PARI-GP Reference Card

(PARI-GP version 1.39)

Starting & Stopping PARI-GP

To enter PARI-GP, just type its name:	`gp`
To exit PARI-GP, type	`\q`

Input/Output and Defaults

set n significant digits	`\precision=`n
set n terms in series	`\serieslength=`n
set prompt string	`\prompt=string`
output of previous line	`%`
output from line n	`%`n
separate multiple statements on line	`;`
extend statement on additional lines	`\`
extend statements on several lines	`{`$seq1$`;` $seq2$`;}`
comment, rest of line ignored	`\\`

Metacommands

print %n in raw format	`\a`n
print %n in pretty format	`\b`n
print list of all functions	`\c`
print defaults	`\d`
kill and restart GP	`\k`
store GP session in `pari.log`	`\l`
print %n in pretty matrix format	`\m`
cycle default print format	`\p`
quit GP	`\q`
print state of stack	`\s`
toggle timer on/off	`#`
read file into GP	`\r` filename
write %n to file	`\w`n filename

Help

print list of all functions	`\c`
describe function	?function

PARI-GP Within Emacs

To enter PARI-GP from within Emacs, type: `M-x gp`

For PARI/Emacs information, see the file `/usr/local/PARI/pari.txt`

help menu window	`M-\c`
describe function	`M-?`
display TEX'd PARI manual	`M-x gpman`
set prompt string	`M-\p`
break line at column 100, insert `\`	`M-\\`
PARI metacommand `\`*letter*	`M-\`*letter*

Reserved Variable Names

$\pi = 3.14159\cdots$	`pi`
Euler's constant $= .577\cdots$	`euler`
square root of -1	`i`
big-oh notation	`O`

PARI Types and Input Formats

1. Integers	$\pm n$
2. Real Numbers	$\pm n.ddd$
3. Integermods	`mod`(n,m)
4. Rational Numbers	n/m
6. Complex Numbers	$x+i*y$
7. p-adic Numbers	$x+O(p^k)$
8. Quadratic Numbers	$x+y*w$
9. Polymods	`mod`(f,g)
10. Polynomials	$a*x^n+\cdots+b$
11. Power Series	$f+O(x^k)$
13. Rational Functions	f/g
17. Row Vectors	$[x,y,z]$
18. Column Vectors	$[x,y,z]$~
19. Matrices	$[x,y;z,t;u,v]$

Standard Operators

basic operations	$+,-,*,/,\hat{}$
Euclidean quotient, remainder	$x\backslash y,\ x\%y$
Euclidean quotient and remainder	`divres`(x,y)
shift x left or right n bits	`shift`(x,n)
comparison operators	$<=,<,>=,>,==,!=$
Boolean operators	$\vert\vert,\ \&\&$
sign of $x=-1,0,1$	`sign`(x)
integer or real factorial of x	$x!$ or `fact`(x)

Conversions

object x with precision n	`prec`(x,n)
simplify the object x	`simplify`(x)

Change Objects

transform x into a vector	`vec`(x)
transform object x into a matrix	`mat`(x)
create PARI object (x mod y)	`mod`(x,y)
make x a polynomial of v	`poly`(x,v)
make x a power series of v	`series`(x,v)
PARI type of object x	`type`(x)

Select Pieces of an Object

length of x	`length`(x)
nth component of x	`compo`(x,n)
nth component of vector 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	`numer`(x)
lowest denominator of x	`denom`(x)

Miscellaneous

conjugate of a number x	`conj`(x)
norm of x, product with conjugate	`norm`(x)
lift of x from mods	`lift`(x)
square of L^2 norm of vector x	`norml2`(x)
kth permutation of $1,\ldots,n$	`permutation`(n,k)
vector of binary digits of $\vert x\vert$	`binary`(x)
random integer between 0 and $2^{31}-1$	`random()`

Sorting

sort x by kth component	`vecsort`(x,k)
sort elements of x in ascending order	`sort`(x)
permutation that sorts elements of x	`indsort`(x)
sort elements of x in ascending lex order	`lexsort`(x)

Programming & User Def'd Funcs.

