# Elementary Number Theory and Logic
# NISER-MA Semester 3 of 2009

Instructor: Deepak Kumar Dalai

November 9, 2009

3rd August 2009

1. **Countability [9, 11]**
   (a) Do $A = \{a, b, c\}$ and $B = \{1, 2, 3\}$ have same cardinality (cardinal number) ?
   (b) Do $N$ and $E = \{2 * n : n \in N\}$ have same cardinality (If yes, why as $E \subset N$) ?
   (c) Definitions: cardinal number, $\sim$ relation, finite/infinite/countable /uncountable set/enumerable [9, Definitions 2.3,2.4];
   (d) Example: $\mathbb{Z}$; Hilbert's paradox on Grand Hotel [11, http://en.wikipedia.org/wiki/Hilbert's_paradox_of_the_Grand_Hotel]; Movie: Hotel Infinity [2, http://www.imdb.com/title/tt0418737].
   (e) Theorem: Every infinite subset of a countable set is countable [9, Theorem 2.8].
   (f) Theorem: The set of all pairs of natural numbers is countable.
      i. The set of all rational numbers is countable.
      ii. Find an operation $*$ such that $(N, *)$ is a group.
      iii. Countable union of countable sets is countable. That is, if $S = \cup_{i=1}^{\infty} E_i$ where $E_i, i = 1, 2, \ldots$ be a sequence of countable sets, then $S$ is countable.
      iv. Let $\{E_n\}, 1 \leq n \leq k$ be a finite set of countable sets and $S = \times_{1 \leq n \leq k} E_n$. Then $S$ is countable.
      v. The set of all algebraic numbers is countable.
   (g) whether all infinite sets are countable ?
   (h) whether collection of all binary strings is countable ?
   (i) whether collection of all unary/decimal strings is countable ?
   (j) whether the set of all real numbers is countable ?
   (k) The real numbers in interval $[0, 1)$ are uncountable.
   (l) Let $A$ be a countable set. Then $2^A$ is uncountable.
   (m) We know from 1(f)iv that cartesian product of finitely many countable set is countable. Whether the cartesian product of countable many nonempty finite set is countable ? Whether the cartesian product of countable many countable set is countable ?
   (n) For next class: I already told that the set of real numbers is uncountable and you accepted and proved. But, how do u define a real number ? (we can realize what is natural number, integer, rational number)

5th August 2009

2. **Construction of Real Numbers(Dedekind's Cut) [9, Chapter 1],[8]**

(a) Purpose of Dedekind's cut: To provide a sound logical foundation of the real number system. (Why do we interested on real numbers?)

(b) Existence of non-rational numbers (for prime $p$, $\sqrt{p}$ is not rational, mathematical symbols like $e, \pi$ etc). Above mentioned non-rational numbers are expressible, but there may some more non-rational numbers because we do not know how to represent them.

(c) $A = \{x \in \mathbb{Q} : x^2 < p\}, B = \{x \in \mathbb{Q} : x^2 > p\}$ for a prime $p$. $A$ and $B$ contain no largest and smallest number respectively.

Hint: For every $s \in A$ or $B$, take $t = s - \frac{s^2-p}{s+p} = \frac{sp+s}{s+p}$ and $t^2 - p = \frac{(p^2-p)(s^2-p)}{(s+p)^2}$.

Motivation: In spite of dense property, rational number system has certain gaps, which leads to incompleteness.

(d) Terminologies(ordered set and field) to get a complete number system.

i. Order relation (i) Trichotomy law (ii) Transitivity.

ii. Ordered set ($<$ in $\mathbb{Q}$)).

iii. Bounded above/below, upper/lower bound.

iv. lub (sup)/glb(inf), uniqueness.
Examples: (i)Examples of sets having of [non]existence of lub/glb (ii)set A and B in Item 2c.

v. Least-upper-bound property (has $\mathbb{Q}$ lub property?).

(e) Theorem: LUB property of an ordered set $S$ implies GLB property of $S$.

(f) Field Axioms(A1-5, M1-5, D1), Ordered field;

(g) Dedekind's cut, $\mathbb{R}$;

10th August 2009

(h) Theorem: $\mathbb{R}$ is an ordered field which has least-upper-bound property. Moreover, $\mathbb{R}$ contains $\mathbb{Q}$ as subfield.

(i) Rationals and Irrationals;

12th August 2009

3. **Fundamentals of Integers**

(a) Principles of induction and the well-ordering principle [5];

(b) Divisibility;

i. Division Algorithm [5];

ii. If $n = 4k + 2$ or $n = 4k + 3$, then $n$ is not a square number.

iii. Notions of divisors/multiples, GCD [5];

iv. If $c$ divides $a_1, \ldots, a_k$, then $c$ divides $a_1u_1 + \ldots + a_ku_k$ for all integers $u_1, \ldots, u_k$.

v. If $a \mid b$ and $c \mid d$, must $a + c \mid b + d$ ?

vi. If $a = qb + r$ then $gcd(a, b) = gcd(b, r)$.

vii. Computing GCD and Euclids algorithm [5, 10], Bezout's identity [3];

viii. How many divisons one needs to run Euclid's algorithm ?

ix. For all +ve integers $n, a$ and $b$ and $gcd(a, n) = 1$ then $n \mid b$

x. Relative prime, Extended Euclid's algorithm and inverse finding Algorithm [10];

xi. For any integers $a, b, p$, if $gcd(a, p) = gcd(b, p) = 1$, then $gcd(ab, p) = 1$.

