Notes
By Owen Fuller
Based on

Lecture 1

Lecture 2

Bezout Lemma: Let $a, b \in \mathbb{Z}$ with (a, b). Then $\exists$ integers s and t such that $as + bt = (a, b)$. Moreover, any common divisor of a and b divides (a, b).
Divison Algorithm: Let $a, b \in \mathbb{Z}$ with $b > 0$. Then there exists a unique pair $q, r \in Z$ such that

$$a = qb + r$$

Euclidean Algorithm:

- $a = q_1 b + r_1$
- $b = q_2 r_1 + r_2$
- $r_k = q_{k+2} r_{k+1} + r_{k+2}$
- The last non-zero remainder r_{k+1} is the $\gcd(a, b)$.

Lecture 3

Distribution of Primes

Theorem 1 There are infinitely many primes
Theorem 2 There are infinitely many primes of the form $4k - 1$
Theorem 3 There are infinitely many primes of the form $3k - 1$
Theorem 4 There are infinitely many primes of the form $4k + 1$
Dirichlet's Theorem If a and b are positive integers not divisible by the same prime, then there are infinitely many primes of the form $ak + b$.

Formal/Informal Definitions of a Ring

Lecture 4

Congruences

The congruence $a \equiv b \mod n$ means the difference $(a - b)$ is divisible by n, or $a = nq + b$.
Complete System of Residues modulo n is a set of integers such that every integer is congruent to modulo n to exactly one integer in the set. A least positive residue for $a \in \mathbb{Z}$ is the smallest $b \in \mathbb{Z}$ such that $a \equiv b \mod n$. e.g modulo 5: a complete system of residues is $\{0, 1, 2, 3, 4\}$.
Theorem 1 If $a, b, c, d, n \in \mathbb{Z}$ with $n > 0$ and $a \equiv b \mod n$ and $c \equiv d \mod n$ then

$$\begin{aligned} a + c \equiv& b + d \mod n \\ a - c \equiv& b - d \mod n \\ ac \equiv& bd \mod n \end{aligned}$$

The Modulo Ring we define $\mathbb{Z}_n$: let n be a positive integer and $a, b, c \in \mathbb{Z}$. Recall that we say that a is congruent to $b \mod n$ if $n|(b - a)$.

- $a \equiv a \mod n$
- $a \equiv b \mod n \implies b \equiv a \mod n$
- $a \equiv b \mod n$ and $b \equiv c \mod n \implies a \equiv c \mod n$

Therefore $\mod n$ defines an equivalence relation on $\mathbb{Z}$. Let $\mathbb{Z}_n$ denote the set of equivalence classes and denote the equivalence class of $a \in \mathbb{Z}$ by $[a]_n \in \mathbb{Z}_n$. Note:

$$[a]_n = \{a + kn : k \in \mathbb{Z}\}$$

This set is called a coset of a. By the Division Algorithm, $\exists! q, r \in \mathbb{Z}$ with $0 \leq r < n$ such that $a = qn + r$. Hence n divides $a - r$ and $[a]_n = [r]_n$, so the equivalence class of a is determined by its remainder on division by n. Hence $\mathbb{Z}_n = \{[0]_n, [1]_n, ..., [n-1]_n\}$ has exactly n elements. Checking that addition and multiplication are well defined

$$[a]_n + [b]_n = [a + b]_n$$

$$[a]_n \cdot [b]_n = [ab]_n$$

With these operations $\mathbb{Z}_n$ becomes a ring.
Commutative a ring R is commutative is $a \cdot b = b \cdot a \forall a, b \in R$
Field is a commutative ring such that every nonzero element in F has a multiplicative inverse (so the set F with the operation of multiplication forms an abelian group).
Wilson's Theorem If p is prime then $(p-1)! \equiv -1 \mod p$.

Lecture 5

Chinese Remainder Theorem

Let $m_1, m_2, ..., m_k$ be natural numbers such that the greatest common divisor of any two of them is 1. Let $a_1, a_2, ..., a_k$ be arbitrary integers. Then there is x such that:

$$\begin{aligned} x \equiv & a_1 \mod m_1 \\ x \equiv & a_2 \mod m_2 \\ & ... \\ x \equiv & a_k \mod m_k \end{aligned}$$

This solution (x) is unique modulo $m_1 m_2 ... m_k$.

