

Introduction to PARI

David Whitehouse
California Institute of Technology

1 Why Use PARI?

Many of the Math 7 homeworks are going to require you to do some number theoretical computations, for example computing the prime factorization of an integer or the greatest common divisor of two numbers. PARI is a VERY useful computer program for doing these computations because it has a lot of these number theoretic functions built in. I strongly encourage you to try it out.

2 How To Get PARI

You can get PARI from the web at

`ftp://megrez.math.u-bordeaux.fr/pub/pari/`

If you are running windows then go to the windows directory and download the files `cygwin1.dll.gz` and `gp-2-1-3.exe.gz`. Once you have unzipped these files to the same directory just double click on the file `gp-sta` and you're ready to go. There are unix and mac versions as well, see the readme file at the address above for more information. You can also telnet to ITS, type "setup pari" and then "gp" to use it, but beware that the version running on ITS is very old and so some of the newer functions have not been implemented in it. (We have asked ITS to put up the latest version of PARI, I'll let you know when they have done this). There are various guides to PARI available from the downloads area of the PARI website at

`www.parigp-home.de`

I would suggest downloading the user's guide, tutorial and reference card from there. It would probably be a good idea to go through the first 15 or so pages of the tutorial [1] although don't worry if it doesn't all make sense, there is plenty of stuff that PARI can do that we won't be covering in this course. I would also recommend printing out the reference card [3]. You do not need to read the user's manual [2] but you should be aware of it.

3 Basic Arithmetic

All the usual operations of addition (+), subtraction (-), multiplication (*) and division (/) work as expected. To raise one number to the power of another use the ^ symbol. PARI can work with integers, rationals, real numbers and complex numbers. The letter I has been reserved by PARI to denote the square root of -1, so if you wish to enter in the number $2 + 3i$ then in PARI you need to type in $2+3*I$. In general PARI keeps numbers in their most precise form, thus if you multiply together two rational numbers then your answer will be another rational number and not its decimal expansion. If for some reason you wish to see the decimal expansion of your computation then adding `"*1.0"` to the end of your input should have the desired effect.

4 Arithmetic Functions

`ceil(x)` gives the smallest integer larger than x

`floor(x)` gives the largest integer smaller than x

`frac(x)` gives the fractional part of x

`round(x)` rounds x to the nearest integer

`gcd(x,y)` gives the greatest common divisor of the integers x and y

`content([a1, a2, ..., an])` gives the gcd of the integers a_1, a_2, \dots, a_n

`lcm(x,y)` gives the lowest common multiple of the integers x and y

`factor(x)` gives the prime factorization of the integer x

`divisors(x)` gives a row vector consisting of the divisors of the integer x

`divrem(x,y)` gives a row vector `[a, b]` such that $x = ay + b$ with $0 \leq b < y$

`issquare(x)` determines whether the integer x is a square, PARI answers with 1 if x is a square and 0 otherwise

5 Prime Numbers

`isprime(x)` determines whether the integer x is prime, PARI answers with 1 if x is prime and 0 otherwise

`prime(n)` gives the n th prime number

`primes(n)` gives a row vector consisting of the first n prime numbers

`nextprime(x)` gives the smallest prime $\geq x$

`precprime(x)` gives the largest prime $\leq x$

6 Functions

`binomial(x,y)` gives the binomial coefficient $\binom{x}{y}$

`sqrt(x)` gives \sqrt{x}

`sqrtn(x,n)` gives $\sqrt[n]{x}$

`sin(x)`, `cos(x)`, `tan(x)` gives $\sin x$, $\cos x$ and $\tan x$ respectively

`asin(x)`, `acos(x)`, `atan(x)` gives $\arcsin x$, $\arccos x$ and $\arctan x$ respectively

`sinh(x)`, `cosh(x)`, `tanh(x)` gives $\sinh x$, $\cosh x$ and $\tanh x$ respectively

`asinh(x)`, `acosh(x)`, `atanh(x)` gives $\operatorname{arcsinh} x$, $\operatorname{arccosh} x$ and $\operatorname{arctanh} x$ respectively

`exp(x)` gives the exponential of x

`log(x)` gives the natural log of x

7 Polynomials

In PARI enter the polynomial $a_0 + a_1x + \dots + a_nx^n$ as

$$\mathbf{a_0 + a_1 * x + \dots + a_n * x^n}$$

You can add, subtract and multiply polynomials together using the same operations as for numbers.

`poldegree(f)` gives the degree of the polynomial f

`polcoeff(f,n)` gives the coefficient of x^n in the polynomial f

`deriv(f,x)` gives the derivative of f with respect to x

`polroots(f)` calculates the complex roots of f

`factor(f)` factors f as a polynomial

8 Linear Algebra

In PARI enter the matrix

$$\begin{pmatrix} a_{11} & a_{12} & \dots & a_{1n} \\ a_{21} & a_{22} & \dots & a_{2n} \\ \vdots & \vdots & \ddots & \vdots \\ a_{m1} & a_{m2} & \dots & a_{mn} \end{pmatrix}$$

as

$$[\mathbf{a}_{11}, \mathbf{a}_{12}, \dots, \mathbf{a}_{1n}; \mathbf{a}_{21}, \mathbf{a}_{22}, \dots, \mathbf{a}_{2n}; \dots; \mathbf{a}_{m1}, \mathbf{a}_{m2}, \dots, \mathbf{a}_{mn}]$$

Column vectors are entered in as matrices with only one column. You can add, subtract and multiply matrices together using the same operations as for numbers.