xii. What does extended Euclid algorithm for $F_{k+1}$ and $F_k$ returns ?

xiii. LCM [5];

17th August 2009

(c) Prime Numbers;

i. The fundamental Theorem of Arithmetic [3];

ii. If $gcd(p, a) = 1$ iff $gcd(p, a^k) = 1$;

iii. For $p$ prime, $p \mid a^k$ then $p \mid a$. Is this still valid for composite $p$ ? [5]

iv. [5, Exercise 2.3]

v. For prime $p$, if $p \mid ab$ then $p \mid a$ or $p \mid b$.

vi. Eisenstein's Criteria and some facts/examples on prime numbers [5];

vii. $3x^4 - 15x^2 + 10$ is irreducible (take $p = 5$), $p$-th cyclotomic polynomial i.e., $1 + x + \ldots + x^{p-1} = \frac{x^p-1}{x-1}$, where $p$ is prime, is irreducible ($f(x) = \frac{(x+1)^p-1}{x}$ is irreducible, then substitute $x$ by $x - 1$);

viii. Infiniteness of prime numbers [5];

ix. There are infinitely many primes of the form $4q + 3$ [5].

x. $p_n \leq 2^{2^{n-1}}$, where $p_n$ is the $n$-th prime [5].

xi. $\pi(x) \geq \lfloor \lg(\lg x)) \rfloor + 1$ (but it is very weak bound, prime number theorem $\lim_{x\to\infty} \pi(x) \to \frac{x}{\ln x}$ is a stronger bound) [5].

xii. Gaps in the series of primes (arbitrarily gaps in the series of primes) [4];

xiii. About the density of primes [5, Exercise 2.24].

xiv. $\sum_p$ is prime $\frac{1}{p}$ diverges. $\sum_{p\leq y} \frac{1}{p} > \log\log y - 1$ for real number $y \geq 2$ [4];

xv. If $2^m + 1$ is prime then $m = 2^n$ for some integer $n \geq 0$, Fermat number/prime [5].

xvi. If $m > 1$ and $a^m - 1$ is a prime, then $a = 2$ and $m$ is prime, Mersenne prime [5].

20th August 2009

(d) **Congruences** [5]

i. Motivation through finite number system and definition;

ii. $\equiv_n$ is an equivalence relation from $\mathbb{N}$ to $\mathbb{N}$;

iii. Operations preserved in equivalence classes, Complete residue system($Z_n$);

iv. Let $f(x) \in Z[x]$ and $n \geq 1$. If $a \equiv b \pmod{n}$ then $f(a) \equiv f(b) \pmod{n}$.

v. Let $f(x) \in Z[x]$ has an integer solution $a$ then $f(a) \equiv 0 \pmod{n}$ for all integers $n \geq 1$.

vi. There is no non-constant polynomial $f(x) \in Z[x]$ such that $f(x)$ is prime for all $x \in Z$.

vii. Theorem : Let $a, b$ and $m > 0$ be given integers and $d = (a, m)$. The congruence $ax \equiv b \pmod{m}$ has a solution iff $d \mid b$. If $x$ is a solution then $x + \frac{m}{d}t$ are the only solutions.

viii. Examples: 1. $10x \equiv 3 \pmod{12}$, 2. $10x \equiv 6 \pmod{12}$.

ix. Corollary: If $(a, n) = 1$, then $ax \equiv b \pmod{n}$ has single solution modulo $n$.

x. A. Let $d$ divides $a, b$ and $n$ and let $a' = a/d, b' = b/d$ and $n' = n/d$, then $ax \equiv b \pmod{n}$ iff $a'x \equiv b' \pmod{n'}$.

B. Let $(a, n) = 1$, $d$ divides $a$ and $b$ and let $a' = a/d, b' = b/d$, then $ax \equiv b \pmod{n}$ iff $a'x \equiv b' \pmod{n'}$.

C. Example [5, 3.12].

xi. Theorem(Lagrange): The congruence $a_n x^n + \ldots + a_1 x + a_0 \equiv 0 \pmod{p}, (a_n, p) = 1$ has at most $n$ solutions [1].

24th August 2009

xii. Chinese reminder theorem.

xiii. Comment at [5, 54], Example [5, 3.16].

xiv. Simultaneous non-linear congruences [5].

xv. $x \equiv y \pmod{m_i}$ for $1 \leq i \leq r$ iff $x \equiv y \pmod{[m_1, \ldots, m_r]}$.

xvi. [5] Let $n_1, \ldots, n_k$ be +ve integers, and let $a_1, \ldots, a_k$ be any integers. Then the simultaneous congruences

$$x \equiv a_1(\bmod n_1), \ldots, x \equiv a_k(\bmod n_k)$$

have a solution iff $gcd(n_i, n_j) \mid (a_i - a_j)$. There is a unique solution modulo $lcm(n1, n2, \ldots, n_k)$.

xvii. Find the solution of the congruences
$x \equiv 11 \pmod{36}$, $x \equiv 7 \pmod{40}$ and $x \equiv 32 \pmod{75}$.

