thm 3.1.6 If $a \equiv b \bmod m$ then $\forall n \in \mathbb{N}^+$, $a^n \equiv b^n \bmod m$

Thm 4.1.1. (The Fundamental Theorem of Arithmetic) Every natural number greater than 1 can be written as a product of primes, and the expression of a number as a product of primes is unique except for the order of the factors.

Definition 5.1.4. A multiplicative inverse modulo p for a natural number a is a natural number b s.t. $ab \equiv 1 \bmod p$

Cor. 5.1.5 If p is a prime and a is a natural number that is not divisible by p, then $\exists\ x \in N$ s.t. $ax \equiv 1 \bmod p$.

Thm 5.1.6 If p is a prime and x is an integer satisfying $x^2 \equiv 1 \bmod p$, then either $x \equiv 1 \bmod p$ or $x \equiv p-1 \bmod p$

Corollary 4.1.3. If p is a prime & $a, b \in N$ s.t. $p \mid ab$, then $p \mid a$ or $p \mid b$ at least one.

Thm 5.1.1. If p is a prime and $a \nmid p$ & if $ab \equiv ac \bmod p$ then $b \equiv c \bmod p$

Thm 5.1.2. If p is a prime & a is any natural that not divisible by p then $a^{p-1} \equiv 1 \bmod p$. FERMAT'S THEOREM

Corollary 5.1.3 $\Leftrightarrow a^p \equiv a \bmod p$

Thm 5.2.1. If p is a prime then $(p-1)! + 1 \equiv 0 \bmod p$
i.e. p divides $(p-1)! + 1$

Thm 5.2.2 If m is a composite > 4 then $(m-1)! \equiv 0 \bmod m$ so that $(m-1)! + 1 \equiv 1 \bmod m$ WILSON'S THEOREM

RSA: $N = pq$
E (encoder)
D (decoder)
$gcd(E, \varphi(N)) = 1$
$R \equiv M^E \bmod N$
$DE \equiv 1 \bmod \varphi(N)$
$M^E \equiv R \pmod N$
$R^D \equiv M \bmod N$

Def 7.2.3 Linear Diophantine equation
$ax + by = c$

Thm 7.2.5 it has integer solutions iff $\gcd(a,b)$ divides c — divides t.

Lemma 7.2.6. If s divides tu and s is relatively prime to u, then s

Def. 7.2.9 φ: Euler function $\varphi(m)$ is the number of numbers in $\{1, 2, \ldots, m-1\}$ that are relatively prime to m.

$\varphi(p) = p - 1$ if prime
$\varphi(pq) = (p-1)(q-1)$

Lemma 7.2.13 If a is relatively prime to m and $ax \equiv ay \bmod m$ then $x \equiv y \bmod m$.

Thm 7.2.14

EULER'S THM:

If m is a natural >1, a is a natural that relatively prime to m. then $\boxed{a^{\varphi(m)} \equiv 1 \bmod m}$.

Fermat theorem is one of its special case.

Chapter 8, Rational #s & irrational #s

Thm 8.1.9. (The Rational Roots Thm)

If $\frac{p}{q}$ is a rational root of the poly

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

and p and q are relatively prime, then p divides a_0 and q divides a_n $\quad p \mid a_0$ & $q \mid a_n$

Theorem 8.2.6. If p is a prime number, then $\sqrt{p}$ is irrational.

Prove $\sqrt{3}+\sqrt{5}$ is irrational.

Sps $\sqrt{3}+\sqrt{5}=r$ is irrational

$$\sqrt{3} = r - \sqrt{5}$$

$$3 = r^2 - 2\sqrt{5}r + 5$$

$$2\sqrt{5}r = r^2 + 2$$

Chapter 9. The complex number.

Definition 9.1.5 complex conjugate

$$\overline{a+bi} = a - bi$$

Definition 9.1.8. The modulus of complex number

$$|a+bi| = \sqrt{a^2+b^2}$$

RSA.