Lecture 6

Euler's Function for $n > 1$ the Euler function $\phi(n)$ is defined as the number of natural numbers not exceeding n which are coprime with n, and $\phi(1) = 1$.
Euler's Theorem Let $n > 1$ be a natural number, and let a be any number such that the greatest common divisor of a and n is 1 (n and a coprime). Then

$$a^{\phi(n)} - 1 \equiv 0 \mod n$$

Theorem 1 If m, n are coprime then $\phi(m \cdot n) = \phi(m) \cdot \phi(n)$.
Theorem 2 Suppose $p(1), ..., p(j)$ are distinct primes that divide m. Then

$$\phi(m) = m(1 - \frac{1}{p(1)})(1 - \frac{1}{p(2)})...(1 - \frac{1}{p(j)})$$

Rings

Consider the following axioms:

- A1 $a + b = b + a$
- A2 $(a + b) + c = a + (b + c)$
- A3 There exists in R an element 0_R st $0_R + a = a + 0_R = a \forall a \in R$
- A4 For each $a \in R$, there exists an element $-a$ st $a + (-a) = (-a) + a = 0_R$
- M1 $a \cdot b = b \cdot a$
- M2 $(a \cdot b) \cdot c = a \cdot (b \cdot c)$
- M3 There exists in R an element 1_R st $1_R \cdot a = a \cdot 1_R = a \forall a \in R$
- D $a \cdot (b + c) = a \cdot b + a \cdot c$ and $(a + b) \cdot c = a \cdot c + b \cdot c$

Ring A set R with two binary operations, addition and multiplication, and satisfying axioms A1, A2, A3, A4, M2 and D.
Commutative Ring A ring where $M1$ is also satisfied.
Ring From Identity A ring where $M3$ is also satisfied.
Commutative Ring with Identity A triple $< R, +, \cdot >$ satisfying all the above axioms.

Lecture 7

Theorem 1 If $n \in \mathbb{N}$ then

$$\sum_{d|n} \phi(d) = n$$

Primitive Roots

Primitive Root Let $p > 0$ be a prime. We say that an integer i is a primitive root modulo p iff all elements $i, i^2, ..., i^{p-1}$ are pairwise distinct modulo p. i.e. $i^m \neq 1 \mod p$ for $0 < m < p - 1$.
Notation Let p be a prime number, then the ring $\mathbb{Z}_p$ is a field and it is denoted $\mathbb{F}_p$. $\mathbb{F}_p[x]$ denotes the polynomial ring with coefficients from ring $\mathbb{F}_p$.
Theorem 2 A nonzero polynomial $f \in \mathbb{F}_p[x]$ of degree n has at most n roots x in $\mathbb{F}_p$.
Theorem 3 Let $p > 0$ be prime, then there exists a natural number i which is a primitive root modulo p.

Lecture 8

Generates Let G be a group. We say that an element $g \in G$ generates G if the set of powers of g and g^{-1} is equal to all of G. If such a g exists, we say that G is cyclic and we write $G = \langle g \rangle$.
Order If $g \in G$, we say that the order of g is the smallest positive integer n such that $g^n = 1$.
Corollary 1 Let G be a finite group which is cyclic. Then $g \in G$ is a generator of G iff the order of g equals $|G|$, the cardinality of G.
Lemma 1 Let G be a group and $g \in G$. If for $m, n \in \mathbb{Z}$ we have $g^m = 1$ and $g^n = 1$ then $g^{(m,n)} = 1$, where (m, n) denotes the greatest divisor of m and n.
Theorem 1 Let G be a finite cyclic group of cardinality N. If $g \in G$ then the order of g divides N (This is also true without the assumption that G is cyclic, which is the Lagrange theorem).
Theorem 2 Let G be a cyclic group and g be a generator of G. Let α be an integer, then element g^α is a generator of G iff $\gcd(\alpha, |G|) = 1$, where $|G|$ denotes the cardinality of G.
Corollary 2 Let G be a finite group which is cyclic. Then G has $\phi(|G|)$ generators.

