Elementary Number Theory and Logic
NISER-AM Semester 3 of 2008

1. **Construction of Real Numbers(Dedekind's Cut) [10, Chapter 1],[8]** (Date: 1,4 Aug'08)
   (a) Purpose of Dedekind's cut;
   (b) Existence of non-rational numbers (e.g., for prime $p$, $\sqrt{p}$ is not rational);
   (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: Inspite of dense property, rational number system has certain gaps, which leads to incompleteness.)
   (d) Terminologies: Order relation, Ordered set, Bounded above/below, lub/glb;
   (e) Least-upper-bound property (has $\mathbb{Q}$ lub property?);
   (f) Theorem: LUB property of an ordered set $S$ implies GLB property of $S$.
   (g) Field Axioms(A1-5, M1-5, D1), Ordered field;
   (h) Dedekind's cut, Definition of $\mathbb{R}$;
   (i) Theorem: $\mathbb{R}$ is an ordered field which has lub property. Moreover, $\mathbb{R}$ contains $\mathbb{Q}$ as subfield.;
   (j) Rationals and Irrationals;
   (k) Theorem: Archimedean property of $\mathbb{R}$;
   (l) $\mathbb{Q}$ is dense in $\mathbb{R}$.

2. **Countibility**(Date: 6 Aug'08)
   (a) Definitions: cardinal number, $\sim$ relation, finite/infinite/countable /uncountable set;
   (b) Theorem: Countable union of countable sets is countable.
   (c) Example: $\mathbb{Q}$ is countable.
   (d) The real numbers in interval $[0, 1)$ are uncountable.
   (e) If $A$ be a countable(infinite) set. Then $2^A$ is uncountable.

3. **Fundamentals of Integers**(Date: 11, 14 Aug'08)
   (a) Principles of induction, the well-ordering principle and their equivalence [6];

(b) Divisibility [6, 4];

  i. Division Algorithm, Notions of divisors/multiples, GCD;
  ii. Computing GCD and Euclids algorithm, Bezout's identity;
  iii. Relative prime, Extended Euclid's algorithm and inverse finding Algorithm;
  iv. LCM;

(c) Prime Numbers [6, 9];

  i. The fundamental Theorem of Arithmetic [5], GCD and LCM in terms of factorization;
  ii. If a positive integer is not a perfect square, then $\sqrt{m}$ is irrational. When $m^{\frac{1}{n}}$ is rational for positive integers $m, n$?
  iii. Infiniteness of prime numbers;
  iv. $p_n \leq 2^{2^{n-1}}$, where $p_n$ is the $n$-th prime.
  v. $\pi(x) \geq \lfloor \lg(\lg x)) \rfloor + 1$ (but it is very weak bound, prime number theorem $\lim_{x\to\infty} \pi(x) \to \frac{x}{\ln x}$ is a stronger bound).
  vi. Gaps in the series of primes (arbitrarily gaps in the series of primes);
  vii. There are infinitely many primes of the form $4q + 3$.
  viii. $\sum_{p \text{ is prime}} \frac{1}{p}$ diverges. $\sum_{p \leq y} \frac{1}{p} > \log\log y - 1$ for real number $y \geq 2$;
  ix. Eisenstein's Criteria and some facts/examples on prime numbers;
  x. $3x^4 - 15x^2 + 10$ 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 $x - 1$);

4. **Congruences** [6, 9](Date: 19, 21 Aug'08)

(a) Motivation through finite number system and definition;

(b) $\equiv_n$ is an equivalence relation from $\mathbb{N}$ to $\mathbb{N}$;

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

(d) Euler's $\phi$ function;

(e) 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 $m$.

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

(g) Theorem: Let $(m, m') = 1$. If $a$ runs through a complete residue system (mod $m$) and $a'$ runs through a complete residue system (mod $m'$), then $am' + am$ runs through a complete residue system (mod $mm'$) [3].

