

# Pari-GP reference card

(PARI-GP version 2.11.0)

Note: optional arguments are surrounded by braces {}.

To start the calculator, type its name in the terminal: **gp**

To exit **gp**, type **quit**, **\q**, or **<C-D>** at prompt.

## Help

describe function	?function
extended description	??keyword
list of relevant help topics	???pattern
name of GP-1.39 function $f$ in GP-2.*	whatnow( $f$ )

## Input/Output

previous result, the result before	%, %', %'', etc.
$n$ -th result since startup	% $n$
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	\\ ...

## Metacommands & Defaults

set default $d$ to $val$	default({ $d$ },{ $val$ })
toggle timer on/off	#
print time for last result	##
print defaults	\d
set debug level to $n$	\g $n$
set memory debug level to $n$	\gm $n$
set $n$ significant digits / bits	\p $n$ , \pb $n$
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 <i>filename</i>

## Debugger / break loop

get out of break loop	break or <C-D>
go up/down $n$ frames	dbg_up({ $n$ }), dbg_down
set break point	breakpoint()
examine object $o$	dbg_x( $o$ )
current error data	dbg_err()
number of objects on heap and their size	getheap()
total size of objects on PARI stack	getstack()

## PARI Types & Input Formats

<b>t_INT</b> . Integers; hex, binary	$\pm 31$ ; $\pm 0x1F$ , $\pm 0b101$
<b>t_REAL</b> . Reals	$\pm 3.14$ , 6.022 E23
<b>t_INTMOD</b> . Integers modulo $m$	Mod( $n$ , $m$ )
<b>t_FRAC</b> . Rational Numbers	$n/m$
<b>t_FFELT</b> . Elt in finite field $\mathbf{F}_q$	ffgen( $q$ , 't)
<b>t_COMPLEX</b> . Complex Numbers	$x + y * I$
<b>t_PADIC</b> . $p$ -adic Numbers	$x + O(p^k)$
<b>t_QUAD</b> . Quadratic Numbers	$x + y * \text{quadgen}(D, 'w)$
<b>t_POLMOD</b> . Polynomials modulo $g$	Mod( $f$ , $g$ )
<b>t_POL</b> . Polynomials	$a * x^n + \dots + b$
<b>t_SER</b> . Power Series	$f + O(x^k)$
<b>t_RFRAC</b> . Rational Functions	$f/g$
<b>t_QFI</b> / <b>t_QFR</b> . Imag/Real binary quad. form	Qfb( $a, b, c, \{d\}$ )
<b>t_VEC</b> / <b>t_COL</b> . Row/Column Vectors	$[x, y, z]$ , $[x, y, z] \sim$
<b>t_VEC</b> integer range	$[1..10]$

<b>t_VECSMALL</b> . Vector of small ints	Vecsmall( $[x, y, z]$ )
<b>t_MAT</b> . Matrices	$[a, b; c, d]$
<b>t_LIST</b> . Lists	List( $[x, y, z]$ )
<b>t_STR</b> . Strings	"abc"
<b>t_INFINITY</b> . $\pm\infty$	+oo, -oo

## Reserved Variable Names

$\pi = 3.14\dots$ , $\gamma = 0.57\dots$ , $C = 0.91\dots$	Pi, Euler, Catalan
square root of $-1$	I
Landau's big-oh notation	O

## Information about an Object

PARI type of object $x$	type( $x$ )
length of $x$ / size of $x$ in memory	# $x$ , sizebyte( $x$ )
real precision / bit precision of $x$	precision( $x$ ), bitprecision
$p$ -adic, series prec. of $x$	padicprec( $x$ ), serprec

## Operators

basic operations	+, -, *, /, ^, sqr
$i=i+1$ , $i=i-1$ , $i=i*j$ , ...	i++, i--, i*=j,...
euclidean quotient, remainder	$x \backslash y$ , $x \backslash y$ , $x \backslash y$ , divrem( $x, y$ )
shift $x$ left or right $n$ bits	$x << n$ , $x >> n$ or shift( $x, \pm n$ )
multiply by $2^n$	shiftmul( $x, n$ )
comparison operators	<=, <, >=, >, ==, !=, ==, lex, cmp
boolean operators (or, and, not)	, &&, !
bit operations	bitand, bitneg, bitor, bitxor, bitneginv
maximum/minimum of $x$ and $y$	max, min( $x, y$ )
sign of $x = -1, 0, 1$	sign( $x$ )
binary exponent of $x$	exponent( $x$ )
derivative of $f$	$f'$
differential operator	diffop( $f, v, d, \{n = 1\}$ )
quote operator (formal variable)	'x
assignment	x = <i>value</i>
simultaneous assignment $x \leftarrow v_1, y \leftarrow v_2$	[x,y] = v

## Select Components

$n$ -th component of $x$	component( $x, n$ )
$n$ -th component of vector/list $x$	$x[n]$
components $a, a + 1, \dots, b$ of vector $x$	$x[a..b]$
$(m, n)$ -th component of matrix $x$	$x[m, n]$
row $m$ or column $n$ of matrix $x$	$x[m, ]$ , $x[, n]$
numerator/denominator of $x$	numerator( $x$ ), denominator

## Random Numbers

random integer/prime in $[0, N[$	random( $N$ ), randomprime
get/set random seed	getrand, setrand( $s$ )

## Conversions

to vector, matrix, vec. of small ints	Col/Vec, Mat, Vecsmall
to list, set, map, string	List, Set, Map, Str
create PARI object ( $x \bmod y$ )	Mod( $x, y$ )
make $x$ a polynomial of $v$	Pol( $x, \{v\}$ )
as Pol, etc., starting with constant term	Polrev, Vecrev, Colrev
make $x$ a power series of $v$	Ser( $x, \{v\}$ )
string from bytes / from format+args	Strchr, Strprintf
TeX string	Strtex( $x$ )
convert $x$ to simplest possible type	simplify( $x$ )
object $x$ with real precision $n$	precision( $x, n$ )
object $x$ with bit precision $n$	bitprecision( $x, n$ )
set precision to $p$ digits in dynamic scope	localprec( $p$ )
set precision to $p$ bits in dynamic scope	localbitprec( $p$ )