Notation The group of units in $\mathbb{Z}_p$ is denoted as $\mathbb{Z}_p^*$.

maybemore

Lecture 9

Binary Codes: A binary word is a sequence of 0s and 1s, with length the total number of 0s and 1s. A binary code is a given set of binary words, e.g. $(1,1,1),(0,0,1)$.
Block Code: is a code having all its codewords the same length. This number is called the length of the code. e.g. $\{(1,1,1,1,1),(0,0,0,0,0)\}$ is a block code (all codewords have length 5).
Binary Linear Code: is a binary block code with the property that the sum of any two codewords is a codeword. The code $\{(0,0,0),(0,1,1),(1,0,1),(1,1,0)\}$ is a linear code.
Definition: For a fixed positive integer n, a block linear code C (called a code for short) of (block) length n over the finite field F is a subspace of the F-vector space $\mathbb{F}_n$. Denote by k the dimension of the code C, that is $\dim_{\mathbb{F}} C = k$.
Remark: Vectors in $\mathbb{F}_n$ will be written as row vectors and called words. $x = (x_1, x_2, \ldots, x_n)$ is often written as the word $x = x_1 x_2 \ldots x_n$.
Also assume $F = \mathbb{F}_2$.
Trivial codes are $C = \{0\}$ and $C = F^n$.
Cyclic Codes: A binary linear code where for every codeword $(c_1, c_2, \ldots, c_n)$, the word $(c_n, c_1, \ldots, c_{n-1})$ is also a codeword, where $c_i \in \{0,1\}$.

Lecture 10

Hamming Metric: Let C be a code over the arbitrary finite field F. The Hamming metric d on C is defined as follows: for all $x = (x_1, \ldots, x_n)$ and $y = (y_1, \ldots, y_n)$ in C,

$$d(x,y) = \{i \in \{1,\ldots,n\} : x_i \neq y_i$$

Weight: of x,

$$wt(x) = d(x,0) = \{i \in \{1,\ldots,n\} : x_i \neq 0\}$$

Minimum Distance: $d(C)$ of C is defined by setting

$$d(C) = \min\{d(x,y) : x,y \in C, x \neq y\}$$

Lemma: Let C be a linear code. Then the minimal distance is equal to the minimal possible weight of a non-zero codeword in this code.

Definition: The triple (n,k,d) comprises the three parameters of a linear code: n is the length of codewords in this code, k is the dimension of the code $\dim_F C = k$ and d is the minimal distance of the code.

Theorem: The Hamming metric is a metric on C.

1. For all $x,y \in C$, we have $d(x,y) \geq 0$ and $d(x,y) = 0$ iff $x = y$.
2. For all $x,y \in C$, $d(x,y) = d(y,x)$.
3. For all $x,y,z \in C$, we have $d(x,y) \leq d(x,z) + d(z,y)$.

Sphere Packing

Lecture 11

The Legendre Symbol

The Legendre Symbol: Let $p > 0$ be prime and let $a \in \mathbb{Z}$ be an integer not divisible by p.

- The Legendre symbol of a modulo p is $\left(\frac{a}{p}\right)$.
- It is 1 if $a \equiv r^2 \mod p$ for some integer r and -1 otherwise.
- If $\left(\frac{a}{p}\right) = 1$, then we say that a is a quadratic residue modulo p.

Theorem 7: Let $p > 0$ be a prime, and a an integer not divisible by p. Then the following hold:

1. Let p be an odd prime. The formula for the Legendre symbol is
$$\left(\frac{a}{p}\right) \equiv a^{\frac{p-1}{2}} \mod p$$
2. The quadratic residue multiplication rule:
$$\left(\frac{a}{p}\right)\left(\frac{b}{p}\right) = \left(\frac{ab}{p}\right)$$
3. $$\left(\frac{a}{p}\right) = \left(\frac{a-p}{p}\right)$$
Moreover, if $a \equiv b \mod p$ then
$$\left(\frac{a}{p}\right) = \left(\frac{b}{p}\right)$$
4. Quadratic reciprocity: Let $p, q > 0$ be distinct odd primes, then
$$\left(\frac{p}{q}\right) = \left(\frac{q}{p}\right)$$
provided that either $p \equiv 1 \mod 4$ or $q \equiv 1 \mod 4$.
5. Quadratic reciprocity: Let $p, q > 0$ be distinct odd primes, then
$$\left(\frac{p}{q}\right) = -\left(\frac{q}{p}\right)$$
provided that either $p \equiv 3 \mod 4$ and $q \equiv 3 \mod 4$.