26th August 2009

xviii. Wilson's lemma: $p$ is a prime iff $(p-1)! \equiv -1 \pmod{p}$ [4, 5].

xix. Complete residue system($\mathbb{Z}_n$), reduced residue system ($U_n$);

xx. Theorem: Let $(a, m) = 1$. Let $r_1, \ldots, r_n$ be a complete, or a reduced, residue system modulo $m$. Then $ar_1, \ldots, ar_n$ is a complete, or a reduced residue system modulo $m$.

xxi. Euler's $\phi$ function;

xxii. Euler's theorem: If $(a, m) = 1$, then $a^{\phi(m)} \equiv 1 \pmod{m}$ and Fermat's little theorem.

xxiii. $7 \mid (n^6 - 1)$ if $7 \nmid n$.

xxiv. If $p$ is prime and $e \geq 1$, then $\phi(p^e) = p^e - p^{e-1}$

xxv. Theorem: Let $A$ be a complete residue system mod $n$, $m, c \in Z$ and $(n, m) = 1$. Then the set $Am + c = \{am + c : a \in A\}$ is also complete residue system mod $n$.

xxvi. If $(m, m') = 1$ then $\phi(mm') = \phi(m)\phi(m')$.

xxvii. $\phi(n) = n \prod_{p|n} (1 - \frac{1}{p})$.

31st August 2009

xxviii. $\sum_{d|m} \phi(d) = m$.

(e) **The Group of Units** [5]

i. $U_n$ is an abelian group under multiplication modulo $n$.

ii. order of an element of a group, cyclic group, generator/primitive root of a cyclic group.

iii. If $ord_m(a) = h$, then the positive integers $k$ such that $a^k \equiv 1 \pmod{m}$ are precisely those for which $h \mid k$. If $(a, m) = 1$ then $ord_m(a) \mid \phi(m)$ [5].

iv. Algorithm to find primitive root; $a \in U_m$ is a primitive root iff $a^{\phi(m)/q} \neq 1$ in $U_m$ for each prime $q \mid \phi(m)$. Find primitive root of $U_{11}, U_9$ [5].

v. Let $a$ be a primitive root mod $m$. Then $a^d$ is a primitive root iff $(d, \phi(m)) = 1$.

vi. If $U_m$ has a primitive root then it has $\phi(\phi(m))$ many.

2nd, 7th and 14th September 2009

vii. If $p$ is prime, then $|\{a \in U_p : ord_p(a) = d, d \mid (p-1)\}| = \phi(d)$ [5].

viii. $U_p$ is cyclic group for any prime $p$ [5].

ix. If $p$ is an odd prime, then $U_{p^e}, e \geq 1$ is cyclic [5].

x. Find a primitive root of $U_{5^e}$ and $U_{7^e}$ for $e \geq 1$.

xi. $U_{2^e}$ is cyclic iff $e = 1$ or 2 [5].

xii. $U_n$ is cyclic iff $n = 1, 2, 4, p^e$ or $2p^e$ where $p$ is an odd prime and $e \geq 1$ [5].

xiii. Find a primitive root of $U_{2.3^e}$ and $U_{2.5^e}$ for $e \geq 1$.

5th october 2009

4. **Elementary Logic [7]**

(a) Introduction;

i. Logic is the analysis of methods of reasoning.

ii. Logic is studied in the form of the argument rather than the content of the argument.

iii. All mice fear cats. Jerry is a mouse. Hence Jerry fears cat.
All mice like cats. Jerry is a mouse. Hence Jerry likes cat.

iv. The truth or falsity of the particular premisses and conclusions is of no concern to the logician. He only wants to know only whether the truth of the premisses implies the truth of the conclusion.

v. The systematic formalization of reasoning is one of the main tasks of the logician.

(b) Propositional Calculus;

i. Sentences may be connected in different ways to form more complicated and compact sentences. Here, we consider only the *truth-functional* combination i.e., the truth or falsity of the new sentence is determined by the truth or falsity of its component sentences.

ii. Propositional connectives;

A. $\sim$ (*negation, not*);

B. $\wedge$ (*conjunction, and*);

C. $\vee$ (*disjunction, or*);

D. $\Rightarrow$ (*conditional/implication, if antecedent then consequent*);

E. $\iff$ (*biconditional/biimplication, if and only if/iff*);

iii. A propositional language $L$ is a propositional atoms (or, statement letters) $A, B, C, \ldots, p, q, r, \ldots$ etc.

iv. An atomic $L$-formula (or, atomic sentence) is an atom of $L$.

v. The set of $L$-formulas (or, statement forms) is generated inductively as follows:

A. If $A$ is an atomic $L$-formula, then $A$ is an $L$-formula.

B. If $\mathcal{A}$ is an $L$-formula, then $(\sim \mathcal{A})$ is an $L$-formula.

C. If $\mathcal{A}$ and $\mathcal{B}$ are $L$-formulas, then $(\mathcal{A} \wedge \mathcal{B}), (\mathcal{A} \vee \mathcal{B}), (\mathcal{A} \Rightarrow \mathcal{B}), (\mathcal{A} \iff \mathcal{B})$ are $L$-formulas.

vi. Example: $((A \iff B) \Rightarrow ((\sim A) \wedge B))$;

vii. The *degree* of a formula $\mathcal{A}$ is the number of propositional connectives present in $\mathcal{A}$. The degree of the formula in the preceding item is 4.

viii. Omitting parenthesises: It would be compact and profitable, to agree on some conventions to avoid the use of so many parenthesises in writing formulas.

