Third training school – RISC 2008

KANT/KASH tutorial

http://www.math.tu-berlin.de/~kant

LESSENI SYLLA

TU Berlin - Fakultät II

Institut für Mathematik Stra. des

17. Juni 136 D-10623 Berlin, Germany

lesseni(at)math.tu-berlin.de

Plan

Plan

- Introduction to KANT/KASH

Plan

- Introduction to KANT/KASH
- First steps in KASH3

Plan

- Introduction to KANT/KASH
- First steps in KASH3
- Applications

Applications

Applications

- Complex Numbers

Applications

- Complex Numbers
- Ideals

Applications

- Complex Numbers
- Ideals
- Residue Class Ring

Applications

- Complex Numbers
- Ideals
- Residue Class Ring
- Finite Fields

Applications

- Complex Numbers
- Ideals
- Residue Class Ring
- Finite Fields
- Lattices

Complex Numbers

Complex Numbers have a default precision of 30.
One can change the precision to arbitrary n.
The complex number `I` such that `I^2=-1` is predefined in KASH3.

Examples: `z:= 3+2*I;` `z^3;` `z^`$1/8$;
`Exp(2*PI*I);` `(2+9*I)/(1+5*I);`

NB: most real functions can be applied to complex numbers.

Some Functions:
`Log` (to the naturel base e), `Argument`, `Modulus`, `ComplexConjugate`, `Imaginary`, `Real`, `Gamma`, `ComplexToPolar`, `SquareRoot`, ...

Complex Numbers

Exercises: $1)$ Using the relation `Gamma(z+1)=z*Gamma(z)` $\forall z \in \mathbb{C}$ such that $Re(z) > 0$, show that `Gamma(n)` is a positive integer $\forall n \in \mathbb{N}\backslash\{0\}$.

$2)$ Give the polar form of:

```
4-7*I;
1/(3+I);
```

Ideals

KASH3 can handle integral ideals and fractional ideals.

Example 1:

```
L:=Ideal(Z,5);
J:=Ideal(EquationOrder(X^2+1),[7,123]);
K:=(1/2)*Ideal(MaximalOrder(X^3+2),4,9);
```

Example 2:

```
M:=MaximalOrder(X^2+5);
N:=Ideal(M,Matrix(Z,2,2,[1,1,0,2]));
ResidueClassField(N);
```

Some Functions:

`Intersection`, `IsPrime`, `AbsoluteNorm`, `Divisors`, `Degree`, `InertiaDegree`, `IsPrincipal`, `RamificationDegree`, `MakeCoprime`, `BasisMatrix`, ...

Ideals

The dictionary between fractional ideals and rational numbers:

Integral ideals	$\leftrightarrow$	integers
Fractional ideals	$\leftrightarrow$	(non zero) rational numbers
Inclusion	$\leftrightarrow$	divisibility
Sum	$\leftrightarrow$	GCD
Intersection	$\leftrightarrow$	LCM
Product	$\leftrightarrow$	product

NB:

If $(I_i)_{i\in J}$ are pairwise coprime ideals then
$\bigcap_{i\in J} I_i = \prod_{j\in J} I_j$.

Ideals

<u>Exercises:</u>

1) `Ideal(Z,6,9);`

2) Compute the intersection, the sum and the product of

   a) `12Z` and `9Z`.

   b) `5Z` and `7Z`.

3) Compute the maximal order `A` of `f:=X^2+5`. Compute the ideal `J` generated by 27 and 33 in `A`. Is it a principal ideal? Give the generator. Give the divisors of `J`. Is it possible to coumpute the residue class field of `J`? Is `A` a PID?

Residue Class Ring

Create the residue class ring $\mathbb{Z}/m\mathbb{Z}$ using the function `ResidueClassRing` or `IntegerRing`.

Example 1:

`A:=ResidueClassRing(6);`

NB: We use the function `Element` or `Coerce` to coerce an element in a set.

Example 2:

`Element(ResidueClassRing(5),16543);`

Some Functions:

`MultiplicativeGroup`, `UnitGroup`, `Size`, `PrimitiveElement`, `AdditiveGroup`, ...

Residue Class Ring

Exercises:

1) Find a function to compute all the square roots of the unity in the residue class ring of integers $modulo\ 9$.

2) Compute the inverse of 23467879 and 765432198673 in the residue class ring of integers $modulo\ 11$. Compute all the units.

3) Compute the order of 6 in the residue class ring of integers $modulo\ 7\hat{}7$.

Finite Fields

Create the finite fields using the functions `FiniteField` or `GF`.

Example:

```
A:=FiniteField(5);
B:=FiniteField(3,2);
C:=FiniteField(9);
```

Some functions: `CharacteristicPolynomial`, `DefiningPolynomial`, `MultiplicativeGroup`, `PrimitiveElement`, `PrimitivePolynomial`, ...

Exercises:

$1)$ Find a function to compute all the irreducible polynomials of degree 2 in the finite field of size 5.

$2)$ Compute all the 6^{th} and the 3^{th} roots of the unity in the finite field of size 7.

Lattices

In KASH3 lattices are represented as matrices. We can compute the Gram matrix and a LLL-reduced basis of a lattice.

`LLL` applied to a matrix M returns a matrix L whose rows are a LLL reduced basis for the lattice (over a real subring) spanned by the rows of M together with a unimodular matrix T over $\mathbb{Z}$ such that L = T * M, and the rank of M.

Also, we get `LLLGram`: it returns a LLL-reduced form of the Gram matrix M, together with the corresponding transformation matrix T and the rank of M.

Lattices

Examples:

```
N:=Matrix(Q,3,[1/2,3,2,3,0,1,2,9/2,2]);
LLL(N);
A:=GramMatrix(N);
LLLGram(A);
```

Exercises:

$1)$ Compute a square matrix 4×4, named A, with coefficients in $\mathbb{Q}$. Compute a unimodular matrix B such that $B.A$ has its rows LLL reduced basis for a lattice over a real subring. Give the rank of A.

$2)$ Is it possible to compute the `LLLGram` matrix of `M:=Matrix`$(4, [1/2, 3, 2, 5, 3, 7, 8, 9, 2, 8, 5, 6, 5, 9, 6, 2]);$