Lemma: If $p \equiv 1 \mod 4$, then
$$\left(\frac{-1}{p}\right) = 1$$

If $p \equiv 3 \mod 4$, then
$$\left(\frac{-1}{p}\right) = -1$$

Lecture 12

Gauss Lemma

Let p be an odd prime, and $a \in \mathbb{Z}$ not divisible by p. Consider the set $S = \{a, 2a, 3a, \dots, \frac{p-1}{2}a\}$. Let S' be the set of remainders of elements from the set S when divided by p, with each remainder larger than $-\frac{p}{2}$ and smaller than $\frac{p}{2}$. Let n denote the number of elements from set S' which are smaller than 0. Then

$$(\frac{a}{p}) = (-1)^n$$

Lecture 13

Polynomials

The following definition works for any ring, but we will only apply it for rings $\mathbb{Z}_p$ where p is prime. Recall that operations in these rings are the same as operations in $\mathbb{Z}$ modulo p. We also denote $\mathbb{F}_p = \mathbb{Z}_p$.

Well-Ordering Principle: Every non-empty set of positive integers contains a least element.

Division Algorithm for Polynomials Let $\mathbb{F}$ be a field, and let $f(x), g(x) \in \mathbb{F}[x], g(x) \neq 0$. Then there exist unique polynomials $q(x), r(x) \in \mathbb{F}[x]$ such that

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

with the degree of $r(x)$ less than the degree of $g(x)$. $q(x)$ is called the quotient and r the remainder when $f(x)$ is divided by $g(x)$.

Definition: Let $\mathbb{F}$ be a field and let $f(x), g(x) \in \mathbb{F}[x], f(x) \neq 0$. We say $f(x)$ divides $g(x)$ in $\mathbb{F}[x]$ if there is a polynomial $h(x) \in \mathbb{F}[x]$ such that $g(x) = f(x)h(x)$. The notation $f(x)|g(x)$ means $f(x)$ divides $g(x)$.

Definition: Let $\mathbb{F}$ be a field and let $f(x), g(x) \in \mathbb{F}[x]$ (not both zero). A polynomial $d(x) \in \mathbb{F}[x]$ is a highest common factor of $f(x)$ and $g(x)$ if $d(x)|f(x)$ and $d(x)|g(x)$ and further, $\deg(d(x))$ is the maximum possible among such $d(x)$.

Bezout Lemma for Polynomials

Euclidean Algorithm for Polynomials

Theorem: The Euclidean algorithm always works.

Lecture 14

Factor Rings of Polynomial Rings

Let $\mathbb{F}$ be a field, and let $f(x) \in \mathbb{F}[x]$. Denote

$$I = f(x)\mathbb{F}[x] = \{f(x)g(x) : g(x) \in \mathbb{F}[x]\}$$

. A factor ring $\mathbb{F}[x]/I$ is a ring whose elements are sets (called cosets) which we can add and multiply by taking representatives of the cosets, and the result does not depend on which representatives we take.

Notice that the cosets are either distinct, i.e. they have nothing in common, or else they are the same coset.

$\mathbb{F}[x]$ can be partitioned into $\mathbb{F}[x]/I = \{r_1 + I, r_2 + I, ...\}$ equivalence classes modulo I. For $r \in \mathbb{F}[x]$ we define

$$r + I = \{r + i : i \in I\}$$

Coset: For any $a \in \mathbb{F}[x]$ the set

$$a + I = \{a + i : i \in I\}$$

is a coset. The element is a is called a representative of the coset $a + I$.
Remark: A coset representative is an element in $\mathbb{F}[x]$ which is an element in this coset. Note that $r \in r + I$, as $r = r + 0_r$ and $0_R \in R$.
Lemma: Let $a, b \in \mathbb{F}[x]$. Then the cosets of a and b are either equal or mutually disjoint. In symbols, either $a + I = b + I$ or $(a + I) \cap (b + I) = \emptyset$.
The cosets of I form a partition of $\mathbb{F}[x]$. In particular, $a + I = b + I$ iff $a - b \in I$. If $a - b \notin I$ then $(a + I) \cap (b + I) = \emptyset$.