Theorem 6.1.1.

Let $N=pq$, p, q distinct primes. let $\varphi(N)=(p-1)(q-1)$.
If k and a are any natural numbers, then $a \cdot a^{k\varphi(N)} = a \bmod N$

Sending a Message.

Message M to send
Computes R between 0 and N
such that $M^E \equiv R \pmod N$
Sends R to the recipient

E
$\gcd(E, \varphi(N)) = 1$

$DE \equiv 1 \bmod \varphi(N)$

$37 \cdot 13 \equiv 1 \bmod 6 \times 10$

$481 \equiv 1 \bmod 60$

Receiving a Message
For such a D.
since $R \equiv M^E \bmod N$
$R^D \equiv M^{ED} \bmod N$
therefore, since $M^{ED} \equiv M \bmod N$
$R^D \equiv M \bmod N$

e.g. $p=7, q=11, N=pq=77$
$E=13$.

$M=71$, $R \equiv M^E \equiv 71^{13} \bmod 77 \equiv (-6)^{13} \bmod 77$
$\equiv 15 \bmod 77$

$M \equiv R^D \bmod N$
$\equiv 15^{37} \bmod 77$
$\equiv 71 \bmod 77$

Continuing Chapter 9.

Chp 7 The Euclidean Algorithm and Applications

Use Euclidean Algorithm to find gcd (13, 60):

$60 = 4 \times 13 + 8$

$13 = 1 \times 8 + 5$

$8 = 1 \times 5 + 3$

$5 = 1 \times 3 + 2$

$3 = 1 \times 2 + 1$

$2 = 1 \times 2$

so gcd (13, 60) = 1

gcd (4, 22)

$22 = 5 \times 4 + 2$

$4 = 2 \times 2$

gcd (4, 22) = 2

~~$3 = 1 \cdot 2 + 1$~~

~~$1 = 3 - 2$~~

~~$1 = 2 \cdot 3 - 5$~~

~~$= 2 \cdot (8 - 5) - 5$~~

$1 = 3 - 2$

$= (8 - 5) - (5 - 3)$

$= (8 - 5) - (5 - (8 - 5))$

$= 8 \cdot 2 - 5 \cdot 3$

$= (13 - 5) \cdot 2 - (13 - 8) 5 \cdot 3$

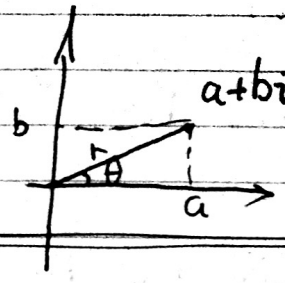
$= 13 \cdot 2 - 5 \cdot 5$

$= 13 \cdot 2 - (13 - 8) \cdot 5$

$= (-3) \cdot 13 + 8 \cdot 5$

$= (60 - 4 \times 13) \cdot 5 - 13 \cdot 3$

$= 60 \times 5 - 23 \cdot 13$



Definition 9.23. The polar form of the complex number with modulus r and argument θ is $r(\cos\theta + i\sin\theta)$

$= \sqrt{a^2+b^2}\left(\frac{a}{\sqrt{a^2+b^2}} + i\frac{b}{\sqrt{a^2+b^2}}\right)$

Theorem 9.26. DeMoivre's Theorem For every natural number n,

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

Proof by induction.

Theorem 9.3.1. THE FUNDAMENTAL THEOREM of ALGEBRA.
Every non-constant polynomial with complex coefficient has a complex root.

Theorem 9.3.4.
If r is a complex number and $p(z)$ is a non-constant polynomial with complex coefficients, then there exists a polynomial $q(z)$ and a constant c such that

$$p(z) = (z-r)q(z) + c$$

Definition 9.3.5. The polynomial $f(z)$ is a factor of the polynomial $p(z)$ if $\exists$ a polynomial $q(z)$ such that $p(z) = f(z)q(z)$

Theorem 9.3.6.
(The factor Theorem)
The complex number r is a root of a polynomial $p(z)$ if and only if $(z-r)$ is a factor of $p(z)$

Theorem 9.3.8
A polynomial of degree n has n complex roots "counting multiplicity".