## Conjugates and Lifts

conjugate of a number $x$	conj( $x$ )
norm of $x$ , product with conjugate	norm( $x$ )
$L^p$ norm of $x$ ( $L^\infty$ if no $p$ )	normlp( $x, \{p\}$ )
square of $L^2$ norm of $x$	norml2( $x$ )
lift of $x$ from Mods and $p$ -adics	lift, centerlift( $x$ )
recursive lift	liftall
lift all <b>t_INT</b> and <b>t_PADIC</b> ( $\rightarrow$ <b>t_INT</b> )	liftint
lift all <b>t_POLMOD</b> ( $\rightarrow$ <b>t_POL</b> )	lifttpol

## Lists, Sets & Maps

**Sets** (= row vector with strictly increasing entries w.r.t. **cmp**)

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( $x, y$ )
does $y$ belong to the set $x$	setsearch( $x, y, \{flag\}$ )
set of all $f(x, y)$ , $x \in X$ , $y \in Y$	setbinop( $f, X, Y$ )
is $x$ a set ?	setisset( $x$ )

**Lists**. create empty list:  $L = \text{List}()$

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( $L, \{flag\}$ )

**Maps**. create empty dictionary:  $M = \text{Map}()$

attach value $v$ to key $k$	mapput( $M, k, v$ )
recover value attach to key $k$ or error	mapget( $M, k$ )
is key $k$ in the dict ? (set $v$ to $M(k)$ )	mapisdefined( $M, k, \{\&v\}$ )
remove $k$ from map domain	mapdelete( $M, k$ )

## GP Programming

### User functions and closures

$x, y$  are formal parameters;  $y$  defaults to Pi if parameter omitted;  
 $z, t$  are local variables (lexical scope),  $z$  initialized to 1.

```
fun(x, y=Pi) = my(z=1, t); seq
fun = (x, y=Pi) -> my(z=1, t); seq
```

attach a help message to $f$	addhelp( $f$ )
undefine symbol $s$ (also kills help)	kill( $s$ )
<b>Control Statements</b> ( $X$ : formal parameter in expression $seq$ )	
if $a \neq 0$ , evaluate $seq_1$ , else $seq_2$	if( $a, \{seq_1\}, \{seq_2\}$ )

eval. $seq$ for $a \leq X \leq b$	for( $X = a, b, seq$ )
...for primes $a \leq X \leq b$	forprime( $X = a, b, seq$ )
...for primes $\equiv a \pmod q$	forprimestep( $X = a, b, q, seq$ )
...for composites $a \leq X \leq b$	forcomposite( $X = a, b, seq$ )
...for $a \leq X \leq b$ stepping $s$	forstep( $X = a, b, s, seq$ )
...for $X$ dividing $n$	fordiv( $n, X, seq$ )
... $X = [n, factor(n)]$ , $a \leq n \leq b$	forfactored( $X = a, b, seq$ )
...as above, $n$ squarefree	forsquarefree( $X = a, b, seq$ )
... $X = [d, factor(d)]$ , $d \mid n$	fordivfactored( $n, X, seq$ )
multivariable <b>for</b> , lex ordering	forvec( $X = v, seq$ )
loop over partitions of $n$	forpart( $p = n, seq$ )
...permutations of $S$	forperm( $S, p, seq$ )
...subsets of $\{1, \dots, n\}$	forsubset( $n, p, seq$ )
... $k$ -subsets of $\{1, \dots, n\}$	forsubset( $[n, k], p, seq$ )
...vectors $v$ , $q(v) \leq B$ ; $q > 0$	forqfvec( $v, q, b, seq$ )
... $H < G$ finite abelian group	forsubgroup( $H = G$ )

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({ $x$ })

Exceptions, warnings

raise an exception / warn	<code>error()</code> , <code>warning()</code>
type of error message $E$	<code>errname(E)</code>
try $seq_1$ , evaluate $seq_2$ on error	<code>iferr(seq_1, E, seq_2)</code>
<b>Functions with closure arguments / results</b>	
select from $v$ according to $f$	<code>select(f, v)</code>
apply $f$ to all entries in $v$	<code>apply(f, v)</code>
evaluate $f(a_1, \dots, a_n)$	<code>call(f, a)</code>
evaluate $f(\dots f(f(a_1, a_2), a_3) \dots, a_n)$	<code>fold(f, a)</code>
calling function as closure	<code>self()</code>

Sums & Products

sum $X = a$ to $X = b$ , initialized at $x$	<code>sum(X = a, b, expr, {x})</code>
sum entries of vector $v$	<code>vecsum(v)</code>
product of all vector entries	<code>vecprod(v)</code>
sum $expr$ over divisors of $n$	<code>sumdiv(n, X, expr)</code>
... assuming $expr$ multiplicative	<code>sumdivmult(n, X, expr)</code>
product $a \leq X \leq b$ , initialized at $x$	<code>prod(X = a, b, expr, {x})</code>
product over primes $a \leq X \leq b$	<code>prodeuler(X = a, b, expr)</code>

Sorting

sort $x$ by $k$ -th component	<code>vecsrt(x, {k}, {fl = 0})</code>
min. $m$ of $x$ ( $m = x[i]$ ), max.	<code>vecmin(x, {&amp;i}), vecmax</code>
does $y$ belong to $x$ , sorted wrt. $f$	<code>vecsearch(x, y, {f})</code>