A^{-1} computes the inverse of the matrix A if it exists (PARI will let you know if your matrix is not invertible)

`matdet(A)` computes the determinant of the matrix A

9 Help

Typing `?` in PARI will give you a list of help topics. If you then enter `?n` where n is a number between 0 and 12 you will get a list of the PARI functions that are in that category. For example `?7` lists all the PARI functions related to polynomials and power series. If you now type in `?` followed by any of these functions PARI will tell you what the function does and how you should enter in the data. So for example `?polroots` tells you that `polroots(x)` gives the complex roots of the polynomial x .

10 Example of PARI Output

Here is a sample of PARI output to get you started, all the lines starting with a `?` is the input, everything else is output by PARI.

```
? ?
```

```
Help topics:
```

```
0: list of user-defined identifiers (variable, alias, function)
```

```
1: Standard monadic or dyadic OPERATORS
```

```
2: CONVERSIONS and similar elementary functions
```

```
3: TRANSCENDENTAL functions
```

```
4: NUMBER THEORETICAL functions
```

```
5: Functions related to ELLIPTIC CURVES
```

```
6: Functions related to general NUMBER FIELDS
```

- 7: POLYNOMIALS and power series
- 8: Vectors, matrices, LINEAR ALGEBRA and sets
- 9: SUMS, products, integrals and similar functions
- 10: GRAPHIC functions
- 11: PROGRAMMING under GP
- 12: The PARI community

Further help (list of relevant functions): ?n (1<=n<=11).

Also:

- ? functionname (short on-line help)
- ? (keyboard shortcuts)
- ? (member functions)

? ?4

addprimes	bestappr	bezout	bezoutres	bigomega
binomial	chinese	content	contfrac	contfracpnqn
core	coredisc	dirdiv	direuler	dirmul
divisors	eulerphi	factor	factorback	factorcantor
factorff	factorial	factorint	factormod	ffinit
fibonacci	gcd	hilbert	isfundamental	isprime
ispseudoprime	issquare	issquarefree	kronecker	lcm
moebius	nextprime	numdiv	omega	precprime
prime	primes	qfbclassno	qfbcompraw	qfbhclassno
qfbnucomp	qfbnupow	qfbpowraw	qfbprimeform	qfbred
quadclassunit	quaddisc	quadgen	quadhilbert	quadpoly
quadray	quadregulator	quadunit	removeprimes	sigma
sqrtint	znlog	znorder	znprimroot	znstar

? ?prime

prime(n): returns the n-th prime (n C-integer).

```
? 6+13
%1 = 19
? 9*1/7
%2 = 9/7
? 9*1/7*1.0
%3 = 1.285714285714285714285714285
? 2^7
%4 = 128
? 1+I - (7+4*I)
%5 = -6 - 3*I
? floor(23/13)
%6 = 1
```

```

? frac(7/3)
%7 = 1/3
? gcd(14,35)
%8 = 7
? lcm(6,15)
%9 = 30
? factor(1638)
%10 =
[2 1]

[3 2]

[7 1]

[13 1]

```

(Aside: this means that the prime factorization of 1638 is $2 \times 3^2 \times 7 \times 13$)

```

? divisors(1638)
%11 = [1, 2, 3, 6, 7, 9, 13, 14, 18, 21, 26, 39, 42, 63, 78, 91, 117,
126, 182, 234, 273, 546, 819, 1638]
? issquare(81)
%12 = 1
? isprime(147)
%13 = 0
? prime(15)
%14 = 47
? nextprime(200)
%15 = 211
? precprime(200)
%16 = 199
? pol=x^3+4*x^2+5*x+2
%17 = x^3 + 4*x^2 + 5*x + 2
? polroots(pol)
%18 = [-2.00000000000000000000000000000000 + 0.E-28*I, -1.00000000000000000000000000000000
+ 0.E-28*I, -1.00000000000000000000000000000000 + 0.E-28*I]
? factor(pol)
%19 =
[x + 1 2]

[x + 2 1]

```

(Aside: this means that $x^3 + 4x^2 + 5x + 2 = (x + 1)^2(x + 2)$)

```

? A=[1,2;3,4]
%20 =

```

```
[1 2]
[3 4]
? v=[1;-1]
%21 =
[1]
[-1]
? A*v
%22 =
[-1]
[-1]
? matdet(A)
%23 = -2
? A^(-1)
%24 =
[-2 1]
[3/2 -1/2]
?\q
Good bye!
```

References

- [1] *A Tutorial for PARI-GP*, from the web at www.parigp-home.de
- [2] *User's Guide to PARI-GP*, from the web at www.parigp-home.de
- [3] *PARI-GP Reference Card*, from the web at www.parigp-home.de