

# PARI-GP Reference Card

(PARI-GP version 2.5.0)

Note: optional arguments are surrounded by braces {}.

## Starting & Stopping GP

to enter GP, just type its name: **gp**  
to exit GP, type **\q** or **quit**

## Help

describe function **?function**  
extended description **??keyword**  
list of relevant help topics **???pattern**

## Input/Output & Defaults

output previous line, the lines before **%, %', %'', etc.**  
output from line  $n$  **%n**  
separate multiple statements on line **;**  
extend statement on additional lines **\**  
extend statements on several lines **{seq<sub>1</sub>; seq<sub>2</sub>};**  
comment **/\* ... \*/**  
one-line comment, rest of line ignored **\\ ...**  
set default  $d$  to  $val$  **default({d},{val},{flag})**  
mimic behavior of GP 1.39 **default(compatible,3)**

## Metacommands

toggle timer on/off **#**  
print time for last result **##**  
print %n in raw format **\a n**  
print defaults **\d**  
set debug level to  $n$  **\g n**  
set memory debug level to  $n$  **\gm n**  
enable/disable logfile **\l {filename}**  
print %n in pretty matrix format **\m**  
set output mode (raw=0, default=1) **\o n**  
set  $n$  significant digits **\p n**  
set  $n$  terms in series **\ps n**  
quit GP **\q**  
print the list of PARI types **\t**  
print the list of user-defined functions **\u**  
read file into GP **\r filename**  
write %n to file **\w n filename**

## GP Within Emacs

to enter GP from within Emacs: **M-x gp, C-u M-x gp**  
word completion **(TAB)**  
help menu window **M-\c**  
describe function **M-?**  
display T<sub>E</sub>X'd PARI manual **M-x gpman**  
set prompt string **M-\p**  
break line at column 100, insert **M-\\**  
PARI metacommand  $\textit{letter}$  **M-\letter**

## Reserved Variable Names

$\pi = 3.14159\dots$  **Pi**  
Euler's constant  $= .57721\dots$  **Euler**  
square root of  $-1$  **I**  
big-oh notation **O**

## PARI Types & Input Formats

**t\_INT/t\_REAL**. Integers, Reals  $\pm n, \pm n.ddd$   
**t\_INTMOD**. Integers modulo  $m$  **Mod( $n, m$ )**  
**t\_FRAC**. Rational Numbers  $n/m$   
**t\_FFELT**. Elt in a Finite Field **ffgen(T)**  
**t\_COMPLEX**. Complex Numbers  $x + y * I$   
**t\_PADIC**.  $p$ -adic Numbers  $x + O(p^k)$   
**t\_QUAD**. Quadratic Numbers  $x + y * \text{quadgen}(D)$   
**t\_POLMOD**. Polynomials modulo  $g$  **Mod( $f, g$ )**  
**t\_POL**. Polynomials  $a * x^n + \dots + b$   
**t\_SER**. Power Series  $f + O(x^k)$   
**t\_QFI/t\_QFR**. Imag/Real bin. quad. forms **Qfb( $a, b, c, \{d\}$ )**  
**t\_RFRAC**. Rational Functions  $f/g$   
**t\_VEC/t\_COL**. Row/Column Vectors  $[x, y, z], [x, y, z]~$   
**t\_MAT**. Matrices  $[x, y, z; t; u, v]$   
**t\_LIST**. Lists **List( $[x, y, z]$ )**  
**t\_STR**. Strings **"aaa"**

## Standard Operators

basic operations  $+, -, *, /, ^$   
**i=i+1, i=i-1, i=i\*j, ...** **i++, i--, i\*=j, ...**  
euclidean quotient, remainder  $x \backslash y, x \backslash y, x \backslash y, \text{divrem}(x, y)$   
shift  $x$  left or right  $n$  bits  $x << n, x >> n$  or **shift( $x, \pm n$ )**  
comparison operators  $<=, <, >=, >, ==, !=$   
boolean operators (or, and, not) **||, &&, !**  
sign of  $x = -1, 0, 1$  **sign( $x$ )**  
maximum/minimum of  $x$  and  $y$  **max, min( $x, y$ )**  
integer or real factorial of  $x$  **x! or factorial( $x$ )**  
derivative of  $f$  w.r.t.  $x$  **f'**

## Conversions

### Change Objects

to vector, matrix, set, list, string **Col/Vec, Mat, Set, List, Str**  
create PARI object ( $x \bmod y$ ) **Mod( $x, y$ )**  
make  $x$  a polynomial of  $v$  **Pol( $x, \{v\}$ )**  
as above, starting with constant term **Polrev( $x, \{v\}$ )**  
make  $x$  a power series of  $v$  **Ser( $x, \{v\}$ )**  
PARI type of object  $x$  **type( $x$ )**  
object  $x$  with precision  $n$  **prec( $x, \{n\}$ )**  
evaluate  $f$  replacing vars by their value **eval( $f$ )**

### Select Pieces of an Object

length of  $x$  **#x or length( $x$ )**  
 $n$ -th component of  $x$  **component( $x, n$ )**  
 $n$ -th component of vector/list  $x$  **x[n]**  
 $(m, n)$ -th component of matrix  $x$  **x[m, n]**  
row  $m$  or column  $n$  of matrix  $x$  **x[m,], x[, n]**  
numerator of  $x$  **numerator( $x$ )**  
lowest denominator of  $x$  **denominator( $x$ )**

### Conjugates and Lifts

conjugate of a number  $x$  **conj( $x$ )**  
conjugate vector of algebraic number  $x$  **conjvec( $x$ )**  
norm of  $x$ , product with conjugate **norm( $x$ )**  
square of  $L^2$  norm of vector  $x$  **norml2( $x$ )**  
lift of  $x$  from Mods **lift, centerlift( $x$ )**

## Random Numbers

random integer between 0 and  $N - 1$  **random({N})**  
get random seed **getrand()**  
set random seed to  $s$  **setrand( $s$ )**

