Computational Algebraic Number Theory

Computational Algebraic Number Theory

http://www.sagemath.org
William Stein
Math 581f

October 12, 2007

Standard Problems of Algebraic Number Theory

Let K be a number field.

1. **Arithmetic:** Fast arithmetic, polynomial factorization, and linear algebra over K.
2. **Rings of integers:** Compute the ring of integers $\mathcal{O}_K$.
3. **Ideal factorizations:** Given a prime number $p \in \mathbb{Z}$, find the decomposition of the ideal $p\mathcal{O}_K$ as a product of prime ideals of $\mathcal{O}_K$. More generally, factor $I \subset \mathcal{O}_K$.
4. **Class groups:** Compute the class group of K, i.e., the group of fractional ideals modulo principal fractional ideals.
5. **Units:** Compute generators for the group $\mathcal{O}_K^*$ of units.
6. **Zeta functions:** Compute values of zeta functions of number fields.
7. **Explicit class field theory:** Explicitly compute certain abelian extensions of a number field K.
8. **Galois representations:** Compute invariants; modularity.

Arithmetic in Number Fields

- By the primitive element theorem $K = \mathbb{Q}(\alpha)$ for some α.
- So $K \cong \mathbb{Q}[x]/(f(x))$ via the map $\alpha \to x$.
- Multiplication in K involves multiplication of polynomials followed by reduction modulo f.
- Keep track of denominator separately, so all polynomial multiplication and reduction is over $\mathbb{Z}$.

SAGE: Arithmetic in Number Fields

- Uses the NTL library in general.
- Uses custom code by Robert Bradshaw for quadratic fields (this is faster than Magma and PARI).

```
sage: K.<a> = NumberField(x^4 + 17*x^3 + 2*x^2 + 3*
sage: b = (a+3)^20
sage: b
-15007159970698815014*a^3 - 15720972747597463l9*a^2
sage: time for _ in xrange(10^5): c=b*b
CPU time: 1.46 s,  Wall time: 1.50 s
```

Sage Quadratic field arithmetic...

Thanks to Robert Bradshaw, quadratic field arithmetic in Sage is very fast in Sage 2.8.7:

```
sage: K.<a> = QuadraticField(7)
sage: b = (2/3)*a + 5/8
sage: time for _ in xrange(10^5): c=b*b + b*b
CPU time: 0.30 s,  Wall time: 0.30 s
```

```
MAGMA:
> K<a> := QuadraticField(7);
> b := (2/3)*a + 5/8;
> time for i in [1..10^5] do c := b*b+b*b; end for;
Time: 0.490
```

```
PARI:
? a = quadgen(4*7);
? b = (2/3)*a + 5/8;
? gettime; for(i=0,10^5,c=b*b+b*b); gettime/1000.0
0.4130000000000000000000000000000000000
```

Polynomial Factorization over Number Fields

- Relative recent algorithm of K. Belabas, M. van Hoeij, J. Klueners, A. Steel, which uses the LLL algorithm to factor polynomials over number fields in polynomial time (See math.NT/0409510 on the arxiv).
- It is a very clever multimodular algorithm.
- Reading their paper, explaining it in your own words, and writing a "toy implementation" with examples, would be a great final project.

SAGE: Polynomial Factorization (part 1)

```
sage: K.<a> = NumberField(x^3 + x + 1); K
Number Field in a with defining polynomial
x^3 + x + 1
sage: S.<t> = K[]; S
Univariate Polynomial Ring in t over Number
Field in a with defining polynomial x^3 + x + 1
sage: f = (t^3 + a*t + a^2)^2 *
                (t^4 - 2/3*a*t + 17); f
t^10 + 2*a*t^8 + (2*a^2 - 2/3*a)*t^7 + ...
sage: factor(f)
(t^3 + a*t + a^2)^2 * (t^4 + (-2/3*a)*t + 17)
```