Input/Output

print with/without $\backslash n$ , $\text{\TeX}$ format	<code>print</code> , <code>printl</code> , <code>printtex</code>
pretty print matrix	<code>printp</code>
print fields with separator	<code>printsep(sep, ...)</code> , <code>printsep1</code>
formatted printing	<code>printf()</code>
write $args$ to file	<code>write</code> , <code>writel</code> , <code>writetex(file, args)</code>
write $x$ in binary format	<code>writebin(file, x)</code>
read file into GP	<code>read({file})</code>
... return as vector of lines	<code>readvec({file})</code>
... return as vector of strings	<code>readstr({file})</code>
read a string from keyboard	<code>input()</code>

Files and file descriptors

File descriptors allows efficient small consecutive reads or writes from or to a given file. The argument  $n$  below is always a descriptor, attached to a file in `r`(ead), `w`(rite) or `a`(ppend) mode.

get descriptor $n$ for file $path$ in given $mode$	<code>fileopen(path, mode)</code>
... from shell $cmd$ output (pipe)	<code>fileextern(cmd)</code>
close descriptor	<code>fileclose(n)</code>
commit pending write operations	<code>fileflush(n)</code>
read logical line from file	<code>fileread(n)</code>
... raw line from file	<code>filereadstr(n)</code>
write $s \backslash n$ to file	<code>filewrite(n, s)</code>
... write $s$ to file	<code>filewritel(n, s)</code>

Timers

CPU time in $ms$ and reset timer	<code>gettime()</code>
CPU time in $ms$ since gp startup	<code>getabstime()</code>
time in $ms$ since UNIX Epoch	<code>getwalltime()</code>
timeout command after $s$ seconds	<code>alarm(s, expr)</code>

Interface with system

allocates a new stack of $s$ bytes	<code>allocatemem({s})</code>
alias $old$ to $new$	<code>alias(new, old)</code>
install function from library	<code>install(f, code, {gpf}, {lib})</code>
execute system command $a$	<code>system(a)</code>
... and feed result to GP	<code>extern(a)</code>
... returning GP string	<code>externstr(a)</code>

Pari-GP reference card

(PARI-GP version 2.11.0)

get $\$VAR$ from environment	<code>getenv("VAR")</code>
expand env. variable in string	<code>Strexpend(x)</code>

Parallel evaluation

These functions evaluate their arguments in parallel (pthreads or MPI); args. must not access global variables and must be free of side effects. Enabled if threading engine is not *single* in gp header.

evaluate $f$ on $x[1], \dots, x[n]$	<code>parapply(f, x)</code>
evaluate closures $f[1], \dots, f[n]$	<code>pareval(f)</code>
as <code>select</code>	<code>parselect(f, A, {flag})</code>
as <code>sum</code>	<code>parsum(i = a, b, expr, {x})</code>
as <code>vector</code>	<code>parvector(n, i, {expr})</code>
eval $f$ for $i = a, \dots, b$	<code>parfor(i = a, {b}, f, {r}, {f2})</code>
... for $p$ prime in $[a, b]$	<code>parforprime(p = a, {b}, f, {r}, {f2})</code>
... multivariate	<code>parforvec(X = v, f, {r}, {f2}, {flag})</code>
declare $x$ as inline (allows to use as global)	<code>inline(x)</code>
stop inlining	<code>uninline()</code>

Linear Algebra

dimensions of matrix $x$	<code>matsize(x)</code>
multiply two matrices	$x * y$
... assuming result is diagonal	<code>matmultodiagonal(x, y)</code>
concatenation of $x$ and $y$	<code>concat(x, {y})</code>
extract components of $x$	<code>vecextract(x, y, {z})</code>
transpose of vector or matrix $x$	<code>mattranspose(x)</code> or $x \sim$
adjoint of the matrix $x$	<code>matadjoint(x)</code>
eigenvectors/values of matrix $x$	<code>mateigen(x)</code>
characteristic/minimal polynomial of $x$	<code>charpoly(x)</code> , <code>minpoly</code>
trace/determinant of matrix $x$	<code>trace(x)</code> , <code>matdet</code>
permanent of matrix $x$	<code>matpermanent(x)</code>
Frobenius form of $x$	<code>matfrobenius(x)</code>
QR decomposition	<code>matqr(x)</code>
apply <code>matqr</code> 's transform to $v$	<code>mathouseholder(Q, v)</code>

Constructors & Special Matrices

$\{g(x): x \in v \text{ s.t. } f(x)\}$	<code>[g(x)   x &lt;- v, f(x)]</code>
$\{x: x \in v \text{ s.t. } f(x)\}$	<code>[x   x &lt;- v, f(x)]</code>
$\{g(x): x \in v\}$	<code>[g(x)   x &lt;- v]</code>
row vec. of $expr$ eval'ed at $1 \leq i \leq n$	<code>vector(n, {i}, {expr})</code>
col. vec. of $expr$ eval'ed at $1 \leq i \leq n$	<code>vectorv(n, {i}, {expr})</code>
vector of small ints	<code>vectorsmall(n, {i}, {expr})</code>
$[c, c \cdot x, \dots, c \cdot x^n]$	<code>powers(x, n, {c = 1})</code>
matrix $1 \leq i \leq m, 1 \leq j \leq n$	<code>matrix(m, n, {i}, {j}, {expr})</code>
define matrix by blocks	<code>matconcat(B)</code>
diagonal matrix with diagonal $x$	<code>matdiagonal(x)</code>
is $x$ diagonal?	<code>matisdiagonal(x)</code>
$x \cdot \text{matdiagonal}(d)$	<code>matmuldiagonal(x, d)</code>
$n \times n$ identity matrix	<code>matid(n)</code>
Hessenberg form of square matrix $x$	<code>mathess(x)</code>
$n \times n$ Hilbert matrix $H_{ij} = (i + j - 1)^{-1}$	<code>mathilbert(n)</code>
$n \times n$ Pascal triangle	<code>matpascal(n - 1)</code>
companion matrix to polynomial $x$	<code>matcompanion(x)</code>
Sylvester matrix of $x$	<code>polsylvestermatrix(x)</code>