Chapter 10. Sizes of Infinite Sets.

Def. 10.1.5.
$f: S \to T$ that is a mapping of each element of S to an element of T. S is called the domain of the function.
The range of a function is the set of all its values.

$$\{f(s) : s \in S\}$$

Def 10.1.6.

A function $f: S \to T$ is one-to-one (or injective) if $f(s_1) \neq f(s_2)$ whenever $s_1 \neq s_2$. That is, a function is one-to-one if it does not send two different elements to the same element.

Def 10.1.7

A function $f: S \to T$ is onto (or surjective) if for every $t \in T$ there is an $s \in S$ such that $f(s) = t$. That is the range of f is all of T.

Def 10.1.13.

We use the notation $|S| = |T|$ to mean that S and T have the same cardinality.

Theorem 10.1.14

The set of natural numbers and the set of positive rational numbers have the same cardinality

Def 10.2.1

A set is countable (sometimes called denumerable, or enumerable) if it is either finite or has the same cardinality as the set of natural numbers. A set is said to be uncountable if it is not countable.

Theorem 1022

The set of all real numbers between 0 and 1 is uncountable.

Theorem 10.2.4

If a and b are real numbers and $a < b$, then $[a, b]$ and $[0, 1]$ have the same cardinality.

Theorem 10.2.6. $|[0,1]| = |(0,1]|$

~~Theo~~ Theorem 10.2.7.
If $|S|=|T|$. $|T|=|U|$ then $|S|=|U|$

Theorem 10.2.8. For $a,b,c,d \in R$. $|(a,b]|=|[c,d]|$

Theorem 10.2.10. The union of a countable number of countable sets is countable.

$S_1 = \{a_{11}, a_{12}, a_{13}, \dots\}$
$S_2 = \{a_{21}, a_{22}, a_{23}, \dots\}$
$S_3 = \{a_{31}, a_{32}, a_{33}, \dots\}$
$S_4 = \{a_{41}, a_{42}, a_{43}, \dots\}$

Theorem 10.3.5 (The Cantor–Schroeder–Bernstein Theorem)
If S and T are sets such that $|S| \leq |T|$ and $|T| \leq |S|$. then $|S|=|T|$.

~~We say that an immdiate ancestor of an element s in S is an "ancestor~~

Cordlary 10.3.6. If S is a subset of T and there exists a function $f: T \to S$ that is one-to-one, then S and T have the same cardinality.

Theorem 10.3.7. If $a<b$. then $|[a,b]|=|(a,b)|=|[a,b)|=|(a,b]|$

Theorem 10.3.8. The cardinality of the set of all real numbers is the same as the cardinality of the unit interval $[0,1]$.

Theorem 10.3.9. A subset of a countable set is countable.

Cordlary 10.3.10. If S is any set and there exists a one-to-one function f mapping S into the set of natural numbers, then S is countable.

Def: 10.3.11 A finite sequence of elements of a set S is an ordered collection of elements of S of the form $(s_1, s_2, \dots, s_k)$.

10.3
Theorem ~~3.10~~.12 The set of all finite sequence of natural numbers is countable.

Corollary ~~3.10~~ 10.3.13 If $\mathcal{L}$ is any countable set, then the set of all finite sequences of elements of $\mathcal{L}$ is countable.

Theorem 10.3.17 The set of all rational numbers is countable.

Theorem 10.3.18 The set of integers is countable.

Def: algebraic

Theorem 10.3.20: The set of algebraic numbers is countable.

Corollary 10.3.21. There exist transcendental numbers

10.3.22
Def: $|S| = |N| = \aleph_0$

10.3.23
Def $|S| = |R| = c$ "the cardinality of the continuum".

10.3.24
Theorem: If S is an infinite set, then $\aleph_0 \leq |S|$

10.3.25
Def: Powerset of S: $P(S)$ the set of all subsets of S.

Theorem: 10.3.26: If S is a finite set with n elements, then the cardinality of $P(S)$ is 2^n.