SAGE: Polynomial Factorization (part 2)

```
sage: # A relative extension
sage: L.<b> = NumberField(t^2 + a); L
Number Field in b with defining polynomial
      t^2 + a over its base field
sage: R.<X> = L[]; R
Univariate Polynomial Ring in X over Number Field
      in b with defining polynomial t^2 + a over it
sage: f = (X^4 + a)^3 * (X^2 + X + a); f
X^14 + X^13 + a*X^12 + 3*a*X^10 + 3*a*X^9 + ...
sage: factor(f)
(x + -a^2) * (x + a^2 + 1) * (x^2 + (-1)*b)^3
      * (x^2 + b)^3
```

Linear Algebra over Number Fields

```
sage: K.<a> = NumberField(x^2 + 17)
sage: n = 40
sage: m = matrix(K, n, [(a+1)^randint(0,3)
                   for _ in xrange(n^2)])
sage: time k = m*m
CPU time: 0.14 s,  Wall time: 0.27 s
sage: time f=m.charpoly()
CPU time: 23.93 s,  Wall time: 26.22 s
sage: m._clear_cache()
sage: g = pari(m)
sage: time h = g.charpoly()
Time: CPU 2.52 s, Wall: 2.76 s
sage: time m.echelonize()
CPU time: 0.35 s,  Wall time: 0.35 s
```

Student project: implement a multimodular algorithm for charpoly and det over number fields.

Linear algebra – same example in Magma

```
> R<x> := PolynomialRing(RationalField());
> K<a> := NumberField(x^2 + 17);
> n := 40;
> m := MatrixAlgebra(K, n)![(1+a)^Random(0, 3) : i
> time k := m*m;
Time: 0.000
> time f := CharacteristicPolynomial(m);
Time: 15.220
> time e := EchelonForm(m);
Time: 0.150
```

Computing the Ring of Integers

Most naive algorithm to compute $\mathcal{O}_K$ in $K \cong \mathbb{Q}[x]/(f(x))$, with f monic and integral.

1. Let $R = \mathbb{Z}[\alpha]$, where α is a root of f.
2. Compute $d = \mathrm{disc}(R) = \mathrm{disc}(f)$.
3. Factor d as $\prod p_i^{e_i}$.
4. We will prove (via easy linear algebra) that if a prime $p \mid [\mathcal{O}_K : R]$, then $p^2 \mid d$.
5. Thus the only primes that divide $[\mathcal{O}_K : R]$ are p_i for which $e_i \geq 2$.
6. For each such prime, check each element β of $\frac{1}{p_i}R$ for integrality, and if integral, replace R by $R[\beta]$.
7. At the end of the above steps, $R = \mathcal{O}_K$.

NOTE: There is a trick due to Lenstra that **very quickly** p-maximizes R, i.e., given p finds and S with $R \subset S$ such that $p \nmid [\mathcal{O}_K : S]$. I might explain it in this class.

SAGE: Computing the Ring of Integers

```
sage: K.<g> = NumberField(x^2 - 5)
sage: time R = K.ring_of_integers(); R
Maximal Order in Number Field in g with defining po
Time: CPU 0.00 s, Wall: 0.00 s
sage: R.basis()
[1/2*g + 1/2, g]
sage: R.basis()[0].minpoly()
x^2 - x - 1
sage: K.<a> = NumberField(x^3 - 2)
sage: time R = K.ring_of_integers(); R
Maximal Order in Number Field in a with defining po
Time: CPU 0.00 s, Wall: 0.00 s
sage: R.basis()
[1, a, a^2]
```

Ideal factorization

Class groups

For later....

Units

For later....

Zeta functions

```
From: Dick Gross <gross@math.harvard.edu>
Subject: zeta(-1)
Date: Mon, 15 Oct 2007 11:45:10 -0400
X-Mailer: Apple Mail (2.752.3)

William,

Nice to see you at the Clay conference.

Are there tables on the web of the values of zeta_k
real number fields k of small degree? If not, would
the time to send me these values for the real cyclo
degree < 20?

Dick
```

For later....

The spring quarter grad course on number theory will be on class field theory.

For later....

Thanks. Questions?