Gaussian elimination

kernel of matrix $x$	<code>matker(x, {flag})</code>
intersection of column spaces of $x$ and $y$	<code>matintersect(x, y)</code>
solve $MX = B$ ( $M$ invertible)	<code>matsolve(M, B)</code>
one sol of $M * X = B$	<code>matinverseimage(M, B)</code>
basis for image of matrix $x$	<code>matimage(x)</code>
columns of $x$ <i>not</i> in <code>matimage</code>	<code>matimagecompl(x)</code>
supplement columns of $x$ to get basis	<code>mat supplement(x)</code>
rows, cols to extract invertible matrix	<code>matindexrank(x)</code>
rank of the matrix $x$	<code>matrank(x)</code>
solve $MX = B \bmod D$	<code>matsolvemod(M, D, B)</code>
image mod $D$	<code>matimagemod(M, D)</code>
kernel mod $D$	<code>matkermod(M, D)</code>
inverse mod $D$	<code>matinvmod(M, D)</code>
determinant mod $D$	<code>matdetmod(M, D)</code>

Lattices & Quadratic Forms

Quadratic forms

evaluate ${}^t x Q y$	<code>qfeval({Q = id}, x, y)</code>
evaluate ${}^t x Q x$	<code>qfeval({Q = id}, x)</code>
signature of quad form ${}^t y * x * y$	<code>qfsign(x)</code>
decomp into squares of ${}^t y * x * y$	<code>qfgaussred(x)</code>
eigenvalues/vectors for real symmetric $x$	<code>qfjacobi(x)</code>

HNF and SNF

upper triangular Hermite Normal Form	<code>mathnf(x)</code>
HNF of $x$ where $d$ is a multiple of $\det(x)$	<code>mathnfmod(x, d)</code>
multiple of $\det(x)$	<code>matdetint(x)</code>
HNF of $(x \mid \text{diagonal}(D))$	<code>mathnfmodid(x, D)</code>
elementary divisors of $x$	<code>matsnf(x)</code>
elementary divisors of $\mathbf{Z}[a]/(f'(a))$	<code>poldiscreduced(f)</code>
integer kernel of $x$	<code>matkerint(x)</code>
$\mathbf{Z}$ -module $\leftrightarrow \mathbf{Q}$ -vector space	<code>matrixqz(x, p)</code>

Lattices

LLL-algorithm applied to columns of $x$	<code>qflll(x, {flag})</code>
... for Gram matrix of lattice	<code>qflllgram(x, {flag})</code>
find up to $m$ sols of $\text{qfnorm}(x, y) \leq b$	<code>qfminim(x, b, m)</code>
$v, v[i] :=$ number of $y$ s.t. $\text{qfnorm}(x, y) = i$	<code>qfrep(x, B, {flag})</code>
perfection rank of $x$	<code>qfperfection(x)</code>
find isomorphism between $q$ and $Q$	<code>qfisom(q, Q)</code>
precompute for isomorphism test with $q$	<code>qfisominit(q)</code>
automorphism group of $q$	<code>qfauto(q)</code>
convert <code>qfauto</code> for GAP/Magma	<code>qfautoexport(G, {flag})</code>
orbits of $V$ under $G \subset \text{GL}(V)$	<code>qforbits(G, V)</code>

Polynomials & Rational Functions

all defined polynomial variables	<code>variables()</code>
get var. of highest priority (higher than $v$ )	<code>varhigher(name, {v})</code>
... of lowest priority (lower than $v$ )	<code>varlower(name, {v})</code>

Based on an earlier version by Joseph H. Silverman

July 2018 v2.35. Copyright © 2018 K. Belabas

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

(PARI-GP version 2.11.0)

## Coefficients, variables and basic operators

degree of $f$	<code>poldegree(f)</code>
coef. of degree $n$ of $f$ , leading coef.	<code>polcoef(f,n), pollead</code>
main variable / all variables in $f$	<code>variable(f), variables(f)</code>
replace $x$ by $y$ in $f$	<code>subst(f,x,y)</code>
evaluate $f$ replacing vars by their value	<code>eval(f)</code>
replace polynomial expr. $T(x)$ by $y$ in $f$	<code>substpol(f,T,y)</code>
replace $x_1, \dots, x_n$ by $y_1, \dots, y_n$ in $f$	<code>substvec(f,x,y)</code>
reciprocal polynomial $x^{\deg f} f(1/x)$	<code>polrecip(f)</code>
gcd of coefficients of $f$	<code>content(f)</code>
derivative of $f$ w.r.t. $x$	<code>deriv(f,{x})</code>
formal integral of $f$ w.r.t. $x$	<code>intformal(f,{x})</code>
formal sum of $f$ w.r.t. $x$	<code>sumformal(f,{x})</code>

## Constructors & Special Polynomials

interpolating pol. eval. at $a$	<code>polinterpolate(X,{Y},{a})</code>
$P_n, T_n/U_n, H_n$	<code>pollegendre, polchebyshev, polhermite</code>
$n$ -th cyclotomic polynomial $\Phi_n$	<code>polcyclo(n,{v})</code>
return $n$ if $f = \Phi_n$ , else 0	<code>poliscyclo(f)</code>
is $f$ a product of cyclotomic polynomials?	<code>poliscycloprod(f)</code>
Zagier's polynomial of index $(n,m)$	<code>polzagier(n,m)</code>