Multiplying Cosets

We can just add and multiply the cosets by taking the representatives and we get the same results, no matter which cosets representatives we take.
Definition: We now define multiplication of these equivalence classes by

$$(a + I) + (b + I) = a + b + I$$

and

$$(a + I) \cdot (b + I) = a \cdot b + I$$

The above addition and multiplication is well defined (that is if we take different representatives of the cosets we get the same result).
Factor Rings: Let $\mathbb{F}$ be a field and let $f(x) \in \mathbb{F}[x]$. Denote

$$I = f(x)\mathbb{F}[x] = \{f(x)g(x) : g(x) \in \mathbb{F}[x]\}$$

Denote by $\mathbb{F}[x]/I$ the set of (distinct) cosets of I in $\mathbb{F}[x]/I$. Then the operations of addition and multiplication on $\mathbb{F}[x]/I$ are given by

$$(a + I) \oplus (b + I) = a + b + I$$
$$(a + I) \odot (b + I) = a \cdot b + I$$

are well defined and make $(R, \oplus, \odot)$ into a ring, called the factor ring of $\mathbb{F}[x]/I$ by I.

Lecture 15

Irreducible Polynomials

Irreducible Polynomial: Let $\mathbb{F}$ be a field and let $f(x) \in \mathbb{F}[x]$. We say that $f(x)$ ir irreducible in $F[x]$ if

$$f(x) = g(x)h(x)$$

with $g(x), h(x) \in \mathbb{F}[x]$ implies that either $g(x) \in \mathbb{F}$ or $h(x) \in \mathbb{F}$.
Theorem 1: Let $f(x) \in \mathbb{F}[x], f(x) \neq 0$ and denote $I = f(x)\mathbb{F}[x]$, then the factor ring $R = \mathbb{F}[x]/I$ is a field iff $f(x)$ is an irreducible polynomial.
Theorem 2: Let p be a prime number and let $f(x) \in \mathbb{F}_p[x]$ be an irreducible polynomial of degree n. Denote $I = f(x)\mathbb{F}_p[x]$. Then the factor ring $R = \mathbb{F}_p[x]/I$ is a field with exactly p^n elements.
Theorem 3: Let p be a prime number and let $f(x) \in \mathbb{F}_p[x]$ be an irreducible polynomial of degree n. Denote $I = f(x)\mathbb{F}_p[x]$. Then the factor ring $R = \mathbb{F}_p[x]/I$ is a field which has an element ξ which is a root of polynomial $f(x)$.
Theorem 4: Let p be a prime number. If $f(x)$ is an irreducible polynomial from $\mathbb{F}_p[x]$, then $f(x)$ divides the polynomial $x^{p^n} - x$ in $\mathbb{F}_p[x]$, where $n = \deg f(x)$.

Lecture 16

Fields

Field: a commutative ring in which every nonzero element has a multiplicative inverse. In other words, if $a \neq 0$, then there is an element, denoted a^{-1}, such that $a \cdot a^{-1} = a^{-1} \cdot a = 1$.
Proposition 1: Let p be prime, then each nonzero element a in the ring $\mathbb{Z}_p = \mathbb{Z}/p\mathbb{Z}$ is invertible, i.e. there exists an element $b \in \mathbb{Z}_p$ such that $ab \equiv 1 \mod p$.
Corollary: For each prime p, $\mathbb{Z}_p$ is a field. We denote this field F_p.
Characteristic: Let $\mathbb{F}$ be a field, and let $n > 0$ be the smallest natural number such that the sum of n copies of the identity element in $\mathbb{F}$ is zero, so $1 + \ldots + 1 = 0$ in $\mathbb{F}$, where 1 appears n-times in the sum. If such an n does not exist, then we say that the characteristic of $\mathbb{F}$.
Lemma: Let $\mathbb{F}$ be a field of characteristic $n > 0$, then n is a prime number.
Subfield: of a field F is a subset $K \subseteq F$ containing 0 and 1 which is closed under the arithmetic operations + - × ÷ (by non-zero elements).
Lemma: Let F be a finite field of characteristic p, then F_p is a subfield of F.
Proposition 2: Suppose that F is a field. Then F contains a smallest subfield P. This subfield P is contained in every subfield of F. We call this subfield P a prime subfield.
Theorem 1: Let F be a field of characteristic p. Then F has exactly p^n elements, for some natural number n.
Lemma: Let R be a ring. If 1=0 in R then R has only one element, the zero element.
Domain: A ring is a domain if a product of any two non-zero elements in this ring is non-zero.
Lemma: Let $\mathbb{F}$ be a field, then $\mathbb{F}$ is a domain.