Control Statements

eval. seq for $a \le X \le b$	`for`$(X=a,b,seq)$
eval. seq for X dividing n	`fordiv`(n,X,seq)
eval. seq for primes $a \le X \le b$	`forprime`$(X=a,b,seq)$
eval. seq for $a \le X \le b$ stepping s	`forstep`$(X=a,b,s,seq)$
if $a\neq 0$, evaluate $seq1$, else $seq2$	`if`$(a,seq1,seq2)$
evaluate seq until $a \neq 0$	`until`(a,seq)
while $a\neq 0$, evaluate seq	`while`(a,seq)

Programming Functions

kill value of variable or function x	`kill`(x)
prettyprint *list* with newline	`pprint`(*list*)
prettyprint *list* w/o a newline	`pprint1`(*list*)
print *list* in raw format with newline	`print`(*list*)
print *list* in raw format w/o a newline	`print1`(*list*)
read a string from keyboard	`read()`
reorder priority of variables $[x,y,z]$	`reorder`$([x,y,z])$
output *list* in TEX format	`texprint`(*list*)

User Defined Functions

`name(list of formal vars, list of local vars)=seq`

Formal & p-adic Series

truncate power series or p-adic number	`trunc`(x)
valuation of x at p	`valuation`(x,p)

Power Series

reverse power series F so $F(f(x))=x$	`reverse`(f)
Taylor expansion around 0 of f w.r.t. x	`taylor`(f,x)
convol $\sum a_k b_k t^k$ of $\sum a_k t^k$ & $\sum b_k t^k$	`convol`(x,y)
$\sum(a_k/k!)*t^k$ from $f=\sum a_k*t^k$	`laplace`(f)

p-adic Functions

square of x, good for 2-adics	`sqr`(x)
Teichmuller character of x	`teich`(x)
Newton polygon of f for prime p	`newtonpoly`(f,p)

Number Fields

vector v for field K of irred. $f\in\mathbf{Q}[X]$	`initalgred`(f)
simple poly defining K	`v[1]`
number of [real,complex] places	`v[2]`
discriminant of K	`v[3]`
index $[\mathbf{Z}_K:\mathbf{Z}[\theta]]$, $\theta=$ root of $v[1]$	`v[4]`
L^2 norm of roots of $v[1]$	`v[5]`
vector of roots of $v[1]$	`v[6]`
integral basis of $\mathbf{Z}_K$ as powers of θ	`v[7]`
integral basis of field def. by $f=0$	`base`(f)
field discriminant of field $f=0$	`discf`(f)
factorization of g in field $f=0$	`factornf`(g,f)
Galois group of field $f=0$, $\deg f\le 7$	`galois`(f)
number of roots of 1 in field $f=0$	`rootsof1`(f)
conjugates of a root r of f	`galoisconj`(f)
symmetric powers of roots of f up to n	`polsym`(f,n)
reverse polymod $a=A(X)$ mod $T(X)$	`modreverse`(a)
small polys defining subfields of $f=0$	`polred`(f),`polred2`(f)
small polys defining suborders of $f=0$	`ordred`(f)
poly of degree $\le k$ 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?	`isisom`(f,g)
is field $f=0$ a subfield of $g=0$?	`isincl`(f,g)

PARI-GP Reference Card

(PARI-GP version 1.39)

Polynomials

replace x by y in f	`subst`(f,x,y)
replace in f newly def'd formal vars.	`eval`(f)
degree n coefficient of f	`coeff`(f,n)
gcd of coefficients of f	`content`(f)
round coefs of f to integers	`rndtoi`(f)
reciprocal poly $x^{\deg f} f(1/x)$	`recip`(f)
complex roots of f	`roots`(f)
complex roots of f (higher precision)	`rootslong`(f)
number of real roots of f	`sturm`(f)
number of real roots of f, $a \le x \le b$	`sturmpart`(f,a,b)
factor f	`factor`(f)
factor $f \in \mathbf{Z}[t]$, factor of degree $\le l$	`factpol`(f,l)
roots of f mod p, good for big p	`rootmod`(f,p)
roots of f mod p, good for small p	`rootmod2`(f,p)
factorization of f mod p	`factmod`(f,p)
factorization of f over $\mathbf{F}_q$, $q=p^a$	`factfq`(f,p,a)
p-adic root of f congruent to a mod p	`apprpadic`(f,a)
p-adic factorization of f to precision r	`factorpadic`(f,p,r)
vector of p-adic roots of f to precision r	`rootpadic`(f,p,r)
Newton polygon of f for prime p	`newtonpoly`(f,p)
interpolating poly evaluated at x	`polint`$(x_{\text{vals}}, y_{\text{vals}}, x)$
nth cyclotomic polynomial	`cyclo`(n)
discriminant of polynomial f	`disc`(f)
resultant of f and g	`resultant`(f,g)
derivative of f w.r.t. x	`deriv`(f,x)
formal integral of f w.r.t. x	`integ`(f,x)