A. Omit the outer parenthesis;

B. Connectives are preferred as following decreasing order: $\sim, \wedge, \vee, \Rightarrow, \iff$ ;

C. Follow by the association to the left in case of same weighted connectives;

ix. Example: $(A \iff B) \Rightarrow \sim A \wedge B$;

x. Exercises of number 2 of section 1, Chapter 1 of [7].

7th october 2009

(c) Assignments and Satisfiability

i. There are two truth values, $T$ and $F$, denoting truth and falsity.

ii. Let $L$ be a propososional language. An *$L$-assignment* is a mapping

$$M : \{p : p \text{ is an atom}\} \mapsto \{T, F\}.$$

Note that, if $L$ has $n$ atoms then there are $2^n$ different $L$-assignments.

iii. **Lemma :** For an $L$-assignment, there is a unique *$L$-valuation*

$$v_M : \{\mathcal{A} : \mathcal{A} \text{ is an } L\text{-formula}\} \mapsto \{T, F\}$$

given by the following clauses:

- $v_M(\sim \mathcal{A}) = \begin{cases} T & \text{if } v_M(A) = F, \\ F & \text{if } v_M(A) = T. \end{cases}$
- $v_M(\mathcal{A} \wedge \mathcal{B}) = \begin{cases} T & \text{if } v_M(\mathcal{A}) = v_M(\mathcal{B}) = T, \\ F & \text{if at least one of } v_M(\mathcal{A}), v_M(\mathcal{B}) \text{ is } F. \end{cases}$
- $v_M(\mathcal{A} \vee \mathcal{B}) = \begin{cases} T & \text{if at least one of } v_M(\mathcal{A}), v_M(\mathcal{B}) \text{ is } T, \\ F & \text{if } v_M(\mathcal{A}) = v_M(\mathcal{B}) = F. \end{cases}$
- $v_M(\mathcal{A} \Rightarrow \mathcal{B}) = v_M(\sim (\mathcal{A} \wedge \sim \mathcal{B}))$.
- $v_M(\mathcal{A} \iff \mathcal{B}) = \begin{cases} T & \text{if } v_M(\mathcal{A}) = v_M(\mathcal{B}), \\ F & \text{if } v_M(\mathcal{A}) \neq v_M(\mathcal{B}). \end{cases}$

iv. Let $M$ be an assignment. A formula $\mathcal{A}$ is said to be *true under $M$* if $v_M(\mathcal{A}) = T$ and *false under $M$* if $v_M(\mathcal{A}) = F$.

v. A formula $\mathcal{A}$ is said to be *satisfiable* if there exists an assignment $M$ which satisfies $\mathcal{A}$ i.e., $v_M(\mathcal{A}) = T$.

vi. A formula is called *tautology* if $v_M(\mathcal{A}) = T$ for all assignments $M$ i.e., $\mathcal{A}$ is true under all assignments (no matter what the truth value of atoms). Examples: $\mathcal{A} \vee (\sim \mathcal{A}), (\mathcal{A} \wedge \mathcal{B}) \Rightarrow \mathcal{A}$.

vii. A formula is called *contradiction* if $v_M(\mathcal{A}) = F$ for all assignments $M$ i.e., $\mathcal{A}$ is false under all assignments (no matter what the truth value of atoms). Examples: $\mathcal{A} \iff (\sim \mathcal{A})$ ($\mathcal{A}$ is a tautology iff $\sim \mathcal{A}$ is a contradiction.)

viii. If $\mathcal{A} \Rightarrow \mathcal{B}$ is a tautology, $\mathcal{A}$ is said to *logically imply* $\mathcal{B}$ or, alternatively, $\mathcal{B}$ is said to be a *logical consequence* of $\mathcal{A}$.

ix. If $\mathcal{A} \iff \mathcal{B}$ is a tautology, $\mathcal{A}$ and $\mathcal{B}$ are said to be *logically equivalent.*

x. If $\mathcal{A}$ and $\mathcal{A} \Rightarrow \mathcal{B}$ are tautologies, then so is $\mathcal{B}$.

xi. Principle of Duality: If $\mathcal{A}$ is a formula involving the connectives $\sim, \wedge$ and $\vee$, and $\mathcal{A}'$ arises from $\mathcal{A}$ by replacing each $\wedge$ by $\vee$ and each $\vee$ by $\wedge$, show that $\mathcal{A}$ is tautology iff $\sim \mathcal{A}'$ is tautology. Hence, if $\mathcal{A} \Rightarrow \mathcal{B}$ is a tautology, so is $\mathcal{B}' \Rightarrow \mathcal{A}'$ and if $\mathcal{A} \iff \mathcal{B}$ is a tautology, so is $\mathcal{A}' \iff \mathcal{B}'$.

(d) Adequate sets of connectives:

i. Every formula containing $n$ atoms generates a corresponding *truth function* of $n$ arguments. The arguments and values of the function are $T$ or $F$. The tabulated format of truth function for each assignment of arguments is called *truth table* of the function.

ii. Every formula can be generated by a formula involving the connectives $\sim, \wedge, \vee$.

iii. disnjuctive normal form, conjuctive normal form.

iv. Every truth function corresponds to a statement form containing as connectives only $\wedge$ and $\sim$, or only $\vee$ and $\sim$, or only $\Rightarrow$ and $\sim$.

