**CS 681: Computational Number Theory and Algebra** **Lecture 1**
**Lecturer: Manindra Agrawal** **Notes by: Zahir Koradia**

**August 2, 2005.**

# 1 References for the Course

1. Modern Computer Algebra by Von Zur Gathen and Jurgen Gerhard.
2. Introduction to Copmutational Number Theory by Victor Shoup (Available on author's website)
3. Writeups and papers on the web.

# 2 Basic Operations

## 2.1 1. In Number Theory

a.Addition, subtraction.
b.Multiplication, division, modulo, factorization, testing primality.
c.LCM,GCD.

## 2.2 2. In Algebra

### 2.2.1 A. Linear Algebra

a.Matrix Operations.
b.Solving system of linear equations.
c.Finding eigen values.

### 2.2.2 B. Polynomial Algebra

a.Addition, Multiplication.
b.Finding roots, factorization.
c.Checking irreducibility.

### 2.2.3 C. Abstract Algebra

a.Finding inverse of a group element.
b.Finding non-trivial homomorphisms.

c.Finding a generator set in a group.
d.Finding cosets.
e.Finding order of an element.

# 3 Tools for Designing Algorithms

1. Chinese remaindering.
2. Fast Fourier Transform.
3. Divide and Cnquer Technique.
4. Short vectors in a Lattice.
5. Elliptical curves.
6. Smooth numbers.
6. Hensel Lifting.

# 4 Reed-Solomon Code(Error correcting code)

Let $I$ be the entire data to be stored in a cd. Break I into chunks of $b * k$ bits.
Let $F$ be the finite field of size $2^b$.
Each chunk is coded seperately.

## 4.1 Coding one chunk of b*k bits

Break the chunk into k blocks of b bits.
Let these be $d_0, d_1, \ldots, d_{k-1}$
Treat each $d_i$ as an element of $F$
Let polynomial $P(x) = \sum_{i=0}^{k-1} d_i * x^i$
Let $e_0, e_1, \ldots, e_{n-1}$ be $n$ distinct elements of $F, n \leq 2^b$
Let $f_j = P(e_j)$
Then codeword corresponding to $d_0, d_1, \ldots, d_{k-1}$ ($k * b$ bits) is $f_0, f_1, \ldots, f_{n-1}$ ($n * b$ bits)
Note that $n > k$. This is where the redundancy comes in.