## Resultant, elimination

discriminant of polynomial $f$	<code>poldisc(f)</code>
find factors of <code>poldisc(f)</code>	<code>poldiscfactors(f)</code>
resultant $R = \text{Res}_v(f,g)$	<code>polresultant(f,g,{v})</code>
$[u,v,R], xu + yv = \text{Res}_v(f,g)$	<code>polresultantext(x,y,{v})</code>
solve Thue equation $f(x,y) = a$	<code>thue(t,a,{sol})</code>
initialize $t$ for Thue equation solver	<code>thueinit(f)</code>

## Roots and Factorization (Complex/Real)

complex roots of $f$	<code>polroots(f)</code>
bound complex roots of $f$	<code>polrootsbound(f)</code>
number of real roots of $f$ (in $[a,b]$ )	<code>polsturm(f,{[a,b]})</code>
real roots of $f$ (in $[a,b]$ )	<code>polrootsreal(f,{[a,b]})</code>
complex embeddings of <code>t_POLMOD z</code>	<code>conjvec(z)</code>

## Roots and Factorization (Finite fields)

factor $f \bmod p$ , roots	<code>factormod(f,p), polrootsmod</code>
factor $f$ over $\mathbf{F}_p[x]/(T)$ , roots	<code>factormod(f,[T,p]), polrootsmod</code>
squarefree factorization of $f$ in $\mathbf{F}_q[x]$	<code>factormodSQF(f,{D})</code>
distinct degree factorization of $f$ in $\mathbf{F}_q[x]$	<code>factormodDDF(f,{D})</code>

## Roots and Factorization ( $p$ -adic fields)

factor $f$ over $\mathbf{Q}_p$ , roots	<code>factorpadic(f,p,r), polrootspadic</code>
$p$ -adic root of $f$ congruent to $a \bmod p$	<code>padicappr(f,a)</code>
Newton polygon of $f$ for prime $p$	<code>newtonpoly(f,p)</code>
Hensel lift $A/\text{lc}(A) = \prod_i B[i] \bmod p^e$	<code>polhensellift(A,B,p,e)</code>
extensions of $\mathbf{Q}_p$ of degree $N$	<code>padicfields(p,N)</code>

## Roots and Factorization (Miscellaneous)

symmetric powers of roots of $f$ up to $n$	<code>polsym(f,n)</code>
Graeffe transform of $f, g(x^2) = f(x)f(-x)$	<code>polgraeffe(f)</code>
factor $f$ over coefficient field	<code>factor(f)</code>
cyclotomic factors of $f \in \mathbf{Q}[X]$	<code>polcyclofactors(f)</code>

## Finite Fields

A finite field is encoded by any element (`t_FFELT`).

find irreducible $T \in \mathbf{F}_p[x]$ , $\deg T = n$	<code>ffinit(p,n,{x})</code>
Create $t$ in $\mathbf{F}_q \simeq \mathbf{F}_p[t]/(T)$	<code>t = ffgen(T,'t)</code>
... indirectly, with implicit $T$	<code>t = ffgen(q,'t); T = t.mod</code>
map $M$ from $\mathbf{F}_q \ni a$ to $\mathbf{F}_{q^k} \ni b$	<code>m = ffembed(a,b)</code>
build $K$ from $\mathbf{F}_q[x]/(P)$ extending $\mathbf{F}_q \ni a$ ,	<code>ffextend(a,P)</code>
evaluate map $m$ on $x$	<code>ffmap(m,x)</code>
inverse map of $m$	<code>ffinvmap(m)</code>
compose maps $m \circ n$	<code>ffcompomap(m,n)</code>
$F^n$ over $\mathbf{F}_q \ni a$	<code>fffrobenius(a,n)</code>
$\#\{\text{monic irred. } T \in \mathbf{F}_q[x], \deg T = n\}$	<code>ffnbirred(q,n)</code>

## Formal & $p$ -adic Series

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

## Transcendental and $p$ -adic Functions

real, imaginary part of $x$	<code>real(x), imag(x)</code>
absolute value, argument of $x$	<code>abs(x), arg(x)</code>
square/nth root of $x$	<code>sqrt(x), sqrtn(x,n,{&amp;z})</code>
trig functions	<code>sin, cos, tan, cotan, sinc</code>
inverse trig functions	<code>asin, acos, atan</code>
hyperbolic functions	<code>sinh, cosh, tanh, cotanh</code>
inverse hyperbolic functions	<code>asinh, acosh, atanh</code>
$\log(x), \log(1+x), e^x, e^x - 1$	<code>log, log1p, exp, expm1</code>
Euler $\Gamma$ function, $\log \Gamma, \Gamma'/\Gamma$	<code>gamma, lngamma, psi</code>
half-integer gamma function $\Gamma(n+1/2)$	<code>gammah(n)</code>
Riemann's zeta $\zeta(s) = \sum n^{-s}$	<code>zeta(s)</code>
Hurwitz's $\zeta(s,x) = \sum (n+x)^{-s}$	<code>zetahurwitz(s,x)</code>
multiple zeta value (MZV), $\zeta(s_1, \dots, s_k)$	<code>zetamult(s,{T})</code>
... init $T$ for MZV with $s_1 + \dots + s_k \leq w$	<code>zetamultinit(w)</code>
all MZVs for all weights $\sum s_i \leq n$	<code>zetamultall(n)</code>
convert MZV id to $[s_1, \dots, s_k]$	<code>zetamultconvert(f,{flag})</code>
incomplete $\Gamma$ function ( $y = \Gamma(s)$ )	<code>incgam(s,x,{y})</code>
complementary incomplete $\Gamma$	<code>incgamc(s,x)</code>
$\int_x^\infty e^{-t} dt/t, (2/\sqrt{\pi}) \int_x^\infty e^{-t^2} dt$	<code>eint1, erfc</code>
dilogarithm of $x$	<code>dilog(x)</code>
$m$ -th polylogarithm of $x$	<code>polylog(m,x,{flag})</code>
$U$ -confluent hypergeometric function	<code>hyperu(a,b,u)</code>
Bessel $J_n(x), J_{n+1/2}(x)$	<code>besselj(n,x), besseljh(n,x)</code>
Bessel $I_\nu, K_\nu, H_\nu^1, H_\nu^2, N_\nu$	<code>(bessel)i,k,h1,h2,n</code>
Lambert $W: x$ s.t. $xe^x = y$	<code>lambertw(y)</code>
Teichmuller character of $p$ -adic $x$	<code>teichmuller(x)</code>