## Lists, Sets & Sorting

sort  $x$  by  $k$ th component **vecsort( $x, \{k\}, \{fl = 0\}$ )**  
**Sets** (= row vector of strings with strictly increasing entries)  
intersection of sets  $x$  and  $y$  **setintersect( $x, y$ )**  
set of elements in  $x$  not belonging to  $y$  **setminus( $x, y$ )**  
union of sets  $x$  and  $y$  **setunion( $x, y$ )**  
look if  $y$  belongs to the set  $x$  **setsearch( $x, y, \{flag\}$ )**  
**Lists**  
create empty list  $L$  **L = List()**  
append  $x$  to list  $L$  **listput( $L, x, \{i\}$ )**  
remove  $i$ -th component from list  $L$  **listpop( $L, \{i\}$ )**  
insert  $x$  in list  $L$  at position  $i$  **listinsert( $L, x, i$ )**  
sort the list  $L$  in place **listsort( $L, \{flag\}$ )**

## Programming & User Functions

**Control Statements** ( $X$ : formal parameter in expression  $seq$ )  
eval.  $seq$  for  $a \leq X \leq b$  **for( $X = a, b, seq$ )**  
eval.  $seq$  for  $X$  dividing  $n$  **fordiv( $n, X, seq$ )**  
eval.  $seq$  for primes  $a \leq X \leq b$  **forprime( $X = a, b, seq$ )**  
eval.  $seq$  for  $a \leq X \leq b$  stepping  $s$  **forstep( $X = a, b, s, seq$ )**  
multivariable for **forvec( $X = v, seq$ )**  
if  $a \neq 0$ , evaluate  $seq_1$ , else  $seq_2$  **if( $a, \{seq_1\}, \{seq_2\}$ )**  
evaluate  $seq$  until  $a \neq 0$  **until( $a, seq$ )**  
while  $a \neq 0$ , evaluate  $seq$  **while( $a, seq$ )**  
exit  $n$  innermost enclosing loops **break({n})**  
start new iteration of  $n$ th enclosing loop **next({n})**  
return  $x$  from current subroutine **return({x})**  
error recovery (try  $seq_1$ ) **trap({err}, {seq<sub>2</sub>}, {seq<sub>1</sub>})**

### Input/Output

print args with/without newline **print(), print1()**  
formatted printing **printf()**  
read a string from keyboard **input()**  
output  $args$  in T<sub>E</sub>X format **printtex( $args$ )**  
write  $args$  to file **write, writel, writetex( $file, args$ )**  
read file into GP **read({file})**

### Interface with User and System

allocates a new stack of  $s$  bytes **allocatemem({s})**  
execute system command  $a$  **system( $a$ )**  
as above, feed result to GP **extern( $a$ )**  
install function from library **install( $f, code, \{gpf\}, \{lib\}$ )**  
alias  $old$  to  $new$  **alias( $new, old$ )**  
new name of function  $f$  in GP 2.0 **whatnow( $f$ )**

### User Defined Functions

**name(formal vars) = my(local vars); seq**  
**struct.member = seq**  
kill value of variable or function  $x$  **kill( $x$ )**

## Iterations, Sums & Products

numerical integration **intnum( $X = a, b, expr, \{flag\}$ )**  
sum  $expr$  over divisors of  $n$  **sumdiv( $n, X, expr$ )**  
sum  $X = a$  to  $X = b$ , initialized at  $x$  **sum( $X = a, b, expr, \{x\}$ )**  
sum of series  $expr$  **suminf( $X = a, expr$ )**  
sum of alternating/positive series **sumalt, sumpos**  
product  $a \leq X \leq b$ , initialized at  $x$  **prod( $X = a, b, expr, \{x\}$ )**  
product over primes  $a \leq X \leq b$  **prodeuler( $X = a, b, expr$ )**  
infinite product  $a \leq X \leq \infty$  **prodinf( $X = a, expr$ )**  
real root of  $expr$  between  $a$  and  $b$  **solve( $X = a, b, expr$ )**

Vectors & Matrices

dimensions of matrix $x$	<code>matsize(<math>x</math>)</code>
concatenation of $x$ and $y$	<code>concat(<math>x, \{y\}</math>)</code>
extract components of $x$	<code>vecextract(<math>x, y, \{z\}</math>)</code>
transpose of vector or matrix $x$	<code>mattranspose(<math>x</math>)</code> or <code>x-</code>
adjoint of the matrix $x$	<code>matadjoint(<math>x</math>)</code>
eigenvectors of matrix $x$	<code>mateigen(<math>x</math>)</code>
characteristic polynomial of $x$	<code>charpoly(<math>x, \{v\}, \{flag\}</math>)</code>
minimal polynomial of $x$	<code>minpoly(<math>x, \{v\}</math>)</code>
trace of matrix $x$	<code>trace(<math>x</math>)</code>

Constructors & Special Matrices

row vec. of $expr$ eval'd at $1 \leq i \leq n$	<code>vector(<math>n, \{i\}, \{expr\}</math>)</code>
col. vec. of $expr$ eval'd at $1 \leq i \leq n$	<code>vectorv(<math>n, \{i\}, \{expr\}</math>)</code>
matrix $1 \leq i \leq m, 1 \leq j \leq n$	<code>matrix(<math>m, n, \{i\}, \{j\}, \{expr\}</math>)</code>
diagonal matrix with diagonal $x$	<code>matdiagonal(<math>x</math>)</code>
$n \times n$ identity matrix	<code>matid(<math>n</math>)</code>
Hessenberg form of square matrix $x$	<code>mathess(<math>x</math>)</code>
$n \times n$ Hilbert matrix $H_{ij} = (i + j - 1)^{-1}$	<code>mathilbert(<math>n</math>)</code>
$n \times n$ Pascal triangle $P_{ij} = \binom{i}{j}$	<code>matpascal(<math>n - 1</math>)</code>
companion matrix to polynomial $x$	<code>matcompanion(<math>x</math>)</code>