12th october 2009

(e) An Axiom System for the Propositional Calculus [7]

i. A *formal theory* $\mathfrak{F}$ is defined when the following conditions are satisfied.
   A. A countable set of symbols is given as the symbols of $\mathfrak{F}$ and a sequence of symbols is called an *expression* of $\mathfrak{F}$.
   B. There is a subset of the expressions of $\mathfrak{F}$ is called *well formed formulas* (in short, "wfs") of $\mathfrak{F}$.
   C. A set of wfs is set aside and called the set of *axioms* of $\mathfrak{F}$
   D. There is a finite set $R_1, R_2, \ldots, R_n$ of relations among wfs, called *rules of inference*. For each $R_i, 1 \leq i \leq n$, there is a unique positive integer $j$ such that, for every set of $j$ wfs and each wf $\mathcal{A}$, one can effectively decide whether the given $j$ wfs are in the relation $R_i$ to $\mathcal{A}$, and, if so, $\mathcal{A}$ is called a *direct consequence* of the given wfs by virtue of inference.

ii. A formal axiomatic theory $L$ [7, Page 30].
   A. **Symbols**:
      (i) *primitive connectives*: $\sim, \Rightarrow, (, )$,
      (ii) *statement letters*: $A, B, \ldots, A_1, A_2, \ldots$.
   B. **wfs**:
      (i) All statement letters are wfs.
      (ii) If $A$ and $B$ are wfs, so are $(\sim A)$ and $A \Rightarrow B$.
   C. **Axioms**: If $\mathcal{A}, \mathcal{B}$ and $\mathcal{C}$ are wfs in $L$, then the followings are axioms of $L$.
      (A1). $(\mathcal{A} \Rightarrow (\mathcal{B} \Rightarrow \mathcal{A}))$
      (A2). $((\mathcal{A} \Rightarrow (\mathcal{B} \Rightarrow \mathcal{C})) \Rightarrow ((\mathcal{A} \Rightarrow \mathcal{B}) \Rightarrow (\mathcal{A} \Rightarrow \mathcal{C})))$
      (A3). $((\sim \mathcal{A} \Rightarrow \sim \mathcal{B}) \Rightarrow ((\sim \mathcal{A} \Rightarrow B) \Rightarrow \mathcal{A}))$
   D. **Inference rules**: The only rule of inference of $L$ is *modus ponens*(MP): If $\mathcal{A} \Rightarrow \mathcal{B}, \mathcal{A}$ then $\mathcal{B}$.

iii. Ex: are they wfs ?
   A. $\Rightarrow (\sim \mathcal{A})$
   B. $(B \Rightarrow \sim \mathcal{A})$
   C. $B \Rightarrow (\sim \mathcal{A})$

14th october 2009

iv. A *proof* and *theorem* in $\mathfrak{F}$.

v. Axiomatic theory, decidable and undecidable theory.

vi. Consequence of a wf $\mathcal{A}$ from a set of wfs $\Gamma$, proof (deduction) of $\mathcal{A}$ from $\Gamma$, $\Gamma \vdash \mathcal{A}$, hypotheses(premisses).

vii. Theorem
   A. If $\Gamma \subseteq \Delta$ and $\Gamma \vdash \mathcal{A}$, then $\Delta \vdash \mathcal{A}$.
   B. $\Gamma \vdash \mathcal{A}$ iff there is a finite subset $\Delta$ of $\Gamma$ such that $\Delta \vdash \mathcal{A}$.
   C. If $\Delta \vdash \mathcal{A}$, and, for each $\mathcal{B} \in \Delta$, $\Gamma \vdash \mathcal{B}$, then $\Delta \vdash \mathcal{A}$.

viii. Lemma: for any $\mathcal{A}, \mathcal{B}, \mathcal{C}$,
   (1). $\vdash_L \mathcal{A} \Rightarrow \mathcal{A}$.
   (2). $\mathcal{A} \Rightarrow \mathcal{B}, \mathcal{B} \Rightarrow \mathcal{C} \vdash_L \mathcal{A} \Rightarrow \mathcal{C}$.
   (3). $\vdash_L (\sim \mathcal{B} \Rightarrow \sim \mathcal{A}) \Rightarrow (\mathcal{A} \Rightarrow \mathcal{B})$.

ix. Deduction Theorem [7, page 32].

x. Soundness Theorem: Every theorem of $L$ is a tautology [7, page 35].

xi. Completeness Theorem: If a wf $\mathcal{A}$ of $L$ is a tautology, then it is a theorem of $L$ [7, page 36].

xii. The system $L$ is consistent i.e., there is no $\mathcal{A}$ such that both $\mathcal{A}, \sim \mathcal{A}$ are theorems of $L$.

xiii. Corollary: $L$ is consistent iff not all wfs are theorems.

xiv. A theory in which not all wfs are theorems is called *absolutely* consistent theory. Therefore, $L$ is absolutely consistent.