(h) Theorem: Let $(m, m') = 1$. If $a$ runs through a reduced residue system (mod $m$) and $a'$ runs through a reduced residue system (mod $m'$), then $am' + am$ runs through a reduced residue system (mod $mm'$) [3].

(i) If $(m, m') = 1$ then $\phi(mm') = \phi(m)\phi(m')$ [3].

(j) $\sum_{d|m} \phi(d) = m$ [3].

(k) $\phi(n) = n \prod_{p|n} (1 - \frac{1}{p})$ [3].

(l) Wilson's lemma: If $p$ is a prime, then $(p-1)! \equiv -1 \pmod{p}$.

(m) For $n \geq 1$, if $a \equiv_n b$ and $c \equiv_n d$ then $a + c \equiv_n b + d$, $ac \equiv_n bd$.

(n) Let $P$ be a polynomial over integers and $n \geq 1$. If $a \equiv_n b$ then $P(a) \equiv_n P(b)$.

(o) $ax \equiv ay \pmod{m}$ iff $x \equiv y \pmod{\frac{m}{(a,m)}}$.

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

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

(r) 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 [3].

(s) Chinese reminder theorem

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

(u) 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 $gcd(n_i, n_j) \mid (a_i - a_j)$.

5. **Quadratic Residues and Reciprocity** [2, 3]

(a) Definition, motivation(1. prime of the form $4k + 1$ as sum of two squares, 2. +ve integer as sum of four squares, 3. Polynomial time probabilistic algorithm to check primality.)

(b) There are exactly $\frac{p-1}{2}$ many quadratic residues and equally many quadratic non-residues in modulo $p$ [3].

(c) Euler's Criterion: If $p$ is an odd prime and $a$ is an integer. Then $a^{\frac{p-1}{2}} \equiv 1 \pmod{p}$;

(d) Legendre symbol;

(e) Corollary: if $p$ is an odd prime,

i. then $a^{\frac{p-1}{2}} \equiv \left(\frac{a}{p}\right) \pmod{p}$;

ii. $\sum_{a=1}^{p-1} \left(\frac{a}{p}\right) = 0$;

(f) Results: For odd prime $p$,

i. if $m_1 \equiv m_2 \pmod{p}$ then $\left(\frac{m_1}{p}\right) = \left(\frac{m_2}{p}\right)$;

ii. $\left(\frac{1}{p}\right) = 1$;

iii. $\left(\frac{a^2}{p}\right) = 1$;

iv. $\left(\frac{m}{p}\right)\left(\frac{n}{p}\right) = \left(\frac{mn}{p}\right)$;

v. $\left(\frac{ab^2}{p}\right) = \left(\frac{a}{p}\right)$;

vi. Examples: Compute $\left(\frac{-46}{17}\right), \left(\frac{20}{31}\right)$;

(g) If $p$ is an odd prime,

$$\left(\frac{-1}{p}\right) = \begin{cases} 1 & \text{if } p \equiv 1 \pmod 4 \\ -1 & \text{if } p \equiv 3 \pmod 4 \end{cases}$$

(h) There are infinitely many primes of the form $4k+1$.

(i) Gauss's lemma (with example $p = 7, a = 3$);

(j) $\left(\frac{2}{p}\right) = (-1)^{\frac{p^2-1}{8}}$;

(k) Theorem: If $p$ is an odd prime and $a$ an odd integer, with $(a, p) = 1$, then $\left(\frac{a}{p}\right) = (-1)^{\sum_{k=1}^{(p-1)/2} \lfloor \frac{ka}{p} \rfloor}$;

(l) Quadratic reciprocity law;

(m) $\left(\frac{p}{q}\right)\left(\frac{q}{p}\right) = (-1)^{\frac{p-1}{2}\frac{q-1}{2}}$ for odd prime $q \neq p$(when does $\left(\frac{p}{q}\right), \left(\frac{q}{p}\right)$ differ ?);