Gaussian elimination

determinant of matrix $x$	<code>matdet(<math>x, \{flag\}</math>)</code>
kernel of matrix $x$	<code>matker(<math>x, \{flag\}</math>)</code>
intersection of column spaces of $x$ and $y$	<code>matintersect(<math>x, y</math>)</code>
solve $M * X = B$ ( $M$ invertible)	<code>matsolve(<math>M, B</math>)</code>
as solve, modulo $D$ (col. vector)	<code>matsolvemod(<math>M, D, B</math>)</code>
one sol of $M * X = B$	<code>matinverseimage(<math>M, B</math>)</code>
basis for image of matrix $x$	<code>matimage(<math>x</math>)</code>
supplement columns of $x$ to get basis	<code>mat supplement(<math>x</math>)</code>
rows, cols to extract invertible matrix	<code>matindexrank(<math>x</math>)</code>
rank of the matrix $x$	<code>matrank(<math>x</math>)</code>

Lattices & Quadratic Forms

upper triangular Hermite Normal Form	<code>mathnf(<math>x</math>)</code>
HNF of $x$ where $d$ is a multiple of $\det(x)$	<code>mathnfmod(<math>x, d</math>)</code>
elementary divisors of $x$	<code>matsnf(<math>x</math>)</code>
LLL-algorithm applied to columns of $x$	<code>qflll(<math>x, \{flag\}</math>)</code>
like qflll, $x$ is Gram matrix of lattice	<code>qflllgram(<math>x, \{flag\}</math>)</code>
LLL-reduced basis for kernel of $x$	<code>matkerint(<math>x</math>)</code>
<b>Z</b> -lattice $\longleftrightarrow$ <b>Q</b> -vector space	<code>matrixqz(<math>x, p</math>)</code>
signature of quad form $t^y * x * y$	<code>qfsign(<math>x</math>)</code>
decomp into squares of $t^y * x * y$	<code>qfgaussred(<math>x</math>)</code>
find up to $m$ sols of $t^y * x * y \leq b$	<code>qfminim(<math>x, b, m</math>)</code>
$v, v[i] :=$ number of sols of $t^y * x * y = i$	<code>qfrep(<math>x, B, \{flag\}</math>)</code>
eigenvals/eigenvecs for real symmetric $x$	<code>qfjacobi(<math>x</math>)</code>

Formal & p-adic Series

truncate power series or $p$ -adic number	<code>truncate(<math>x</math>)</code>
valuation of $x$ at $p$	<code>valuation(<math>x, p</math>)</code>
<b>Dirichlet and Power Series</b>	
Taylor expansion around 0 of $f$ w.r.t. $x$	<code>taylor(<math>f, x</math>)</code>
$\sum a_k b_k t^k$ from $\sum a_k t^k$ and $\sum b_k t^k$	<code>serconvol(<math>x, y</math>)</code>
$f = \sum a_k t^k$ from $\sum (a_k / k!) t^k$	<code>serlaplace(<math>f</math>)</code>
reverse power series $F$ so $F(f(x)) = x$	<code>serreverse(<math>f</math>)</code>
Dirichlet series multiplication / division	<code>dirmul, dirdiv(<math>x, y</math>)</code>
Dirichlet Euler product ( $b$ terms)	<code>direuler(<math>p = a, b, expr</math>)</code>

p-adic Functions

Teichmuller character of $x$	<code>teichmuller(<math>x</math>)</code>
Newton polygon of $f$ for prime $p$	<code>newtonpoly(<math>f, p</math>)</code>

PARI-GP Reference Card

(PARI-GP version 2.5.0)

Polynomials & Rational Functions

degree of $f$	<code>poldegree(<math>f</math>)</code>
coefficient of degree $n$ of $f$	<code>polcoeff(<math>f, n</math>)</code>
round coeffs of $f$ to nearest integer	<code>round(<math>f, \{\&amp;e\}</math>)</code>
gcd of coefficients of $f$	<code>content(<math>f</math>)</code>
replace $x$ by $y$ in $f$	<code>subst(<math>f, x, y</math>)</code>
discriminant of polynomial $f$	<code>poldisc(<math>f</math>)</code>
resultant of $f$ and $g$	<code>polresultant(<math>f, g, \{v\}, \{flag\}</math>)</code>
as above, give $[u, v, d], xu + yv = d$	<code>bezoutres(<math>x, y</math>)</code>
derivative of $f$ w.r.t. $x$	<code>deriv(<math>f, x</math>)</code>
formal integral of $f$ w.r.t. $x$	<code>intformal(<math>f, x</math>)</code>
reciprocal poly $x^{\deg f} f(1/x)$	<code>polrecip(<math>f</math>)</code>
interpol. pol. eval. at $a$	<code>polinterpolate(<math>X, \{Y\}, \{a\}, \{\&amp;e\}</math>)</code>
initialize $t$ for Thue equation solver	<code>thueinit(<math>f</math>)</code>
solve Thue equation $f(x, y) = a$	<code>thue(<math>t, a, \{sol\}</math>)</code>

Roots and Factorization

number of real roots of $f, a < x \leq b$	<code>polsturm(<math>f, \{a\}, \{b\}</math>)</code>
complex roots of $f$	<code>polroots(<math>f</math>)</code>
symmetric powers of roots of $f$ up to $n$	<code>polsym(<math>f, n</math>)</code>
roots of $f$ mod $p$	<code>polrootsmod(<math>f, p, \{flag\}</math>)</code>
factor $f$	<code>factor(<math>f, \{lim\}</math>)</code>
factorization of $f$ mod $p$	<code>factormod(<math>f, p, \{flag\}</math>)</code>
factorization of $f$ over $F_{p^a}$	<code>factorff(<math>f, p, a</math>)</code>
$p$ -adic fact. of $f$ to prec. $r$	<code>factorpadic(<math>f, p, r, \{flag\}</math>)</code>
$p$ -adic roots of $f$ to prec. $r$	<code>polrootspadic(<math>f, p, r</math>)</code>
$p$ -adic root of $f$ cong. to $a$ mod $p$	<code>padicappr(<math>f, a</math>)</code>
Newton polygon of $f$ for prime $p$	<code>newtonpoly(<math>f, p</math>)</code>