## Iterations, Sums & Products

### Numerical integration for meromorphic functions

Behaviour at endpoint for Double Exponential (DE) methods: either a scalar ( $a \in \mathbf{C}$ , regular) or  $\pm\infty$  (decreasing at least as  $x^{-2}$ ) or

$(x-a)^{-\alpha}$ singularity	<code>[a,a]</code>
exponential decrease $e^{-\alpha x }$	<code>[<math>\pm\infty, \alpha</math>], <math>\alpha &gt; 0</math></code>
slow decrease $ x ^\alpha$	<code>... <math>\alpha &lt; -1</math></code>
oscillating as $\cos(kx)$	<code><math>\alpha = k\mathbf{I}, k &gt; 0</math></code>
oscillating as $\sin(kx)$	<code><math>\alpha = -k\mathbf{I}, k &gt; 0</math></code>
numerical integration	<code>intnum(<math>x=a,b,f,{T}</math>)</code>
weights $T$ for intnum	<code>intnuminit(<math>a,b,K,{m}</math>)</code>
weights $T$ incl. kernel $K$	<code>intfuncinit(<math>a,b,K,{m}</math>)</code>
integrate $(2i\pi)^{-1} f$ on circle $ z-a =R$	<code>intcirc(<math>x=a,R,f,{T}</math>)</code>

### Other integration methods

$n$ -point Gauss-Legendre	<code>intnumgauss(<math>x=a,b,f,{n}</math>)</code>
weights for $n$ -point Gauss-Legendre	<code>intnumgaussinit(<math>\{n\}</math>)</code>
Romberg integration (low accuracy)	<code>intnumromb(<math>x=a,b,f,{flag}</math>)</code>

### Numerical summation

sum of series $f(n), n \geq a$ (low accuracy)	<code>suminf(<math>n=a,expr</math>)</code>
sum of alternating/positive series	<code>sumalt, sumpos</code>
sum of series using Euler-Maclaurin	<code>sumnum(<math>n=a,f,{T}</math>)</code>
$\sum_{n \geq a} F(n)$ , $F$ rational function	<code>sumnumrat(<math>F,a</math>)</code>
$\dots \sum_{n \geq a} (-1)^n F(n)$	<code>sumaltrat(<math>F,a</math>)</code>
$\dots \sum_{p \geq a} F(p^s)$	<code>sumeulerrat(<math>F,\{s=1\},\{a=2\}</math>)</code>
weights for <code>sumnum</code> , $a$ as in DE	<code>sumnuminit(<math>\{\infty,a\}</math>)</code>
sum of series by Monien summation	<code>sumnummonien(<math>n=a,f,{T}</math>)</code>
weights for <code>sumnummonien</code>	<code>sumnummonieninit(<math>\{\infty,a\}</math>)</code>
sum of series using Abel-Plana	<code>sumnumap(<math>n=a,f,{T}</math>)</code>
weights for <code>sumnumap</code> , $a$ as in DE	<code>sumnumapinit(<math>\{\infty,a\}</math>)</code>
sum of series using Lagrange	<code>sumnumlagrange(<math>n=a,f,{T}</math>)</code>
weights for <code>sumnumlagrange</code>	<code>sumnumlagrangeinit</code>

### Products

product $a \leq X \leq b$ , initialized at $x$	<code>prod(<math>X=a,b,expr,\{x\}</math>)</code>
product over primes $a \leq X \leq b$	<code>prodeuler(<math>X=a,b,expr</math>)</code>
infinite product $a \leq X \leq \infty$	<code>prodinfn(<math>X=a,expr</math>)</code>
$\prod_{n \geq a} F(n)$ , $F$ rational function	<code>prodnumrat(<math>F,a</math>)</code>
$\dots \prod_{p \geq a} F(p^s)$	<code>prodeulerrat(<math>F,\{s=1\},\{a=2\}</math>)</code>

### Other numerical methods

real root of $f$ in $[a,b]$ ; bracketed root	<code>solve(<math>X=a,b,f</math>)</code>
... by interval splitting	<code>solvestep(<math>X=a,b,f,{flag=0}</math>)</code>
limit of $f(t), t \rightarrow \infty$	<code>limitnum(f,{k},{alpha})</code>
asymptotic expansion of $f$ at $\infty$	<code>asypnum(f,{k},{alpha})</code>
numerical derivation w.r.t $x: f'(a)$	<code>derivnum(<math>x=a,f</math>)</code>
evaluate continued fraction $F$ at $t$	<code>contfraceval(<math>F,t,\{L\}</math>)</code>
power series to cont. fraction ( $L$ terms)	<code>confracinit(<math>S,\{L\}</math>)</code>
Padé approximant (deg. denom. $\leq B$ )	<code>bestapprPade(<math>S,\{B\}</math>)</code>

