Summer 2013
NSERC USRA Report
Primality Testing and Factorization of Polynomials
Jiashuo Liu

It is easy to determine whether an integer is prime. One can use AKS Algorithim (Agrawal, Kayal and Saxena) or Miller Rabin Test. My first part of research is determining whether an ideal in the rings of integer is a prime ideal. We examined corresponding AKS and Miller Rabin Test in the number field.

To be precise, the problem is the following: given an ideal $\mathcal{A}$ of $\mathcal{O}_K$, where $K = \mathbb{Q}(\alpha)$ is a finite extension of $\mathbb{Q}$, α is algebraic over $\mathbb{Q}$, O_K is the rings of integers above $\mathbb{Z}$. If we find the integer a such that $a\mathbb{Z} = \mathcal{A} \cap \mathbb{Z}$, then a is prime if and only if $\mathcal{A}$ is a prime ideal. We can use Miller Rabin Algorithim to test the primality of a. The primality of a determines the primality of $\mathcal{A}$. The Miller Rabin Algorithim states the following:

Miller Rabin Test of $\mathbb{Z}$: Let m be a number, if $m > 2$ and is even, then m is not a prime. Assume m is odd, write $m - 1 = 2^e n$ with n odd. Let $f \leq e - 1$ be maximal such that there exists $x \in (\mathbb{Z}/m\mathbb{Z})^\times$ with $x^{n2^f} = -1$. Set

$$B = \{a \in (\mathbb{Z}/m\mathbb{Z})^\times \mid a^n \equiv 1 \pmod{m} \text{or there exists } 0 \leq j < e : a^{n2^j} \equiv -1 \pmod{m}\}$$

If $B = (\mathbb{Z}/m\mathbb{Z})^\times$, then m is prime. Equivalently, if m is composite, then B is not the entire multiplicative group.

Miller Rabin Test of number field: Given K a finite Galois extension of $\mathbb{Q}$, let O_K be the rings of integers over $\mathbb{Q}$. Let M be an ideal of O_K, define $[O_K : M] = m$. If m is even, then M is not a prime. Otherwise, write $m - 1 = 2^e n$ with n odd. Let $f \leq e - 1$ be maximal such that there exists $x \in (\mathbb{Z}/m\mathbb{Z})^\times$ with $x^{n2^f} = -1$.

$$B = \{a \in (O_K/M)^\times \mid a^n \equiv 1 \pmod{m} \text{or there exists } 0 \leq j < e : a^{n2^j} \equiv -1 \pmod{m}\}$$

If $B = (O_K/M)^\times$, then M is prime. Equivalently, if M is not a prime, then B is not the entire multiplicative group.

My second part of the research is on factorizations of polynomials. For any given ideal $\mathcal{A}$ in O_K, we have $\mathcal{A} = \prod_i \tilde{p}_i^{e_i}$ where each $\tilde{p}_i$ are prime ideals above prime integers p_i. We wish to factor integer polynomials. Fix $f \in \mathbb{Z}[x]$, a monic polynomial of α, assuming p is prime not dividing $\Delta(f)$, we can find the factors of f modulo p. In other words, we can determine the irreudicible factor of $\overline{f} \equiv f \pmod{p}$. If $\overline{g}$ is an irreducible factor of $\overline{f}$, then we can find the irreducible factor g of f such that $\overline{g} \equiv g \pmod{p}$. We can easily find factors $\overline{g}$ of $\overline{f}$; we need to check the irreducibility of $\overline{g}$. This can be done either by using probability argument or by assuming the General Riemann Hypothesis. With the assumption of GRH, if $\overline{g} \mid \overline{f}$, then we use Miller Rabin Test to decide if (g), the ideal generated by $\overline{g}$ is prime ideal. If $(\overline{g})$ is prime ideal, then $\overline{g}$ is irreducible factor of $\overline{f}$. Therefore, g is a irreducible factor of f.