Special Polynomials

$n$ th cyclotomic polynomial in var. $v$	<code>polcyclo(<math>n, \{v\}</math>)</code>
$d$ -th degree subfield of $\mathbf{Q}(\zeta_n)$	<code>polsubcyclo(<math>n, d, \{v\}</math>)</code>
$n$ -th Legendre polynomial	<code>pollegendre(<math>n, \{v = x\}</math>)</code>
$n$ -th Tchebicheff polynomial	<code>polchebyshev(<math>n, \{flag\}, \{v = x\}</math>)</code>
Zagier's polynomial of index $n, m$	<code>polzagier(<math>n, m</math>)</code>

Transcendental Functions

real, imaginary part of $x$	<code>real(<math>x</math>), imag(<math>x</math>)</code>
absolute value, argument of $x$	<code>abs(<math>x</math>), arg(<math>x</math>)</code>
square/ $n$ th root of $x$	<code>sqrtn(<math>x, n, \{\&amp;z\}</math>)</code>
trig functions	<code>sin, cos, tan, cotan</code>
inverse trig functions	<code>asin, acos, atan</code>
hyperbolic functions	<code>sinh, cosh, tanh</code>
inverse hyperbolic functions	<code>asinh, acosh, atanh</code>
exponential of $x$	<code>exp(<math>x</math>)</code>
natural log of $x$	<code>ln(<math>x</math>)</code> or <code>log(<math>x</math>)</code>
gamma function $\Gamma(x) = \int_0^\infty e^{-t} t^{x-1} dt$	<code>gamma(<math>x</math>)</code>
logarithm of gamma function	<code>lngamma(<math>x</math>)</code>
$\psi(x) = \Gamma'(x) / \Gamma(x)$	<code>psi(<math>x</math>)</code>
incomplete gamma function ( $y = \Gamma(s)$ )	<code>incgam(<math>s, x, \{y\}</math>)</code>
exponential integral $\int_x^\infty e^{-t} / t dt$	<code>eint1(<math>x</math>)</code>
error function $2 / \sqrt{\pi} \int_x^\infty e^{-t^2} dt$	<code>erfc(<math>x</math>)</code>
dilogarithm of $x$	<code>dilog(<math>x</math>)</code>
$m$ th polylogarithm of $x$	<code>polylog(<math>m, x, \{flag\}</math>)</code>
$U$ -confluent hypergeometric function	<code>hyperu(<math>a, b, u</math>)</code>
$J$ -Bessel function, $J_{n+1/2}(x)$	<code>besselj(<math>n, x</math>), besseljh(<math>n, x</math>)</code>
$K$ -Bessel function of index $nu$	<code>besselk(<math>nu, x</math>)</code>

Elementary Arithmetic Functions

vector of binary digits of $ x $	<code>binary(<math>x</math>)</code>
give bit number $n$ of integer $x$	<code>bittest(<math>x, n</math>)</code>
ceiling of $x$	<code>ceil(<math>x</math>)</code>
floor of $x$	<code>floor(<math>x</math>)</code>
fractional part of $x$	<code>frac(<math>x</math>)</code>
round $x$ to nearest integer	<code>round(<math>x, \{\&amp;e\}</math>)</code>
truncate $x$	<code>truncate(<math>x, \{\&amp;e\}</math>)</code>
gcd/LCM of $x$ and $y$	<code>gcd(<math>x, y</math>), lcm(<math>x, y</math>)</code>
gcd of entries of a vector/matrix	<code>content(<math>x</math>)</code>
<b>Primes and Factorization</b>	
add primes in $v$ to the prime table	<code>addprimes(<math>v</math>)</code>
the $n$ th prime	<code>prime(<math>n</math>)</code>
vector of first $n$ primes	<code>primes(<math>n</math>)</code>
smallest prime $\geq x$	<code>nextprime(<math>x</math>)</code>
largest prime $\leq x$	<code>precprime(<math>x</math>)</code>
factorization of $x$	<code>factor(<math>x, \{lim\}</math>)</code>
reconstruct $x$ from its factorization	<code>factorback(<math>f, \{e\}</math>)</code>

Divisors

number of distinct prime divisors	<code>omega(<math>x</math>)</code>
number of prime divisors with mult	<code>bigomega(<math>x</math>)</code>
number of divisors of $x$	<code>numdiv(<math>x</math>)</code>
row vector of divisors of $x$	<code>divisors(<math>x</math>)</code>
sum of ( $k$ -th powers of) divisors of $x$	<code>sigma(<math>x, \{k\}</math>)</code>

Special Functions and Numbers

binomial coefficient $\binom{x}{y}$	<code>binomial(<math>x, y</math>)</code>
Bernoulli number $B_n$ as real	<code>bernreal(<math>n</math>)</code>
Bernoulli vector $B_0, B_2, \dots, B_{2n}$	<code>bernvec(<math>n</math>)</code>
$n$ th Fibonacci number	<code>fibonacci(<math>n</math>)</code>
number of partitions of $n$	<code>numbpart(<math>n</math>)</code>
Euler $\phi$ -function	<code>eulerphi(<math>x</math>)</code>
Möbius $\mu$ -function	<code>moebius(<math>x</math>)</code>
Hilbert symbol of $x$ and $y$ (at $p$ )	<code>hilbert(<math>x, y, \{p\}</math>)</code>
Kronecker-Legendre symbol $(\frac{x}{y})$	<code>kronecker(<math>x, y</math>)</code>