Elementary Arithmetic Functions

vector of binary digits of $ x $	<code>binary(<math>x</math>)</code>
bit number $n$ of integer $x$	<code>bittest(<math>x, n</math>)</code>
Hamming weight of integer $x$	<code>hammingweight(<math>x</math>)</code>
digits of integer $x$ in base $B$	<code>digits(<math>x, \{B = 10\}</math>)</code>
sum of digits of integer $x$ in base $B$	<code>sumdigits(<math>x, \{B = 10\}</math>)</code>
integer from digits	<code>fromdigits(<math>v, \{B = 10\}</math>)</code>
ceiling/floor/fractional part	<code>ceil, floor, frac</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>	
extra prime table	<code>addprimes()</code>
add primes in $v$ to prime table	<code>addprimes(<math>v</math>)</code>
remove primes from prime table	<code>removeprimes(<math>v</math>)</code>
Chebyshev $\pi(x)$ , $n$ -th prime $p_n$	<code>primepi(<math>x</math>), 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>preprime(<math>x</math>)</code>
factorization of $x$	<code>factor(<math>x, \{lim\}</math>)</code>
...selecting specific algorithms	<code>factorint(<math>x, \{flag = 0\}</math>)</code>
$n = df^2$ , $d$ squarefree/fundamental	<code>core(<math>n, \{fl\}</math>), coredisc</code>
certificate for (prime) $N$	<code>primecert(<math>N</math>)</code>
verifies a certificate $c$	<code>primecertisvalid(<math>c</math>)</code>
convert certificate to Magma/PRIMO	<code>primecertexport</code>
recover $x$ from its factorization	<code>factorback(<math>f, \{e\}</math>)</code>
$x \in \mathbf{Z}$ , $ x  \leq X$ , $\gcd(N, P(x)) \geq N$	<code>zncoppersmith(<math>P, N, X, \{B\}</math>)</code>
divisors of $N$ in residue class $r \bmod s$	<code>divisorslenstra(<math>N, r, s</math>)</code>
<b>Divisors and multiplicative functions</b>	
number of prime divisors $\omega(n)$ / $\Omega(n)$	<code>omega(<math>n</math>), bigomega</code>
divisors of $n$ / number of divisors $\tau(n)$	<code>divisors(<math>n</math>), numdiv</code>
sum of ( $k$ -th powers of) divisors of $n$	<code>sigma(<math>n, \{k\}</math>)</code>
Möbius $\mu$ -function	<code>moebius(<math>x</math>)</code>
Ramanujan's $\tau$ -function	<code>ramanujantau(<math>x</math>)</code>
<b>Combinatorics</b>	
factorial of $x$	<code><math>x!</math> or factorial(<math>x</math>)</code>
binomial coefficient $\binom{x}{k}$	<code>binomial(<math>x, \{k\}</math>)</code>
Bernoulli number $B_n$ as real/rational	<code>bernreal(<math>n</math>), bernfrac</code>
Bernoulli polynomial $B_n(x)$	<code>bernpol(<math>n, \{x\}</math>)</code>
$n$ -th Fibonacci number	<code>fibonacci(<math>n</math>)</code>
Stirling numbers $s(n, k)$ and $S(n, k)$	<code>stirling(<math>n, k, \{flag\}</math>)</code>
number of partitions of $n$	<code>numbpart(<math>n</math>)</code>
$k$ -th permutation on $n$ letters	<code>numtoperm(<math>n, k</math>)</code>
convert permutation to $(n, k)$ form	<code>permtotnum(<math>v</math>)</code>
order of permutation $p$	<code>permorder(<math>p</math>)</code>
signature of permutation $p$	<code>permsign(<math>p</math>)</code>
<b>Multiplicative groups <math>(\mathbf{Z}/N\mathbf{Z})^*</math>, <math>\mathbf{F}_q^*</math></b>	
Euler $\phi$ -function	<code>eulerphi(<math>x</math>)</code>
multiplicative order of $x$ (divides $\phi$ )	<code>znorder(<math>x, \{o\}</math>), fforder</code>
primitive root mod $q$ / $x$ .mod	<code>znprimroot(<math>q</math>), ffprimroot(<math>x</math>)</code>
structure of $(\mathbf{Z}/n\mathbf{Z})^*$	<code>znstar(<math>n</math>)</code>
discrete logarithm of $x$ in base $g$	<code>znlog(<math>x, g, \{o\}</math>), fflag</code>
Kronecker-Legendre symbol $(\frac{x}{y})$	<code>kronecker(<math>x, y</math>)</code>
quadratic Hilbert symbol (at $p$ )	<code>hilbert(<math>x, y, \{p\}</math>)</code>

<b>Miscellaneous</b>	
integer square / $n$ -th root of $x$	<code>sqrntint(<math>x</math>), sqrtnint(<math>x, n</math>)</code>
largest integer $e$ s.t. $b^e \leq b$ , $e = \lfloor \log_b(x) \rfloor$	<code>logint(<math>x, b, \{\&amp;z\}</math>)</code>
CRT: 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>gcdext(<math>x, y</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>
rational approximation to $x$ (den. $\leq B$ )	<code>bestappr(<math>x, \{B\}k</math>)</code>
recognize $x \in \mathbf{C}$ as polmod mod $T \in \mathbf{Z}[X]$	<code>bestapprnf(<math>x, T</math>)</code>

Characters

Let $cyc = [d_1, \dots, d_k]$ represent an abelian group $G = \oplus (\mathbf{Z}/d_j\mathbf{Z}) \cdot g_j$ or any structure $G$ affording a .cyc method; e.g. <code>znstar(<math>q, 1</math>)</code> for Dirichlet characters. A character $\chi$ is coded by $[c_1, \dots, c_k]$ such that $\chi(g_j) = e(n_j/d_j)$ .	
$\chi \cdot \psi$ ; $\chi^{-1}$ ; $\chi \cdot \psi^{-1}$ ; $\chi^k$	<code>charmul, charconj, chardiv,, charpow</code>
order of $\chi$	<code>charorder(<math>cyc, \chi</math>)</code>
kernel of $\chi$	<code>charker(<math>cyc, \chi</math>)</code>
$\chi(x)$ , $G$ a GP group structure	<code>chareval(<math>G, \chi, x, \{z\}</math>)</code>
Galois orbits of characters	<code>chargalois(<math>G</math>)</code>

