Kısa Sage Kılavuzu: Temel Sayılar Kuramı

William Stein (Türkçe'ye uyarlayan Kürşat Aker)

Sage Sürüm 3.4

`http://wiki.sagemath.org/quickref`

Bu belge boyunca, $m, n, a, b, vb.$ tamsayılardır ($\in$`ZZ`).

`ZZ` = $\mathbf{Z}$ = tamsayılar

Tamsayılar

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

n'nin m ile bölümünden *kalan* = `n % m`

`gcd(n,m)`, `gcd(`*sayı listesi*`)` obeb

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

`lcm(n,m)`, `lcm(`*sayı listesi*`)` ekok

binom katsayı $\binom{m}{n}$ = `binomial(m,n)`

`n`'nin verilen *taban*'ındaki ifadesi: `n.digits(`*taban*`)`

`n`'nin bu *taban*'daki basamak sayısı: `n.ndigits(`*taban*`)`

(*taban* tercihe bağlıdır, belirtilmezse 10 olarak varsayılır)

$n \mid m$ (n, m'yi böler) : `n.divides(m)`

bölenler – $d \mid n$ olan tüm d'ler: `n.divisors()`

faktöriyel – $n!$ = `n.factorial()`

Asal Sayılar

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

çarpanlara ayırma: `factor(n)`

asal mı?: `is_prime(n)`, `is_pseudoprime(n)`

asal kuvveti mi?: `is_prime_power(n)`

$\pi(x) = |\{p : p \leq x \text{ asal }\}|$ = `prime_pi(x)`

asal sayılar kümesi: `Primes()`

$\{p : m \leq p < n$ ve p asal$\}$ =`prime_range(m,n)`

asal kuvvetleri: `prime_powers(m,n)`

ilk n asal sayı: `primes_first_n(n)`

bir sonraki ve bir önceki asal sayı: `next_prime(n)`, `previous_prime(n)`, `next_probable_prime(n)`

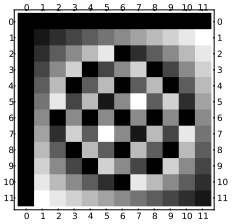
bir sonraki ve bir önceki asal kuvveti: `next_prime_power(n)`, `pevious_prime_power(n)`

$2^p - 1$ için Lucas-Lehmer asallık testi:

```
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
```

Modüler Aritmetik ve Kalandaşlık

```
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')
```



Euler $\phi(n)$ fonksiyonu: `euler_phi(n)`

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

Karesel kalandaşlar: `quadratic_residues(n)`

Karesel kalandaş olmayanlar: `quadratic_residues(n)`

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

a'nın n'ye göre kalanı ($\in \mathbf{Z}/n\mathbf{Z}$): `Mod(a, n)`

n'ye göre ilkel kökler = `primitive_root(n)`

a'nın çarpmaya göre tersi $\in \mathbf{Z}/n\mathbf{Z}$: `a.inverse_mod(n)`

$a^m \in \mathbf{Z}/n\mathbf{Z}$: `power_mod(a, m, n)`

Çin Kalan Teoremi: `x = crt(a,b,m,n)`
Öyle bir x bul ki, $x \equiv a \pmod{m}$ ve $x \equiv b \pmod{n}$'dir.

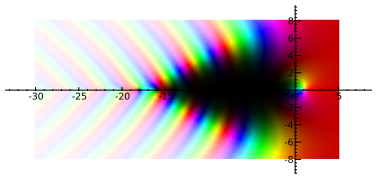
kesikli logaritma: `log(Mod(6,7), Mod(3,7))`

a'nın mertebesi = `Mod(a,n).multiplicative_order()`

a'nın mod n'de karekökü = `Mod(a,n).sqrt()`

Özel Fonksiyonlar

```
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)`

Sürekli Kesirler

```
continued_fraction(pi)
```

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

sürekli kesir: `c=continued_fraction(x,` *hassasiyet*`)`

`c`'nin yakınsarları: `c.convergents()`

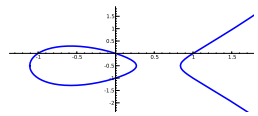
yakınsar payı, p_n = `c.pn(n)`

yakınsar paydası, q_n = `c.qn(n)`

değer: `c.value()`

Eliptik Eğriler

```
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'nin öncüsü =`E.conductor()`

E'nin diskriminantı, Δ = `E.discriminant()`

E'nin rankı = `E.rank()`

$E(\mathbf{Q})$'nın serbest üretenleri = `E.gens()`

j-değişmezi = `E.j_invariant()`

$N_p = E$'nin mod p'deki noktalarının sayısı = `E.Np(`*asal*`)`

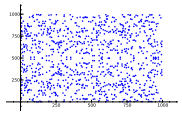
$a_p = p + 1 - N_p$ =`E.ap(`*asal*`)`

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

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

Mod p'de Eliptik Eğriler

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



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

$E(\mathbf{F}_p)$'nin nokta sayısı = `E.cardinality()`

$E(\mathbf{F}_p)$'nin üretenleri = `E.gens()`

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