Miscellaneous

integer or real factorial of $x$	<code>x!</code> or <code>fact(<math>x</math>)</code>
integer square root of $x$	<code>sqrntint(<math>x</math>)</code>
solve $z \equiv x$ and $z \equiv y$	<code>chinese(<math>x, y</math>)</code>
minimal $u, v$ so $xu + yv = \gcd(x, y)$	<code>bezout(<math>x, y</math>)</code>
multiplicative order of $x$ (intmod) (i=0)	<code>znorder(<math>x, \{o\}</math>)</code>
primitive root mod prime power $q$	<code>znprimroot(<math>q</math>)</code>
structure of $(\mathbf{Z}/n\mathbf{Z})^*$	<code>znstar(<math>n</math>)</code>
continued fraction of $x$	<code>contfrac(<math>x, \{b\}, \{lmax\}</math>)</code>
last convergent of continued fraction $x$	<code>contfracpnqn(<math>x</math>)</code>
best rational approximation to $x$	<code>bestappr(<math>x, k</math>)</code>

True-False Tests

is $x$ the disc. of a quadratic field?	<code>isfundamental(<math>x</math>)</code>
is $x$ a prime?	<code>isprime(<math>x</math>)</code>
is $x$ a strong pseudo-prime?	<code>ispseudoprime(<math>x</math>)</code>
is $x$ square-free?	<code>issquarefree(<math>x</math>)</code>
is $x$ a square?	<code>issquare(<math>x, \{\&amp;n\}</math>)</code>
is $pol$ irreducible?	<code>polisirreducible(<math>pol</math>)</code>

Based on an earlier version by Joseph H. Silverman  
May 2011 v2.26. Copyright © 2011 K. Belabas  
GP copyright by The PARI Group

Permission is granted to make and distribute copies of this card provided the copyright and this permission notice are preserved on all copies.

Send comments and corrections to {Karim.Belabas@math.u-bordeaux.fr}

# PARI-GP Reference Card (2)

(PARI-GP version 2.5.0)

## Elliptic Curves

Elliptic curve initially given by 5-tuple  $E = [a_1, a_2, a_3, a_4, a_6]$ . Points are  $[x, y]$ , the origin is  $[0]$ .

Initialize elliptic struct.  $ell$ , i.e create `ellinit( $E, \{flag\}$ )`

$a_1, a_2, a_3, a_4, a_6, b_2, b_4, b_6, b_8, c_4, c_6, disc, j$ . This data can be recovered by typing `ell.a1, ..., ell.j`. If  $flag$  omitted, also

•  $E$  defined over  $\mathbf{R}$

$x$ -coords. of points of order 2	<code>ell.roots</code>
real and complex periods	<code>ell.omega</code>
associated quasi-periods	<code>ell.eta</code>
volume of complex lattice	<code>ell.area</code>

•  $E$  defined over  $\mathbf{Q}_p$ ,  $|j|_p > 1$

$x$ -coord. of unit 2 torsion point	<code>ell.roots</code>
Tate's $[u^2, u, q]$	<code>ell.tate</code>
Mestre's $w$	<code>ell.w</code>

change curve  $E$  using  $v = [u, r, s, t]$

change point  $z$  using  $v = [u, r, s, t]$

add points  $z_1 + z_2$

subtract points  $z_1 - z_2$

compute  $n \cdot z$

check if  $z$  is on  $E$

order of torsion point  $z$

$y$ -coordinates of point(s) for  $x$

point  $[\wp(z), \wp'(z)]$  corresp. to  $z$

complex  $z$  such that  $p = [\wp(z), \wp'(z)]$

**Curves over finite fields, Pairings**

random point on  $E$

structure  $\mathbf{Z}/d_1\mathbf{Z} \times \mathbf{Z}/d_2\mathbf{Z}$  of  $E(\mathbf{F}_p)$

Weil pairing of  $m$ -torsion pts  $x, y$  `ellweilpairing( $ell, x, y, m$ )`

Tate pairing of  $x, y$ ;  $x$   $m$ -torsion `elltatepairing( $ell, x, y, m$ )`

**Curves over  $\mathbf{Q}$  and the  $L$ -function**

canonical bilinear form taken at  $z_1, z_2$  `ellbil( $ell, z_1, z_2$ )`

canonical height of  $z$  `ellheight( $ell, z, \{flag\}$ )`

height regulator matrix for pts in  $x$  `ellheightmatrix( $ell, x$ )`

cond, min mod, Tamagawa num  $[N, v, c]$  `ellglobalred( $ell$ )`

Kodaira type of  $p$ -fiber of  $E$  `elllocalred( $ell, p$ )`

minimal model of  $E/\mathbf{Q}$  `ellminimalmodel( $ell, \{&v\}$ )`

$p$ th coeff  $a_p$  of  $L$ -function,  $p$  prime `ellap( $ell, p$ )`

$k$ th coeff  $a_k$  of  $L$ -function `ellak( $ell, k$ )`

vector of first  $n$   $a_k$ 's in  $L$ -function `ellan( $ell, n$ )`

$L(E, s)$ , set  $A \approx 1$  `elllseries( $ell, s, \{A\}$ )`

order of vanishing at 1 `ellanalyticrank( $ell, \{eps\}$ )`

$L^{(r)}(E, 1)$  `ellLi( $ell, r$ )`

root number for  $L(E, \cdot)$  at  $p$  `ellrootno( $ell, \{p\}$ )`

torsion subgroup with generators `elltors( $ell$ )`

modular parametrization of  $E$  `elltaniyama( $ell$ )`

**Elldata package, Cremona's database:**

db code  $\leftrightarrow$   $[conductor, class, index]$  `ellconvertname( $s$ )`