Non Examinable

Theorem: For every prime number p and for every natural number n there is exactly one field with p^n elements (up to an isomorphism).
Corollary: Every finite field with p^n elements is of the form $\mathbb{F}_p[x]/f(x)\mathbb{F}_p[x]$ for an irreducible polynomial $f(x) \in \mathbb{F}_p[x]$ of degree n (up to an isomorphism of fields).

Lecture 17

Gaussian Integers

Gaussian Integers: Define

$$\mathbb{Z}[i] = \{a + ib : a, b \in \mathbb{Z}\}$$

Then $\mathbb{Z}[i]$ is closed under + × - and therefore is a ring. Let $z = a + ib$ be a Gaussian integer, then as usual we denote $|z| = |a + ib| = \sqrt{a^2 + b^2}$ (where $a, b \in \mathbb{Z}$)
Units in $\mathbb{Z}[i]$: We say that a Guassian integer $z = a + bi$ is a unit if there is a Gaussian integer $z' = a' + ib'$ such that $z \cdot z' = 1$.
Remark: If c, c' are Gaussian integers then $|c \cdot c'| = |c| \cdot |c'|$.
Lemma 1: Let $z = a + ib$ be a unit in $\mathbb{Z}[i]$, then $|z| = 1$. So z could be $1, -1, i, -i$.

Divisors: Let z, z' be GI. We say $z \neq 0$ divides z' iff $z' = z \cdot w$ for some GI w.
Irreducible: Let $z = a + ib$ be a non-zero, non-unit GI. We say that z is an irreducible GI if whenever $z = u \cdot v$ for GI u, v, it follows that either u or v is a unit.
Prime: Let $z = a + ib$ be a non-zero, non-unit GI. z is a prime GI if whenever $z|u \cdot v$ for GI u, v, it follows that either $z|u$ or $z|v$.

Gaussian Integer Results

Division Algorithm for Gaussian Integers: Let $z, w \in \mathbb{Z}[i]$ with $w \neq 0$, there exists $q, r \in \mathbb{Z}[i]$ with

$$z = qw + r$$

and either $r = 0$ or $|r| < |w|$.
Greatest Common Divisor: Let $a, b \in \mathbb{Z}[i]$ (not both zero). A gcd of a and b is a GI that divides both of them and has the maximal possible absolute value (as a complex number). Such an integer always exists, as $1|a$ and $1|b$, and clearly the aboslute value of a common divisor can exceed $\min(|a|, |b|)$ (so we are taking the maximum over a nonempty finite set).
Bezout Lemma for Gaussian Integers: Let a, b be GI (not both zero) and let d be a gcd of a and b. Then there exists integers s and t such that $as + bt = d$. Moreover, any common divisor of a and b divides d.

Lecture 18

Theorem PI: Let $z = a + ib$ be a GI, then z is a prime GI iff z is an irreducible GI.
Corollary: 2 is not a prime GI, but 7 is a prime GI.
Theorem: Let $p = 4k+1$ be a prime in $\mathbb{Z}$ for some integer $k > 0$. Then $p = a^2 + b^2$ for suitable $a, b \in \mathbb{Z}$.
Integral Domain: A non-zero commutative ring in which the product of any two non-zero elements is non-zero.
Associate: Let R be an integral domain and let $a, b \in R$. We say that a is an associate of b if $a = bu$, where u is a unit. So if a is an associate of b then b is an associate of a.
Theorem UF: Let a be a non-zero GI. Then either a is a unit or a may be expressed as a product of primes.
Theorem: Let $1 < n \in \mathbb{N}$. Suppose that

$$n = 2^c p_1^{a_1} \dots p_s^{q_s} q_1^{d_1} \dots q_t^{d_t}$$

is the prime factorisation of n into positive primes with each p and q being of the form $p = 4k+1$ and $q = 4k + 3$. Then there exist integers a, b with $n = a^2 + b^2$ iff each d_i is even.
Lemma 2: Let p be prime. p cannot be written as $x^2 + y^2$ for non-zero integers x, y iff p is an irreducible GI.

Lecture 19

Exercises

Lecture 20

Exercises

Lecture 21

0.1 Braces

Lecture 22

Definitions

Examples

Knowing a number $x \text{mod} N$ is equivalent to knowing $x \text{mod}$ each of the prime powers $p_j^{e_j}$ in $N = p_1^{e_1} ... p_n^{e_n}$.