(n) $\left(\frac{p}{q}\right)\left(\frac{q}{p}\right) = \begin{cases} 1 & \text{if } p \equiv 1 \pmod 4 \text{ or } q \equiv 1 \pmod 4 \\ -1 & \text{if } p \equiv q \equiv 3 \pmod 4 \end{cases}$

$$\left(\frac{p}{q}\right) = \begin{cases} \left(\frac{q}{p}\right) & \text{if } p \equiv 1 \pmod 4 \text{ or } q \equiv 1 \pmod 4 \\ -\left(\frac{q}{p}\right) & \text{if } p \equiv q \equiv 3 \pmod 4 \end{cases}$$

(o) Compute $\left(\frac{a}{p}\right), (a, p) = 1$ (hint: $a = \pm 2^{k_0} p_1^{k_1} \ldots p_r^{k_r}$), $\left(\frac{17}{29}\right)$;

(p) Definition: Jacobi symbol [1];

(q) Results: For odd integers $P$ and $Q$,

i. if $m_1 \equiv m_2 \pmod P$ then $\left(\frac{m_1}{P}\right) = \left(\frac{m_2}{P}\right)$;

ii. $\left(\frac{m}{P}\right)\left(\frac{n}{P}\right) = \left(\frac{mn}{P}\right)$;

iii. $\left(\frac{m}{P}\right)\left(\frac{m}{Q}\right) = \left(\frac{m}{PQ}\right)$;

iv. $\left(\frac{a^2 n}{P}\right) = \left(\frac{n}{P}\right)$ whenever $(a, P) = 1$;

v. $\left(\frac{-1}{P}\right) = (-1)^{\frac{P-1}{2}}$;

vi. $\left(\frac{2}{P}\right) = (-1)^{\frac{P^2-1}{8}}$;

vii. $\left(\frac{P}{Q}\right)\left(\frac{Q}{P}\right) = (-1)^{\frac{P-1}{2}\frac{Q-1}{2}}$;

(r) If $x^2 \equiv n \pmod P$ has a solution then $\left(\frac{n}{P}\right) = 1$, but the converse is not true.

(s) Theorem: If $p$ is an odd prime and $(a, p) = 1$, then the congruence $x^2 \equiv a \pmod{p^n}, n \geq 1$ has a solution iff $\left(\frac{a}{p}\right) = 1$;

(t) Example: Find the the solution of $x^2 \equiv 23 \pmod{7^2}$, if any;

(u) Theorem: Let $a$ be an odd integer. Then

i. $x^2 \equiv a \pmod 2$ always has a solution;

ii. $x^2 \equiv a \pmod 4$ has a solution iff $a \equiv 1 \pmod 4$;

iii. $x^2 \equiv a \pmod{2^n}, n > 2$ has a solution iff $a \equiv 1 \pmod 8$;

(v) Corollary: Let $n = 2^{k_0} p_1^{k_1} \dots p_r^{k_r}$ be the prime factorization of $n > 1$ and $(a, n) = 1$. Then $x^2 \equiv a \pmod{n}$ is solvable iff

   i. $\left(\frac{a}{p_i}\right) = 1$ for $i = 1, 2, \dots, r$;
   ii. $a \equiv 1 \pmod{4}$ if $4 \mid n$, but $8 \nmid n$;
   iii. $a \equiv 1 \pmod{8}$ if $8 \mid n$;

6. **Continuing...**

## References


[1] T. M. Apostol. *Introduction to Analytic Number Theory*, Springer-Verlag, 1976.

[2] D. M. Burton. *Elementary Number Theory*, Mc-Graw-Hill.

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

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

[5] I. N. Herstein. *Topics in Algebra*.

[6] G. A. Jones and J. M. Jones. *Elementary Number Theory*, Springer Undergraduate Mathematics Series, Springer, 1998.

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

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

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

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