Dirichlet Characters

initialize $G = (\mathbf{Z}/q\mathbf{Z})^*$	<code>G = znstar(<math>q, 1</math>)</code>
convert datum $D$ to $[G, \chi]$	<code>znchar(<math>D</math>)</code>
is $\chi$ odd?	<code>zncharisodd(<math>G, \chi</math>)</code>
real $\chi \rightarrow$ Kronecker symbol $(D/.)$	<code>znchartokronecker(<math>G, \chi</math>)</code>
conductor of $\chi$	<code>zncharconductor(<math>G, \chi</math>)</code>
$[G_0, \chi_0]$ primitive attached to $\chi$	<code>znchartoprimitive(<math>G, \chi</math>)</code>
induce $\chi \in \hat{G}$ to $\mathbf{Z}/N\mathbf{Z}$	<code>zncharinduce(<math>G, \chi, N</math>)</code>
$\chi_p$	<code>znchardecompose(<math>G, \chi, p</math>)</code>
$\prod_p  (\chi, N)  \chi_p$	<code>znchardecompose(<math>G, \chi, Q</math>)</code>
complex Gauss sum $G_a(\chi)$	<code>znchargauss(<math>G, \chi</math>)</code>

Conrey labelling

Conrey label $m \in (\mathbf{Z}/q\mathbf{Z})^* \rightarrow$ character	<code>znconreychar(<math>G, m</math>)</code>
character $\rightarrow$ Conrey label	<code>znconreyexp(<math>G, \chi</math>)</code>
log on Conrey generators	<code>znconreylog(<math>G, m</math>)</code>
conductor of $\chi$ ( $\chi_0$ primitive)	<code>znconreyconductor(<math>G, \chi, \{\chi_0\}</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 $x$ a perfect power?	<code>ispower(<math>x, \{k\}, \{\&amp;n\}</math>)</code>
is $x$ a perfect power of a prime? ( $x = p^n$ )	<code>isprimepower(<math>x, \&amp;n\}</math>)</code>
... of a pseudoprime?	<code>ispseudoprimepower(<math>x, \&amp;n\}</math>)</code>
is $x$ powerful?	<code>ispowerful(<math>x</math>)</code>
is $x$ a totient? ( $x = \varphi(n)$ )	<code>istotient(<math>x, \{\&amp;n\}</math>)</code>
is $x$ a polygonal number? ( $x = P(s, n)$ )	<code>ispolygonal(<math>x, s, \{\&amp;n\}</math>)</code>
is $pol$ irreducible?	<code>polisirreducible(<math>pol</math>)</code>

Graphic Functions

crude graph of $expr$ between $a$ and $b$	<code>plot(<math>X = a, b, expr</math>)</code>
<b>High-resolution plot</b> (immediate plot)	
plot $expr$ between $a$ and $b$	<code>plotth(<math>X = a, b, expr, \{flag\}, \{n\}</math>)</code>
plot points given by lists $lx, ly$	<code>plotthraw(<math>lx, ly, \{flag\}</math>)</code>
terminal dimensions	<code>plotsizes()</code>

Rectwindow functions

init window $w$ , with size $x, y$	<code>plotinit(<math>w, x, y</math>)</code>
erase window $w$	<code>plotkill(<math>w</math>)</code>
copy $w$ to $w_2$ with offset $(dx, dy)$	<code>plotcopy(<math>w, w_2, dx, dy</math>)</code>
clips contents of $w$	<code>plotclip(<math>w</math>)</code>
scale coordinates in $w$	<code>plotscale(<math>w, x_1, x_2, y_1, y_2</math>)</code>
plot $in\ w$	<code>plotrecth(<math>w, X = a, b, expr, \{flag\}, \{n\}</math>)</code>
plot $throw\ in\ w$	<code>plotrecththrow(<math>w, data, \{flag\}</math>)</code>
draw window $w_1$ at $(x_1, y_1), \dots$	<code>plotdraw(<math>[[w_1, x_1, y_1], \dots]</math>)</code>

Low-level Rectwindow Functions

set current drawing color in $w$ to $c$	<code>plotcolor(<math>w, c</math>)</code>
current position of cursor in $w$	<code>plotcursor(<math>w</math>)</code>
write $s$ at cursor's position	<code>plotstring(<math>w, s</math>)</code>
move cursor to $(x, y)$	<code>plotmove(<math>w, x, y</math>)</code>
move cursor to $(x + dx, y + dy)$	<code>plotrmove(<math>w, dx, dy</math>)</code>
draw a box to $(x_2, y_2)$	<code>plotbox(<math>w, x_2, y_2</math>)</code>
draw a box to $(x + dx, y + dy)$	<code>plotrbox(<math>w, dx, dy</math>)</code>
draw polygon	<code>plotlines(<math>w, lx, ly, \{flag\}</math>)</code>
draw points	<code>plotpoints(<math>w, lx, ly</math>)</code>
draw line to $(x + dx, y + dy)$	<code>plotrline(<math>w, dx, dy</math>)</code>
draw point $(x + dx, y + dy)$	<code>plotrpoint(<math>w, dx, dy</math>)</code>
draw point $(x + dx, y + dy)$	<code>plotrpoint(<math>w, dx, dy</math>)</code>

Convert to Postscript or Scalable Vector Graphics

The format $f$ is either "ps" or "svg".	
as plot	<code>plotthexport(<math>f, X = a, b, expr, \{flag\}, \{n\}</math>)</code>
as plotdraw	<code>plotthrawexport(<math>f, lx, ly, \{flag\}</math>)</code>
as plotdraw	<code>plotexport(<math>f, [[w_1, x_1, y_1], \dots]</math>)</code>

Based on an earlier version by Joseph H. Silverman  
July 2018 v2.35. Copyright © 2018 K. Belabas  
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)