Vectors and Matrices

$n \times n$ identity matrix	`idmat`(n)
dimensions of matrix x	`matsize`(x)
concatenation of x and y	`concat`(x,y)
extract components of x as spec'ed by y	`extract`(x,y)
extract rows and cols. from matrix x	`matextract`(x,y)
transpose of vector or matrix x	`trans`(x) or x`~`
determinant of matrix x	`det`(x)
trace of matrix x	`trace`(x)
eigenvectors of matrix x	`eigen`(x)
adjoint of the matrix x	`adj`(x)
characteristic poly of x with variable y	`char`(x,y)
rank of the matrix x	`rank`(x)
solve $x*u=y$ by Gaussian elimination	`gauss`(x,y)
inverse of real matrix x	`matinvr`(x)
basis for image of matrix x	`image`(x)
supplement columns of x to get basis	`supplement`(x)
rows, cols to extract invertible matrix	`indexrank`(x)
kernel of matrix x ($\mathbf{Z}$, $\mathbf{R}$, $\mathbf{C}$ coefs)	`ker`(x),`keri`(x),`kerr`(x)
one sol of $x*u=y$, matrix x, vector y	`inverseimage`(x,y)
LLL-algorithm functions	`lll, lllint, lllgram`
linear relation on coords of x	`lindep`(x)

Elliptic and Modular Functions

elliptic j-function $1/q+744+\cdots$	`jell`(x)
Dedekind η func. $\prod(1-q^n)$	`eta`(x)
Riemann's zeta $\zeta(s)=\sum n^{-s}$	`zeta`(s)
arithmetic-geometric mean	`agm`(x,y)

Elliptic Curves

Elliptic curve is initially given by 5-tuple `e=[a1,a2,a3,a4,a6]`. Generate longer vectors E with more info. using `initell` and `smallinitell`. Points are `[x,y]`, the origin is `[0]`.

Generate 13 component vector E	`smallinitell`(e)
$a_1,a_2,a_3,a_4,a_6,b_2,b_4,b_6,b_8,c_4,c_6,\Delta,j$	
Generate 19 component vector E	`initell`(e)
First 13 components same as `smallinitell`	
`e` defined over $\mathbf{R}$	
x-coords. of points of order 2	$E[14]$
real and complex periods	$E[15], E[16]$
associated quasi-periods	$E[17], E[18]$
volume of complex lattice	$E[19]$
`e` defined over $\mathbf{Q}_p$, $\lvert j\rvert_p > 1$	
x-coord. of unit 2 torsion point	$E[14]$
Tate's u^2, u, q, Mestre's w	$E[15], E[16], E[17], E[18]$
change coords using $v=[u,r,s,t]$	`chell`(e,v), `chptell`(x,v)
cond, min mod, Tamgwa nmbr $[N,v,c]$	`globalred`(e)
Kodaira type of p fiber of e	`localred`(e,p)
add points $z1+z2$	`addell`$(e,z1,z2)$
subtract points $z1-z2$	`subell`$(e,z1,z2)$
compute nz	`powell`(e,z,n)
check if z is on e	`isoncurve`(e,z)
order of torsion point z	`orderell`(e,z)
torsion subgroup with gens	`torsell`(e)
y-coordinates of point(s) for x	`ordell`(e,x)
canonical height of z	`hell`(e,z)
canonical height using Tate's series	`hell2`(e,z)
height regulator matrix for list of pts x	`mathell`(e,x)
pth coeff a_p of L-function, p prime	`apell`(e,p)
kth coeff a_k of L-function	`akell`(e,k)
vector of first n a_k's in L-function	`anell`(e,n)
$L(e,s)$, set $N=$ cond., $A\approx 1$	`lseriesell`(e,s,N,A)
point $[\wp(t),\wp'(t)]$ corresp. to t	`pointell`(e,t)
point t with $z=[\wp(t),\wp'(t)]$	`zell`(e,z)
modular parametrization of e	`taniyama`(e)