generators of Mordell-Weil group `ellgenerators( $E$ )`

look up  $E$  in database `ellidentify( $E$ )`

all curves matching criterion `ellsearch( $N$ )`

loop over curves with cond. from  $a$  to  $b$  `forell( $E, a, b, seq$ )`

## Elliptic & Modular Functions

arithmetic-geometric mean

elliptic  $j$ -function  $1/q + 744 + \dots$

Weierstrass  $\sigma$  function

Weierstrass  $\wp$  function

Weierstrass  $\zeta$  function

modified Dedekind  $\eta$  func.  $\prod(1 - q^n)$

Jacobi sine theta function

$k$ -th derivative at  $z=0$  of  $\theta(q, z)$

Weber's  $f$  functions

Riemann's zeta  $\zeta(s) = \sum n^{-s}$

`agm( $x, y$ )`

`ellj( $x$ )`

`ellsigma( $ell, z, \{flag\}$ )`

`ellwp( $ell, \{z\}, \{flag\}$ )`

`ellzeta( $ell, z$ )`

`eta( $x, \{flag\}$ )`

`theta( $q, z$ )`

`thetanulk( $q, k$ )`

`weber( $x, \{flag\}$ )`

`zeta( $s$ )`

## Graphic Functions

crude graph of  $expr$  between  $a$  and  $b$  `plot( $X = a, b, expr$ )`

**High-resolution plot** (immediate plot)

plot  $expr$  between  $a$  and  $b$  `ploto( $X = a, b, expr, \{flag\}, \{n\}$ )`

plot points given by lists  $lx, ly$  `plotdraw( $lx, ly, \{flag\}$ )`

terminal dimensions

`plotsizes()`

**Rectwindow functions**

init window  $w$ , with size  $x, y$

`plotinit( $w, x, y$ )`

erase window  $w$

`plotkill( $w$ )`

copy  $w$  to  $w_2$  with offset  $(dx, dy)$

`plotcopy( $w, w_2, dx, dy$ )`

scale coordinates in  $w$

`plotscale( $w, x_1, x_2, y_1, y_2$ )`

ploto in  $w$  `plotrecth( $w, X = a, b, expr, \{flag\}, \{n\}$ )`

plotdraw in  $w$  `plotrecthdraw( $w, data, \{flag\}$ )`

draw window  $w_1$  at  $(x_1, y_1), \dots$  `plotdraw( $[[w_1, x_1, y_1], \dots]$ )`

**Low-level Rectwindow Functions**

set current drawing color in  $w$  to  $c$

`plotcolor( $w, c$ )`

current position of cursor in  $w$

`plotcursor( $w$ )`

write  $s$  at cursor's position

`plotstring( $w, s$ )`

move cursor to  $(x, y)$

`plotmove( $w, x, y$ )`

move cursor to  $(x + dx, y + dy)$

`plotrmove( $w, dx, dy$ )`

draw a box to  $(x_2, y_2)$

`plotbox( $w, x_2, y_2$ )`

draw a box to  $(x + dx, y + dy)$

`plotrbox( $w, dx, dy$ )`

draw polygon

`plotlines( $w, lx, ly, \{flag\}$ )`

draw points

`plotpoints( $w, lx, ly$ )`

draw line to  $(x + dx, y + dy)$

`plotrline( $w, dx, dy$ )`

draw point  $(x + dx, y + dy)$

`plotrpoint( $w, dx, dy$ )`

**Postscript Functions**

as ploto `psploto( $X = a, b, expr, \{flag\}, \{n\}$ )`

as plotdraw `psplotdraw( $lx, ly, \{flag\}$ )`

as plotdraw `psdraw( $[[w_1, x_1, y_1], \dots]$ )`

## Binary Quadratic Forms

create  $ax^2 + bxy + cy^2$  (distance  $d$ )

`qfb( $a, b, c, \{d\}$ )`

reduce  $x$  ( $s = \sqrt{D}$ ,  $l = \lfloor s \rfloor$ )

`qfbred( $x, \{flag\}, \{D\}, \{l\}, \{s\}$ )`

composition of forms

$x*y$  or `qfbnucomp( $x, y, l$ )`

$n$ -th power of form

$x^n$  or `qfbnpow( $x, n$ )`

composition without reduction

`qfbcomprow( $x, y$ )`

$n$ -th power without reduction

`qfbpowrow( $x, n$ )`

prime form of disc.  $x$  above prime  $p$

`qfbprimeform( $x, p$ )`

class number of disc.  $x$

`qfbclassno( $x$ )`

Hurwitz class number of disc.  $x$

`qfbhclassno( $x$ )`

## Quadratic Fields

quadratic number  $\omega = \sqrt{x}$  or  $(1 + \sqrt{x})/2$

`quadgen( $x$ )`

minimal polynomial of  $\omega$

`quadpoly( $x$ )`

discriminant of  $\mathbf{Q}(\sqrt{D})$

`quaddisc( $x$ )`

regulator of real quadratic field

`quadregulator( $x$ )`

fundamental unit in real  $\mathbf{Q}(x)$

`quadunit( $x$ )`

class group of  $\mathbf{Q}(\sqrt{D})$

`quadclassunit( $D, \{flag\}, \{t\}$ )`

Hilbert class field of  $\mathbf{Q}(\sqrt{D})$

`quadhilbert( $D, \{flag\}$ )`

ray class field modulo  $f$  of  $\mathbf{Q}(\sqrt{D})$

`quadray( $D, f, \{flag\}$ )`

## General Number Fields: Initializations

A number field  $K$  is given by a monic irreducible  $f \in \mathbf{Z}[X]$ .

