Sage 快速参考:
基本数论

William Stein

Sage Version 3.4

http://wiki.sagemath.org/quickref

文中 m, n, a, b 等均为 ZZ 中元素

ZZ = **Z** = 所有整数

整数

$\ldots, -2, -1, 0, 1, 2, 3, 4, 5, 6, 7, 8, 9, 10, \ldots$

n 被 m 除的余数 `n % m`

`gcd(n,m)`, `gcd(`*list*`)`

扩展 gcd $g = sa + tb = \gcd(a, b)$: `g,s,t=xgcd(a,b)`

`lcm(n,m)`, `lcm(`*list*`)`

二项式系数 $\binom{m}{n}$ = `binomial(m,n)`

数值按进制展开: `n.digits(`*base*`)`

数值按进制展开的位数: `n.ndigits(`*base*`)`

(基 是可选项, 默认为 10)

整除 $n \mid m$: `n.divides(m)` 若 $nk = m$ 对于某 k

约数 – 所有满足 $d \mid n$ 的 d: `n.divisors()`

阶乘 – $n!$ = `n.factorial()`

素数

$2, 3, 5, 7, 11, 13, 17, 19, 23, 29, 31, 37, 41, 43, 47, \ldots$

素因数分解: `factor(n)`

素数检验: `is_prime(n)`, `is_pseudoprime(n)`

素幂检验: `is_prime_power(n)`

$\pi(x) = \#\{p : p \le x$ 为素数$\}$ = `prime_pi(x)`

素数集合: `Primes()`

$\{p : m \le p < n$ 且 p 为素数$\}$ =`prime_range(m,n)`

素数幂: `prime_powers(m,n)`

前 n 个素数: `primes_first_n(n)`

后一个素数与前一个素数: `next_prime(n)`, `previous_prime(n)`, `next_probable_prime(n)`

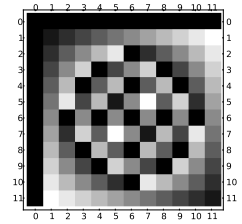
后一个与前一个素数幂: `next_prime_power(n)`, `pevious_prime_power(n)`

$2^p - 1$ 的 Lucas-Lehmer 素性检验

```
def is_prime_lucas_lehmer(p):
    s = Mod(4, 2^p - 1)
    for i in range(3, p+1): s = s^2 - 2
    return s == 0
```

模算术与同余

```
k=12; m = matrix(ZZ, k, [(i*j)%k for i in [0..k-1] for j in [0..k-1]]); m.plot(cmap='gray')
```



欧拉 $\phi(n)$ 函数: `euler_phi(n)`

Kronecker 符号 $\left(\frac{a}{b}\right)$ = `kronecker_symbol(a,b)`

二次剩余: `quadratic_residues(n)`

二次非剩余: `quadratic_residues(n)`

环 $\mathbf{Z}/n\mathbf{Z}$ = `Zmod(n) = IntegerModRing(n)`

a 模 n 视为 $\mathbf{Z}/n\mathbf{Z}$ 中的元素: `Mod(a, n)`

模 n 的本原根 = `primitive_root(n)`

$n \pmod m$ 的逆: `n.inverse_mod(m)`

乘方 $a^n \pmod m$: `power_mod(a, n, m)`

中国剩余定理: `x = crt(a,b,m,n)`

寻找 x 满足 $x \equiv a \pmod m$ 且 $x \equiv b \pmod n$

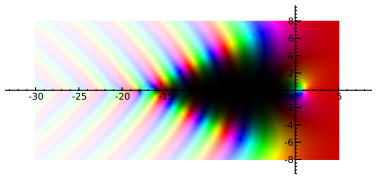
离散对数: `log(Mod(6,7), Mod(3,7))`

$a \pmod n$ 的阶 =`Mod(a,n).multiplicative_order()`

$a \pmod n$ 的平方根 =`Mod(a,n).sqrt()`

特殊函数

```
complex_plot(zeta, (-30,5), (-8,8))
```



$\zeta(s) = \prod_p \frac{1}{1-p^{-s}} = \sum \frac{1}{n^s}$ = `zeta(s)`

$\mathrm{Li}(x) = \int_2^x \frac{1}{\log(t)} dt$ = `Li(x)`

$\Gamma(s) = \int_0^\infty t^{s-1} e^{-t} dt$ = `gamma(s)`

连分数

```
continued_fraction(pi)
```

$$\pi = 3 + \cfrac{1}{7 + \cfrac{1}{15 + \cfrac{1}{1 + \cfrac{1}{292 + \cdots}}}}$$

连分数: `c=continued_fraction(x, `*bits*`)`

近似分数: `c.convergents()`

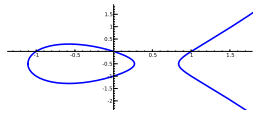
部分分子 p_n = `c.pn(n)`

部分分母 q_n = `c.qn(n)`

值: `c.value()`

椭圆曲线

```
EllipticCurve([0,0,1,-1,0]).plot(plot_points=300,thickness=3)
```



`E = EllipticCurve([`a_1, a_2, a_3, a_4, a_6`])`

$$y^2 + a_1xy + a_3y = x^3 + a_2x^2 + a_4x + a_6$$

E 的导子 N =`E.conductor()`

E 的判别式 Δ =`E.discriminant()`

E 的秩 = `E.rank()`

$E(\mathbf{Q})$ 的自由生成系 = `E.gens()`

j-不变量 = `E.j_invariant()`

$N_p = \#\{E$ 模 p 的解$\}$ = `E.Np(`*prime*`)`

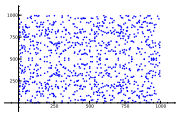
$a_p = p + 1 - N_p$ =`E.ap(`*prime*`)`

$L(E, s) = \sum \frac{a_n}{n^s}$ = `E.lseries()`

$\mathrm{ord}_{s=1} L(E, s)$ = `E.analytic_rank()`

模 p 椭圆曲线

```
EllipticCurve(GF(997), [0,0,1,-1,0]).plot()
```



`E = EllipticCurve(GF(p), [`a_1, a_2, a_3, a_4, a_6`])`

$\#E(\mathbf{F}_p)$ = `E.cardinality()`

$E(\mathbf{F}_p)$ 的生成系 = `E.gens()`

$E(\mathbf{F}_p)$ =`E.points()`