(f) Quantification Theory (Predicate logic).

i. Simple examples where propositional calculus can not be used.
Every person is precious. Sachin is a person. Therefore Sachin is precious.
How to write the above argument in logical form. Is it A, B, then C ?

ii. Predicate. P(x): P is a property of the object x. Ex, P stands for "is a person". Sachin is a constant object can be abbreviated by s. So, P(s) stands for Sachin is a person.

iii. Objects: constant, variable;

iv. Quantifiers. Universal quantifier: $(\forall x)(P(x) \Rightarrow R(x))$, $P(s)$, $R(s)$.
All prime numbers are odd. $(\forall x)(P(x) \Rightarrow O(x))$.
Some primes are even. $(\exists x)(P(x) \wedge E(x))$. Existential quantifier.

v. Relation between quantifiers: $(\exists x)\mathcal{A} \equiv \sim((\forall x) \sim \mathcal{A})$.

vi. Examples

A. Paris is beautiful. $B(p)$

B. If Federer practices he will win. $P(s) \Rightarrow W(s)$

C. All Math students are intelligent. $(\forall x)(M(x) \Rightarrow I(x))$

D. Some Math students are not intelligent. $(\exists x)(M(x) \wedge \sim I(x))$.

E. All grass is green. $(\forall y)G(y) \Rightarrow N(y)$

F. There is a winning combination. $(\exists x)(C(x) \wedge W(x))$.

G. Some students are brilliant in the NISER. $(\exists z)(N(x) \wedge B(x))$.

H. Non-unary predicate: Everybody loves Paris. $(\forall x)(L(x, p))$

I. Every even number is divisible by 2. $(\forall x)(E(x) \Rightarrow D(x, 2))$

J. There is no prime number between 23 and 29. $\sim(\exists z)(P(x) \wedge B(x, 23, 29))$.

K. Multiple quantifiers: Everybody is loved by somebody. $(\forall x)(\exists y)(L(x, y))$

L. Order of quantifiers does matter: Somebody is loved by everybody. $(\exists x)(\forall y)(L(x, y))$

M. How can we write it? : Any two numbers can be added together. $(\forall x)(\forall y)(\exists z)(E(x+y, z))$

vii. Functions (returns something): Amitabh's father is a professor. $(\exists x)(F(x, A) \wedge P(x))$ (is it okay ?)
We need another idea of a function. $P(f(A))$.

viii. Any two numbers can be added together. $(\forall x)(\forall y)(\exists z)(E(a(x, y), z))$

ix. Examples

A. Billy's father loves his mother. $L(f(b), m(b))$.

B. The square of every odd number is odd. $(\forall x)(O(x) \Rightarrow O(s(x)))$.

A. Alphabet of a quantifivcation theory, L:
(i) Constants: $a, b, c, \ldots, a_1, a_2, \ldots,$ (sometimes called individual symbols);
(ii) Variables: $x, y, z, x_1, x_2, \ldots$;
(iii) Panctuation symbols: $(,)$ and ,;
(iv) Logical connectives: $\sim, \Rightarrow, (\wedge, \vee, \iff)$;
(v) Quantifiers: $\forall, (\exists)$;
(vi) Predicate letters: $P_i^n$;
(vii) Function letters: $f_i^n$.

B. terms: The function letters applied to the variables and individual constants generate the terms, that is
(i) variables and constants are terms;
(ii) If $f_i^n$ is a function letter and $t_1, t_2, \ldots, t_n$ are terms, then $f_i^n(t_1, \ldots, t_n)$ is a term;
(iii) An expression is a term only if can be shown to be a term on the basis of clauses (i) and (ii).

C. Atomic formulas: The predicate letters applied to the terms yeild atomic formulas, that is, if $P_i^n$ is a predicate letter and $t_1, t_2, \ldots, t_n$ are terms, then $P_i^n(t_1, \ldots, t_n)$ is an atomic formula.

D. Well formed formulas: The well formed formulas (wfs) quantification theory is defined as follows:
(i) Every atomic formula is wf; (ii) If $\mathcal{A}$ and $\mathcal{B}$ are wfs then $(\sim \mathcal{A}), (\mathcal{A} \Rightarrow \mathcal{B})$ are wfs; (iii) If $\mathcal{A}$ is a wf and $x$ is a variable then $(\forall x)(\mathcal{A})$ is a wf; (iv) An expression is a wf only if can be shown to be a wf on the basis of clauses (i), (ii) and (iii).

E. Scope: In the wf $(\forall x)\mathcal{A}$ and $(\exists x)\mathcal{A}$, $\mathcal{A}$ is is said to be the scope of the quantifier $(\forall x)$ or $(\exists x)$.
Examples (position of brackets does mean): (i) $(\forall x)(P_1^2(x, y) \Rightarrow P_2^1(x))$ (ii) $(\forall x)P_1^2(x, y) \Rightarrow P_2^1(x)$

F. Bound: when a variable $x$ occurs within a scope of a quantifier $(\forall x)$ or $(\exists x)$, it is said to be bound. If a variable is not bounded, then it is said as free.

9th November 2009

G. Interpretation: An interpretation of a predicate logic is an association of the terms of the language with objects in a domain, together with an association of atomic wf with relations over the domain.
There are two essential ingrediants then:
(1) a non-empty domain of objects $D$;
(2) an association function $I$ which links constants, function symbols and predicate letters to $D$.

| **predicate logic symbols** | **Interpretation over non-empty domain D** |
|---|---|
| Constant | Element of D |
| n-ary function letter | Mapping of n-tuples of elememts of D into elements of D |
| n-ary predicate letter | n-ary relations on D |
| Quantifiers | The set D |

Examples of [6].

H. Valuation: A valuation $v$, in an interpretation, $I$, of a predicate logic, $L$, is a function from the terms of $L$ to the domain $D$, such that
(1) $v(c) = I(c)$. i.e., the same value as given by $I$ itself;
(2) $v(f_i^n(t_1, \ldots, t_n)) = f_i^n(v(t_1), \ldots, v(t_n))$;
(3) $v(x_i) \in D$, i.e., each variable is mapped onto some element of $D$.