Theorem 10.3.27. For every set S, $|S| < |P(S)|$

Theorem 10.3.28 The cardinality of the set of all sets of natural numbers is the same as the cardinality of the set of real numbers. That is $|P(N)| = c$, or $2^{\aleph_0} = c$.

Def. 10.3.29 The unit square in the plane is the subset of the plane consisting of all points whose x and y coordinates are

both between 0 & 1. That is, the unit square is the set S defined by
$S = \{(x,y) : 0 \le x \le 1,\ 0 \le y \le 1\}$
Theorem ~~3.10~~ 10.3.30. The cardinality of the unit square in the plane is c.

Chapter 12 Constructability.

Def. 12.2.1 A real number is constructible if the point corresponding to it on the number line can be obtained from the marked points 0 and 1 by performing a finite sequence of constructions using only a straightedge and compass.

Theorem 12.2.2 Every integer is constructible
Theorem 12.2.3 Every rational number is constructible.

Def 12.2.8 A number field is a set F of real numbers satisfying
i). The numbers 0 & 1 are both in F.
ii). If $x, y \in F$ then $x+y$ & $x \cdot y \in F$
iii). $x \in F \Rightarrow -x \in F$
iv). $x \in F$ & $x \neq 0 \Rightarrow \frac{1}{x} \in F$

Theorem 12.2.9 ~~The set of all~~ If F is any number field, then F contains all rational numbers.

Theorem 12.2.11. The set C of constructible numbers is a number field.

Theorem 12.2.13. Let F be any number field & sps that r is a positive number in F. If $\sqrt{r}$ is not in F, and
$F(\sqrt{r}) = \{a + b\sqrt{r};\ a \in F, b \in F\}$ then $F(\sqrt{r})$ is a number field.

Thm 12.2.16 If r is a positive constructible number, then $\sqrt{r}$ is constructible

Def 12.2.17. A tower of number fields is a finite sequence $F_0, F_1, F_2, \cdots, F_n$ of number fields such that $F_0 = \mathbb{Q}$ and for each i from 1 to n there is a positive # r_i in F_{i-1} s.t. $\sqrt{r_i}$ is not in F_{i-1} & $F_i = F_{i-1}(\sqrt{r_i})$

$\{F_i\}$ such that $F_0 \subset F_1 \subset \cdots \subset F_n$

Def 12.3.1 A surd is a number that is in some number field that is in a tower. That is, x is a surd if $\exists$ a tower $F_0 \subset F_1 \subset \cdots \subset F_n$ s.t. $x \in F_n$. s.t. x is in F_n.

Thm 12.3.2 The set of all surds is ~~the~~ a number field. Moreover, if r is a positive surd then $\sqrt{r}$ is a surd.

Thm 12.3.3. Every surd is constructible.

Thm 12.3.5. The point (x,y) is constructible iff both of the coordinates x & y are constructible numbers.

Thm 12.3.12. The field of constructible numbers is the same as the field of surds.

Thm 12.3.13 θ (acute angle) is constructible with straightedge and compass if and only if $\cos\theta$ is a constructible number.

~~Axiom~~ Thm 12.3.16. For any angle θ, $\cos 3\theta = 4\cos^3\theta - 3\cos\theta$

Cor. 12.3.17 If $x = 2\cos 20^\circ$, then $x^3 - 3x - 1 = 0$.

Thm 12.3.21 If $a + b\sqrt{r}$ is a root of a polynomial with rational coefficients, then $a - b\sqrt{r}$ is also a root of the polynomial.

Thm 12.3.22 If a cubic equation with rational coefficients has a constructible root, then the equation has a rational root.

Thm 12.3.23 20° not constructible

Cor 12.3.24 60° not trisected.