init number field structure  $nf$

`nfinit( $f, \{flag\}$ )`

**nf members:**

polynomial defining  $nf$ ,  $f(\theta) = 0$

`nf.pol`

number of real/complex places

`nf.r1/r2/sign`

discriminant of  $nf$

`nf.disc`

$T_2$  matrix

`nf.t2`

vector of roots of  $f$

`nf.roots`

integral basis of  $\mathbf{Z}_K$  as powers of  $\theta$

`nf.zk`

different

`nf.diff`

codifferent

`nf.codiff`

index

`nf.index`

recompute  $nf$  using current precision

`nfnewprec( $nf$ )`

init relative  $rnf$  given by  $g = 0$  over  $K$

`rnfinit( $nf, g$ )`

init  $bnf$  structure

`bnfinit( $f, \{flag\}$ )`

**bnf members:** same as  $nf$ , plus

underlying  $nf$

`bnf.nf`

classgroup

`bnf.clgp`

regulator

`bnf.reg`

fundamental units

`bnf.fu`

torsion units

`bnf.tu`

compute a  $bnf$  from small  $bnf$

`bnfinit( $sbnf$ )`

add  $S$ -class group and units, yield  $bnf$  s

`bnfsunit( $nf, S$ )`

init class field structure  $bnr$

`bnrinit( $bnf, m, \{flag\}$ )`

**bnr members:** same as  $bnf$ , plus

underlying  $bnf$

`bnr.bnf`

big ideal structure

`bnr.bid`

modulus

`bnr.mod`

structure of  $(\mathbf{Z}_K/m)^*$

`bnr.zkst`

## Basic Number Field Arithmetic (nf)

Elements are `t_INT`, `t_FRAC`, `t_POL`, `t_POLMOD`, or `t_COL` (on integral basis `nf.zk`). Basic operations (prefix `nfelt`): `(nfelt)add`, `mul`, `pow`, `div`, `diveuc`, `mod`, `divrem`, `val`, `trace`, `norm`  
express  $x$  on integer basis `nfalgtobasis(nf, x)`  
express element  $x$  as a polmod `nfbasistoalg(nf, x)`  
reverse polmod  $a = A(X) \bmod T(X)$  `modreverse(a)`  
integral basis of field def. by  $f = 0$  `nfbasis(f)`  
field discriminant of field  $f = 0$  `nfdisc(f)`  
Galois group of field  $f = 0$ ,  $\deg f \leq 11$  `polgalois(f)`  
smallest poly defining  $f = 0$  `polredabs(f, {flag})`  
small polys defining subfields of  $f = 0$  `polred(f, {flag}, {p})`  
poly of degree  $\leq k$  with root  $x \in \mathbf{C}$  `algdep(x, k)`  
small linear rel. on coords of vector  $x$  `lindep(x)`  
are fields  $f = 0$  and  $g = 0$  isomorphic? `nfisism(f, g)`  
is field  $f = 0$  a subfield of  $g = 0$ ? `nfisincl(f, g)`  
compositum of  $f = 0$ ,  $g = 0$  `polcompositum(f, g, {flag})`  
subfields (of degree  $d$ ) of  $nf$  `nfsubfields(nf, {d})`  
roots of unity in  $nf$  `nfrootsof1(nf)`  
roots of  $g$  belonging to  $nf$  `nfroots({nf}, g)`  
factor  $g$  in  $nf$  `nfactor(nf, g)`  
factor  $g$  mod prime  $pr$  in  $nf$  `nfactormod(nf, g, pr)`  
conjugates of a root  $\theta$  of  $nf$  `nfgaloisconj(nf, {flag})`  
apply Galois automorphism  $s$  to  $x$  `nfgaloisapply(nf, s, x)`  
quadratic Hilbert symbol (at  $p$ ) `nfhilbert(nf, a, b, {p})`  
**Dedekind Zeta Function**  $\zeta_K$   
 $\zeta_K$  as Dirichlet series,  $N(I) < b$  `dirzetak(nf, b)`  
init  $nfz$  for field  $f = 0$  `zetakinit(f)`  
compute  $\zeta_K(s)$  `zetak(nfz, s, {flag})`  
Artin root number of  $K$  `bnrrootnumber(bnr, chi, {flag})`

## Class Groups & Units (bnf, bnr)

$a_1, \{a_2\}, \{a_3\}$  usually  $bnr$ ,  $subgp$  or  $bnf$ ,  $module$ ,  $\{subgp\}$   
remove GRH assumption from  $bnf$  `bnfcertify(bnf)`  
expo. of ideal  $x$  on class gp `bnfisprincipal(bnf, x, {flag})`  
expo. of ideal  $x$  on ray class gp `bnrisprincipal(bnr, x, {flag})`  
expo. of  $x$  on fund. units `bnfisunit(bnf, x)`  
as above for  $S$ -units `bnfissunit(bnfs, x)`  
signs of real embeddings of  $bnf$ .fu `bnfsignunit(bnf)`

### Class Field Theory

ray class number for mod.  $m$  `bnrclassno(bnf, m)`  
discriminant of class field ext `bnrdisc(a1, {a2}, {a3})`  
ray class numbers,  $l$  list of mods `bnrclassnolist(bnf, l)`  
discriminants of class fields `bnrdisclist(bnf, l, {arch}, {flag})`  
decode output from `bnrdisclist` `bnfdecodemodule(nf, fa)`  
is modulus the conductor? `bnrisconductor(a1, {a2}, {a3})`  
conductor of character  $chi$  `bnrconductorofchar(bnr, chi)`  
conductor of extension `bnrconductor(a1, {a2}, {a3}, {flag})`  
conductor of extension def. by  $g$  `rnfconductor(bnf, g)`  
Artin group of ext. def'd by  $g$  `rnfnormgroup(bnr, g)`  
subgroups of  $bnr$ , index  $\leq b$  `subgrouplist(bnr, b, {flag})`  
rel. eq. for class field def'd by  $sub$  `rnfkummer(bnr, sub, {d})`  
same, using Stark units (real field) `bnrstark(bnr, sub, {flag})`

## PARI-GP Reference Card (2)

(PARI-GP version 2.5.0)

### Ideals

Ideals are elements, primes, or matrix of generators in HNF.  
is  $id$  an ideal in  $nf$  ? `nfisideal(nf, id)`  
is  $x$  principal in  $bnf$  ? `bnfisprincipal(bnf, x)`  
principal ideal generated by  $x$  `idealprincipal(nf, x)`  
principal idele generated by  $x$  `ideleprincipal(nf, x)`  
give  $[a, b]$ , s.t.  $a\mathbf{Z}_K + b\mathbf{Z}_K = x$  `idealtwoelt(nf, x, {a})`  
put ideal  $a$  ( $a\mathbf{Z}_K + b\mathbf{Z}_K$ ) in HNF form `idealhnf(nf, a, {b})`  
norm of ideal  $x$  `idealnrm(nf, x)`  
minimum of ideal  $x$  (direction  $v$ ) `idealmin(nf, x, v)`  
LLL-reduce the ideal  $x$  (direction  $v$ ) `idealred(nf, x, {v})`