Sums and Products

The letter X denotes a simple variable name and represents the formal parameter used in the function.

row vec. of *expr* eval'ed at $1\le X\le n$	`vector`(n,X,expr)
col. vec. of *expr* eval'ed at $1\le X\le n$	`vvector`(n,X,expr)
matrix $1\le X\le m$, $1\le Y\le n$	`matrix`(m,n,X,Y,expr)
sum $X=a$ to $X=b$, initialized at x	`sum`$(x,X=a,b,\mathit{expr})$
sum *expr* over divisors of n	`divsum`(n,X,expr)
product $a\le X\le b$, initialized at x	`prod`$(x,X=a,b,\mathit{expr})$
product over primes $a\le X\le b$	`prodeuler`$(X=a,b,\mathit{expr})$
infinite product $a\le X\le\infty$	`prodinf`$(X=a,\mathit{expr})$
infinite product of $1+\mathit{expr}$	`prodinf1`$(X=a,\mathit{expr})$
real root of *expr* between a and b	`solve`$(X=a,b,\mathit{expr})$

True-False Tests

Is x the disc. of a quadratic field?	`isfund`(x)
Is x a prime?	`isprime`(x)
Is x a strong pseudo-prime?	`ispsp`(x)
Is x square-free?	`issqfree`(x)
Is x a square?	`issquare`(x)

Elementary Arithmetic Functions

ceiling of x	`ceil`(x)
floor of x	`floor`(x)
fractional part of x	`frac`(x)
round x to nearest integer	`round`(x)
gcd of x and y	`gcd`(x,y)
LCM of x and y	`lcm`(x,y)
gcd of entries of a vector/matrix	`content`(x)

Primes and Factorization

the nth prime	`prime`(n)
vector of first n primes	`primes`(n)
smallest prime $\ge x$	`nextprime`(x)
factorization of x	`factor`(x)
factor integer x for primes up to l	`boundfact`(x,l)
factor integer x for default primes	`smallfact`(x)

Divisors

number of distinct prime divisors	`omega`(x)
number of prime divisors with mult	`bigomega`(x)
number of divisors of x	`numdiv`(x)
row vector of divisors of x	`divisors`(x)
sum of divisors of x	`sigma`(x)
sum of kth powers of divisors of x	`sigmak`(k,x)

Special Functions and Numbers

binomial coefficient $\binom{x}{y}$	`bin`(x,y)
Bernoulli number B_n as real	`bernreal`(n)
Bernoulli vector $B_0,B_2,\ldots,B_{2n}$	`bernvec`(n)
nth Legendre polynomial	`legendre`(n)
nth Tchebicheff polynomial	`tchebi`(n)
Euler ϕ-function	`phi`(x)
Möbius μ-function	`mu`(x)
Hilbert symbol of x and y	`hilb`(x,y,p) or `hilb`(x,y)
Kronecker-Legendre symbol $\left(\frac{x}{y}\right)$	`kro`(x,y)

Miscellaneous

integer square root of x	`isqrt`(x)
solve $z\equiv x$ and $z\equiv y$	`chinese`(x,y)
minimal u,v so $xu+yv=\gcd(x,y)$	`bezout`(x,y)
primitive root mod prime power q	`primroot`(q)
multiplicative order of x mod n	`order`(x,n)
continued fraction functions	`cf, pnqn`
best rational approx to x	`bestappr`(x,k)

Elementary Transcendental Functions

real, imaginary part of x	`real`(x), `imag`(x)
absolute value, argument of x	`abs`(x), `arg`(x)
trig functions	`sin, cos, tan`
inverse trig functions	`asin, acos, atan`
hyperbolic functions	`sinh, cosh, tanh`
inverse hyperbolic functions	`asinh, acosh, atanh`
exponential of x	`exp`(x)
natural log of x	`ln`(x) or `log`(x)
square root of x	`sqrt`(x)
gamma function $\Gamma(x)=\int_0^\infty e^{-t}t^{x-1}dt$	`gamma`(x)

Send comments and corrections to J.H. Silverman, Math. Dept., Brown Univ., Providence, RI 02912 USA. (jhs@gauss.math.brown.edu)