Computational tools for algebraic number theory

Grubb video introduction to CoCalc

Number theory as an empirical subject

$a^2+b^2=c^2$

quadratic reciprocity (Legendre, Gauss)

prime number theorem (Gauss, de la Vallée Poussin – Hadamard)

Fermat's last theorem

modularity of elliptic curves (Taniyama, Shimura, Weil, Cremona, Wiles, Taylor-Wiles)

$a^4+b^4+c^4=d^4$ (Euler, Elkies)

95800^4 + 217519^4 + 414560^4 = 422481^4

The L-Functions and Modular Forms Database

https://www.lmfdb.org

Absence of evidence vs. evidence of absence

A mathematician is like a blind person in a dark room looking for a black cat which isn't there. -- attribution unknown

$p(x) = x^3 + \cdots$ roots $\alpha_1, \alpha_2, \alpha_3 \in \mathbb{R}$

$$(\alpha_1 - \alpha_2)^2 (\alpha_1 - \alpha_3)^2 (\alpha_2 - \alpha_3)^2 > 0.$$

if $\alpha_1 \in \mathbb{R}$ $\alpha_2, \alpha_3 \in \mathbb{C} - \mathbb{R}$

$$\underbrace{(\alpha_1 - \alpha_2)^2 (\alpha_1 - \alpha_3)^2}_{} \underbrace{(\alpha_2 - \alpha_3)^2}_{} < 0.$$

Active tools for computational number theory

- Pari/GP (open-source, custom language or C API) Henri Cohen
- Magma (closed-source, custom language) — US educational institutions have free access
- SageMath (open-source, Python) Cython
- Nemo (open-source, Julia; part of the Oscar project)

Pari/GP $\subseteq$ SageMath

A quick start with CoCalc

See Thomas Grubb's video introduction.

Note: CoCalc can only provide access to open-source platforms (this excludes Magma).

Number fields in SageMath

Examples of constructing number fields:

- Quadratic fields (real or imaginary)
- Cyclotomic fields
- Adjoining a root of a polynomial
- Splitting field of a polynomial
- Iterated extensions

More functionality as time permits

- Trace and norm
- Discriminant
- Minimal polynomial
- Ring of integers
- Class number
- Unit group
- Factorization (in class number 1 cases)

In [7]:
```
K = QuadraticField(-1)
```

In [8]:
```
K
```

Out[8]:
```
Number Field in a with defining polynomial x^2 + 1 with a = 1*I
```

In [9]:
```
K(5).factor()
```

Out[9]:
```
(a) * (-a - 2) * (2*a + 1)
```

In [10]:
```
K2 = QuadraticField(2)
```

In [11]:
```
K2(7).factor()
```

Out[11]:
```
(-1) * (-2*a + 1) * (2*a + 1)
```

In [12]:
```
K3 = CyclotomicField(5)
```

In [15]:
```
z = K3.gen()
```

In [16]:
```
K3.<z> = CyclotomicField(5)
```

In [17]:
```
z^5
```

Out[17]:
```
1
```

In [18]:
```
z.minpoly()
```

Out[18]:
```
x^4 + x^3 + x^2 + x + 1
```

In [19]:
```
P.<x> = PolynomialRing(Rationals())
```

In [20]:
```
K4.<a> = NumberField(x^3-x+1)
```

In [21]:
```
K4.discriminant()
```

Out[21]:
```
-23
```

In [22]:
```
a^4
```

Out[22]:
```
a^2 - a
```

In [23]:
```
a.norm()
```

Out[23]:
```
-1
```

In [24]:
```
a.trace()
```

In [25]:
```
K5.<b> = (x^3-x+1).splitting_field()
```

In [26]:
```
K5.degree()
```

Out[26]:
```
6
```

In [27]:
```
K5
```

Out[27]:
```
Number Field in b with defining polynomial x^6 + 3*x^5 + 19*x^4 + 35*x^3 + 127*x^2 + 73*x + 271
```

In [29]:
```
(x^3-x+1).roots(K5)
```

Out[29]:
```
[(1/69*b^5 + 2/69*b^4 + 13/69*b^3 + 2/69*b^2 + 12/23*b - 100/69, 1),
 (-3/575*b^5 - 3/575*b^4 - 1/575*b^3 + 147/575*b^2 + 6/23*b + 906/575, 1),
 (-16/1725*b^5 - 41/1725*b^4 - 14/75*b^3 - 491/1725*b^2 - 18/23*b - 218/1725,
  1)]
```

In [30]:
```
K6.<c> = NumberField(x^3-x+a)
```

In [31]:
```
K6
```

Out[31]:
```
Number Field in c with defining polynomial x^3 - x + a over its base field
```

In [32]:
```
K4
```

Out[32]:
```
Number Field in a with defining polynomial x^3 - x + 1
```

In [34]:
```
K4.class_number()
```

Out[34]:
```
1
```

In [35]:
```
K4.ring_of_integers()
```

Out[35]:
```
Maximal Order in Number Field in a with defining polynomial x^3 - x + 1
```

In [36]:
```
R = K4.ring_of_integers()
```

In [39]:
```
K4.unit_group()
```

Out[39]:
```
Unit group with structure C2 x Z of Number Field in a with defining polynomial x^3 - x + 1
```

In [41]:
```
l = K4.unit_group().gens()
```

In [44]:
```
K4(l[1])
```

Out[44]:
```
a
```

In [45]:
```
a.multiplicative_order()
```

Out[45]:
```
+Infinity
```