I. Satisfiability:
(i) If $\mathcal{A} = A_j^n(t_1, \ldots, t_n)$ is an atomic wf and $A_j^n$ is the corresponding relation of the interpretation, I, then a valuation, $v$, satisfies $\mathcal{A}$ iff $A_j^n(v(t_1), \ldots, v_(t_n))$.
(ii) $v$ satisfies $\sim \mathcal{A}$ iff $v$ does not satisfy $\mathcal{A}$.
(iii) $v$ satisfies $\mathcal{A} \Rightarrow \mathcal{B}$ iff either $v$ does not satisfy $\mathcal{A}$ or $v$ satisfies $\mathcal{B}$.
(iv) $v$ satisfies $(\forall x_i)\mathcal{A}$ iff every valuation $w$ which differs at the variable $x_i$ satisfies $\mathcal{A}$. ($v$ satisfies $(\exists x_i)\mathcal{A}$ iff there are some valuation $w$ which differs at the variable $x_i$ satisfies $\mathcal{A}$.)

J. (i) A wf $\mathcal{A}$ is true (for the given interpretation $I$) iff every valuation in $I$ satisfies $\mathcal{A}$.
(ii) A wf $\mathcal{A}$ is false (for the given interpretation $I$) iff there is no valuation in $I$ satisfies $\mathcal{A}$.
(iii) An interpretation, $I$, is said to be a model for a set $\Gamma$ of wfs iff every wf in $\Gamma$ is true for $I$.
(iv) A wf $\mathcal{A}$ is said to be logically valid iff $\mathcal{A}$ is true for every interpretation.

(v) A wf $\mathcal{A}$ is said to be satisfiable iff there is an interpretation, $I$, for which $\mathcal{A}$ is satisfied by atleast one valuation in $I$.
(vi) A wf $\mathcal{A}$ is said to be logically valid iff $\sim \mathcal{A}$ is not satisfiable.
(vi) A wf $\mathcal{A}$ is said to be contradictory iff $\sim \mathcal{A}$ is logically valid i.e., $\sim \mathcal{A}$ is false for every interpretation.

x. first order languages (what is second order languages ?).

xi. First order theory; examples and its properties.

# References


[1] K. Chandrasekharan. *Introduction to Analytic Number Theory.* Springer-Verlag, 1968.

[2] The Internet Movie DataBAse. Imdb.

[3] I. N. Herstein. *Topics in Algebra.* John-Wiley & Sons, 1975.

[4] H. S. Zuckerman I. Niven and H. L. Montogomery. *An Introduction To The Theory of Numbers.* Willey Students Edition.

[5] G. A. Jones and J. M. Jones. *Elementary Number Theory.* Springer, 1998.

[6] J. Kelly. *The Essence of Logic.* PHI, 2002.

[7] E. Mendelson. *Introduction to Mathematical Logic.* Chapman & Hall/CRC, 2001.

[8] PlanetMath. http://planetmath.org.

[9] W. Rudin. *Principles of Mathematical Analysis.* McGraw-Hill Inc, Newyork, 1976.

[10] C. E Leiserson T. H. Coremen and R. L. Rivest. *Introduction to Algorithms.* PHI.

[11] WikiPedia. http://www.wikipedia.org/.

**NATIONAL INSTITUTE OF SCIENCE EDUCATION AND RESEARCH, BHUBANESWAR**

**Quiz 1(MA301): Elementary Number Theory**

(Construction of Real Numbers, Countability, Divisibility, Prime Numbers, Groups of Unit)

**Date: 07.09.2009** **Max Time:** 1 **Hour** **Total Mark:** 45

(You can answer as much you can, but you will score 40 as maximum)

1. Define real numbers through Dedekind's cut. [5]
2. Prove or disprove that the set of all functions $f : \mathbb{N} \mapsto \{0, 1\}$ is countable. [5]
3. Prove that [5 + 5]
   (a) if $gcd(a, b) = 1$ then $gcd(a + ab, b) = 1$;
   (b) if $F_k$ is the $k$-th number in Fibbonaci sequence then $gcd(F_{k+1}, F_k) = 1$ for any positive integer $k$.
4. Determine [5 + 5]
   (a) the last two digits of $9^{9^9}$;
   (b) $n$ such that $\phi(n) = \frac{n}{2}$.
5. Show that [5 + 5]
   (a) if $n$ is composite then $\phi(n) \leq n - \sqrt{(n)}$;
   (b) if the smallest prime factor $p$ of the positive integer $n$ exceeds $n^{\frac{1}{3}}$, then $\frac{n}{p}$ must be prime or 1.
6. Find a primitive root for $U_{11^e}$ for each $e \geq 1$. [5]

*I know numbers are beautiful. If they aren't beautiful, nothing is.*
**–Paul Erdös**

