```
> restart; with(numtheory);
```

[GIgcd, bigomega, cfrac, cfracpol, cyclotomic, divisors, factorEQ, factorset, fermat, imagunit, index, integral_basis, invcfrac, invphi, iscyclotomic, issqrfree, ithrational, jacobi, kronecker, λ, legendre, mcombine, mersenne, migcdex, minkowski, mipolys, mlog, mobius, mroot, msqrt, nearestp, nthconver, nthdenom, nthnumer, nthpow, order, pdexpand, ϕ, π, pprimroot, primroot, quadres, rootsunity, safeprime, σ, sq2factor, sum2sqr, τ, thue, φ] **(1)**

```
> numtheory[index](3,2,11); # discrete log of 2 with prim root 2
  modulo 11
```

8 **(2)**

```
> 2 &^ 8 mod 11; # check answer
```

3 **(3)**

```
> numtheory[primroot](11); # get first primitive root mod 11
```

2 **(4)**

```
> # check that it is prim root
  for i from 1 to 10 do i, 2&^ i mod 11; od;
```

1, 2
2, 4
3, 8
4, 5
5, 10
6, 9
7, 7
8, 3
9, 6
10, 1 **(5)**

```
> 2*2&^7 mod 11; # sol to 2 * x^7 equiv 3 (mod 11)
```

3 **(6)**

```
> # five 5-th roots of 10 modulo 11
  for i from 1 to 9 by 2 do 2 &^ i mod 11, (2 &^ i) &^ 5 mod 11;
  od;
```

2, 10
8, 10
10, 10
7, 10
6, 10 **(7)**

```
> g13 := numtheory[primroot](13);
```

$g13 := 2$ **(8)**

```
> a := 2 &^ 9 mod 13;
```

$a := 5$ **(9)**

```
> numtheory[index](a,g13,13);
```

9 **(10)**

```
> 2 &^ 9 mod 13;
```

5 **(11)**

```
> b1:= 8; b1 &^ 3 mod 13; # first 3-rd root of 5
```

$b1 := 8$
5 **(12)**

```
> b2:=2 &^ 7 mod 13; # second 3-rd root of 5
```

$b2 := 11$ **(13)**

```
> b2 &^ 3 mod 13;
```

(14)

5 **(14)**

```
> b3:=2 &^ 11 mod 13; # third 3-rd root of 5
```

$b3 := 7$ **(15)**

```
> b3 &^ 3 mod 13;
```

5 **(16)**

```
> 10 &^ 5 mod 11; # another 5-th root of 10 modulo 11
```

10 **(17)**

```
> # the 5 5-th roots of 10 modulo 11
  for i from 1 to 10 by 2 do # all odd indices
     2 &^ i mod 11,(2 &^ i) &^ 5 mod 11; od;
```

2, 10
8, 10
10, 10
7, 10
6, 10 **(18)**

```
> # the 8 8-th roots of 16 modulo 17
  for i from 1 to 16 do i,i &^ 8 mod 17; od;
```

1, 1
2, 1
3, 16
4, 1
5, 16
6, 16
7, 16
8, 1
9, 1
10, 16
11, 16
12, 16
13, 1
14, 16
15, 1
16, 1 **(19)**

```
> # all 11 quartic residues modulo 23
  # (all residues with even index)
  for i from 1 to 22 do i,i &^ 4 mod 23; od;
```

1, 1
2, 16
3, 12
4, 3
5, 4
6, 8
7, 9
8, 2
9, 6
10, 18
11, 13
12, 13
13, 18
14, 6
15, 2
16, 9

17, 8
18, 4
19, 3
20, 12
21, 16
22, 1 **(20)**

```
> p := 23;
```

$p := 23$ **(21)**

```
> a := 6; a &^ 11 mod 23; # Legendre symbol of 6 modulo 23
```

$a := 6$

1 **(22)**

```
> b := 6 &^ ((23+1)/4) mod 23; # squareroot of 6
```

$b := 12$ **(23)**

```
> b^2 mod 23;
```

6 **(24)**

> \`?\`

\`?\` **(25)**

```
>
```