### Ideal Operations

add ideals  $x$  and  $y$  `idealadd(nf, x, y)`  
multiply ideals  $x$  and  $y$  `idealmul(nf, x, y, {flag})`  
intersection of ideals  $x$  and  $y$  `idealintersect(nf, x, y, {flag})`  
 $n$ -th power of ideal  $x$  `idealpow(nf, x, n, {flag})`  
inverse of ideal  $x$  `idealinv(nf, x)`  
divide ideal  $x$  by  $y$  `idealdiv(nf, x, y, {flag})`  
Find  $(a, b) \in x \times y$ ,  $a + b = 1$  `idealaddtoone(nf, x, {y})`

### Primes and Multiplicative Structure

factor ideal  $x$  in  $nf$  `idealfactor(nf, x)`  
expand ideal factorization in  $nf$  `idealfactorback(nf, f, e)`  
decomposition of prime  $p$  in  $nf$  `idealprimedec(nf, p)`  
valuation of  $x$  at prime ideal  $pr$  `idealval(nf, x, pr)`  
weak approximation theorem in  $nf$  `idealchinese(nf, x, y)`  
give  $bid$  = structure of  $(\mathbf{Z}_K/id)^*$  `idealstar(nf, id, {flag})`  
discrete log of  $x$  in  $(\mathbf{Z}_K/bid)^*$  `ideallog(nf, x, bid)`  
idealstar of all ideals of norm  $\leq b$  `ideallist(nf, b, {flag})`  
add Archimedean places `ideallistarch(nf, b, {ar}, {flag})`  
init `prmod` structure `nfmodprinit(nf, pr)`  
kernel of matrix  $M$  in  $(\mathbf{Z}_K/pr)^*$  `nfkermodpr(nf, M, prmod)`  
solve  $Mx = B$  in  $(\mathbf{Z}_K/pr)^*$  `nfsolvemodpr(nf, M, B, prmod)`

## Galois theory over $\mathbf{q}$

initializes a Galois group structure `galoisinit(pol, {den})`  
action of  $p$  in `nfgaloisconj` form `galoispermopol(G, {p})`  
identifies as abstract group `galoisidentify(G)`  
exports a group for GAP or MAGMA `galoisexport(G, {flag})`  
subgroups of the Galois group  $G$  `galoissubgroups(G)`  
subfields from subgroups of  $G$  `galoissubfields(G, {flag}, {v})`  
fixed field `galoisfixedfield(G, perm, {flag}, {v})`  
is  $G$  abelian? `galoisisabelian(G, {flag})`  
abelian number fields `galoissubcyclo(N, H, {flag}, {v})`

## Relative Number Fields (rnf)

Extension  $L/K$  is defined by  $g \in K[x]$ . We have  $order \subset L$ .  
absolute equation of  $L$  `rnfequation(nf, g, {flag})`  
relative `nfalgtobasis` `rnfalgtobasis(rnf, x)`  
relative `nfbasistoalg` `rnfbasistoalg(rnf, x)`  
relative `idealhnf` `rnfidealhnf(rnf, x)`  
relative `idealmul` `rnfidealmul(rnf, x, y)`  
relative `idealtwoelt` `rnfidealtwoelt(rnf, x)`

### Lifts and Push-downs

absolute  $\rightarrow$  relative repres. for  $x$  `rnfeltabstorel(rnf, x)`  
relative  $\rightarrow$  absolute repres. for  $x$  `rnfeltreltoabs(rnf, x)`  
lift  $x$  to the relative field `rnfeltup(rnf, x)`  
push  $x$  down to the base field `rnfeltdown(rnf, x)`  
idem for  $x$  ideal: `(rnfideal)reltoabs, astorel, up, down`

### Projective $\mathbf{Z}_K$ -modules, maximal order

relative `polred` `rnfpolred(nf, g)`  
relative `polredabs` `rnfpolredabs(nf, g)`  
characteristic poly. of  $a \bmod g$  `rnfcharpoly(nf, g, a, {v})`  
relative Dedekind criterion, prime  $pr$  `rnfdedekind(nf, g, pr)`  
discriminant of relative extension `rnfdisc(nf, g)`  
pseudo-basis of  $\mathbf{Z}_L$  `rnfpseudobasis(nf, g)`  
relative HNF basis of  $order$  `rnfhnfbasis(bnf, order)`  
reduced basis for  $order$  `rnflllgram(nf, g, order)`  
determinant of pseudo-matrix  $A$  `rnfdet(nf, A)`  
Steinitz class of  $order$  `rnfstesinitz(nf, order)`  
is  $order$  a free  $\mathbf{Z}_K$ -module? `rnfisfree(bnf, order)`  
true basis of  $order$ , if it is free `rnfbasis(bnf, order)`

### Norms

absolute norm of ideal  $x$  `rnfidealnrmabs(rnf, x)`  
relative norm of ideal  $x$  `rnfidealnrmrel(rnf, x)`  
solutions of  $N_K/\mathbf{Q}(y) = x \in \mathbf{Z}$  `bnfisintnorm(bnf, x)`  
is  $x \in \mathbf{Q}$  a norm from  $K$ ? `bnfisnorm(bnf, x, {flag})`  
initialize  $T$  for norm eq. solver `rnfisnorminit(K, pol, {flag})`  
is  $a \in K$  a norm from  $L$ ? `rnfisnorm(T, a, {flag})`

Based on an earlier version by Joseph H. Silverman  
May 2011 v2.26. Copyright © 2011 K. Belabas  
GP copyright by The PARI Group

Permission is granted to make and distribute copies of this card provided the copyright and this permission notice are preserved on all copies.

Send comments and corrections to (Karim.Belabas@math.u-bordeaux.fr)