**NATIONAL INSTITUTE OF SCIENCE EDUCATION AND RESEARCH, BHUBANESWAR**

**Mid Sem Test(MA301): Elementary Number Theory**

**Date: 19.09.2009** **Max Time:** 2 **Hours** **Total Mark:** $\epsilon > 0$

1. Answer the followings $[\mathbf{.07 + .08 + .05 + .05}] \times \epsilon$
   (a) Prove $m^{\phi(n)} + n^{\phi(m)} \equiv 1 \pmod{mn}$, if $gcd(m, n) = 1$;
   (b) Find the last digit of the hexadecimal expansion of $5^{999,999} + 999,999^5$.
   (c) Show that $\{1^2, 2^2, \ldots, m^2\}$ is never a complete residue system modulo $m$ if $m > 2$;
   (d) If $p$ is an odd prime then show that $1^p + 2^p + \ldots + (p-1)^p \equiv 0 \pmod{p}$.
2. Show that $\mathbb{Q}$ is not well ordered set under usual $<$ order relation ? Is it possible to define an order relation $<'$ on $\mathbb{Q}$ to make $\mathbb{Q}$ as well ordered set under $<'$ ? Justify your answer. $[\mathbf{.1}] \times \epsilon$
3. Determine $[\mathbf{.05 + .05 + .05 + .05}] \times \epsilon$
   (a) $n$ such that $\phi(n) = \frac{n}{3}$;
   (b) the last digit of 13-ary representation of $11! + 12! + 13! + 14! + \ldots + 110!$;
   (c) $gcd(a + b, p^4)$ and $gcd(ab, p^4)$, if $gcd(a, p^2) = p$ and $gcd(b, p^3) = p^2$ and $p$ is prime.
   (d) the highest power of $p$ dividing $(p^n)!$ (*The Educational Times*, 1881);
4. Answer the followings $[\mathbf{.15 + .15}] \times \epsilon$
   (a) Is $U_{1250}$ cyclic ? If so, find a primitive element of $U_{1250}$ and find the number of primitive elements of $U_{1250}$?
   (b) Solve the congruences $x^4 \equiv 4 \pmod{13}$.
5. Answer the followings $[\mathbf{.05 + .1}] \times \epsilon$
   (a) Show that $42 \mid (n^7 - n)$ for any integer $n$.
   (b) A group of 5 thieves had stolen some gold biscuits from a bank. When they distributed equally with each other, 4 biscuits left. So, they fought each other and killed one thief. When they distributed equally the same again, 1 biscuit left. They fought again and one of them died. They distributed equally again with each other and 2 biscuits left. So, they fought again. Meanwhile, police came and they left all biscuits. However, how many gold biscuits were stolen?

*God invented the integers; all else is the work of man.*
**–Kronecker**

**NATIONAL INSTITUTE OF SCIENCE EDUCATION AND RESEARCH, BHUBANESWAR**

**Assignment 1(MA301): Logic (Propositional Calculus)**

**Date: 03.11.2009** **Deadline: 09.11.2009**

1. Write the followings senetences as statement forms using statement letters and verify whether the arguments are valid.
   (a) If Godel joins NISER, he lives in Bhubaneswar. Godel lives in Bhubaneswar. Therefore, Godel joins NISER.
   (b) Sachin or Dravid will be ranked in ICC's top 10 best batsmen list. If Sachin is ranked then Juvraj will be ranked unless Viru is ranked. Viru will be ranked if Dravid is not ranked. Therefore, Yuvraj will be ranked in the ICC's top 10 best batsman list.
   (c) If sensex is not improved then RBI cuts interest rate of loans or bankrupts result. If RBI does not cut interest rate, taxes are reduced. If taxes are reduced and sensex is not improved, then bankrupts will not result. So, RBI cuts interest rate.
   (d) If Federer reached Wimbeldon final then Nadal slipped up or Murray played very well. Nadal did not slip up unless Federer reached the final. Murray did not played well. Therefore, Federer reached the final if and only if Nadal slipped up.
   (e) If Godel joins NISER, he will be happy. If he is happy and likes his work, he will do good research unless he is paid well. If he is paid well, he likes his work. Therefore, if he joins NISER, he will do good research.
2. Let $L$ be the usual formal axiomatic theory for the propositional calculus. Prove the followings without using deduction theorem.
   (a) $\mathcal{A} \Rightarrow \mathcal{B}, \mathcal{B} \Rightarrow \mathcal{C} \vdash_L \mathcal{A} \Rightarrow \mathcal{C}$;
   (b) $\mathcal{A} \Rightarrow (\mathcal{B} \Rightarrow \mathcal{C}) \vdash_L \mathcal{B} \Rightarrow (\mathcal{A} \Rightarrow \mathcal{C})$;
3. Let $L$ be the usual formal axiomatic theory for the propositional calculus. Prove the followings.
   (a) $B, \mathcal{A} \Rightarrow (\mathcal{B} \Rightarrow \mathcal{C}) \vdash_L \mathcal{A} \Rightarrow \mathcal{C}$;
   (b) $\vdash_L \mathcal{A} \Rightarrow \mathcal{A}$;
4. For any wfs $\mathcal{A}, \mathcal{B}$ and $\mathcal{C}$, show that the followings are theorems of $L$.
   (a) $\mathcal{A} \Rightarrow (\mathcal{B} \Rightarrow (\mathcal{A} \wedge \mathcal{B}))$;
   (b) $\mathcal{A} \Rightarrow (\sim \mathcal{B} \Rightarrow \sim (\mathcal{A} \Rightarrow \mathcal{B}))$
   (c) $(\sim \mathcal{B} \Rightarrow \sim \mathcal{A}) \Rightarrow (\mathcal{A} \Rightarrow \mathcal{B})$.

*Logic is the anatomy of thought.*
– **Albert Einstein**