



AN INTRODUCTION TO PARI/GP

Marine Rougnant

Université de Franche-Comté (Besançon, France)

Institute of Mathematical Sciences (Chennai, India)

19/02/24 – 23/02/24



UNIVERSITÉ DE
FRANCHE-COMTÉ

- Pari : C library, allowing fast computations
- gp : easy-to-use interactive shell giving acces to the PARI functions
- GP : name of gp's scripting language
- gp2c : CP \rightarrow PARI compiler allows to convert GP scripts to C

- PARI/GP user's guide
- refcards
 - Basic GP
 - Number Fields
 - Elliptic Curves
 - L-functions
 - Modular Forms/Symbols
- Short help :
? ? atan
atan(x): arc tangent of x.
- Long help :
? ??atan
atan(x):
Principal branch of $\tan^{-1}(x) = \log((1+ix)/(1-ix))/2i$

??

??refcard

??refcard-nf

??tutorial

??? determinant

algdisc

charker

charpoly

ellheightma

matdet

matdetint

matdetmod

mathnfmod

nfdetint

nfhnfmod

polresultant

qfminimize

Also inspect the output of:

?? "Finite abelian groups"

?? "Relative extensions"

BASIC COMMANDS

- Assignment operator :

```
? a=1
```

```
%13 = 1
```

```
? a
```

```
%14 = 1
```

```
? a; \\ nothing printed
```

- Multi-line programs : surround the lines by braces.
- Define a user function :

```
f(x) =
```

```
{
```

```
    my (a = 2*x); \\ local variables
```

```
    my (b = a^2);
```

```
    return (a + b);
```

```
}
```

- Comments : everything following \\ to end of line, as well as /* this text */.

BASIC COMMANDS

```
? 1+1
%1 = 2
? 57!
%2 = 40526919504877216755680601905432...
? 2/6
%3 = 1/3
? 7\2
%4 3
? 7%2
%5 1
? (1+I)^2
%6 = 2*I
? (x+1)^(-2)
%7 = 1/(x^2 + 2*x + 1)
? Mod(2,5)^3 \\ in Z/5Z
%8 = Mod(3, 5)
? Mod(x, x^2+x+1) \\ in Q[x]/(x^2+x+1)
%9 = Mod(x, x^2 + x + 1)
```


Polymorphism : the domain is determined where inputs make sense and computations performed there :

```
? factor(91)
```

```
%13 = [7,1;13,1]
```

```
? factor(91+I)
```

```
%14 = [-1,1;1+I,1;4+5*I,1;1+10*I,1]
```

```
? factor(x^4+4)
```

```
%15 = [x^2-2*x+2,1;x^2+2*x+2,1]
```

```
? factor((x^4+4)*I)
```

```
%16 = [x+(-1-I),1;x+(1-I),1;x+(-1+I),1;x+(1+I),1]
```

```
? factor((x^4+1)*Mod(1,a^2-2))
```

```
%17 = [x^2+Mod(-a,a^2-2)*x+1,1;x^2+Mod(a,a^2-2)*x+1,1]
```

```
? factor((x^4+4)*Mod(1,13))
```

```
%18 = [Mod(1,13)*x+Mod(4,13),1;Mod(1,13)*x+Mod(6,13)
```



```
? V = [1,2,3];  
? W = [4,5,6]~;  
? M = [1,2,3;4,5,6];  
? V*W  
%4 = 32  
? M*W  
%5 = [32,77]~  
? U = [1..10]  
%6 = [1,2,3,4,5,6,7,8,9,10]
```

VECTORS AND MATRICES

```
? V[2]
%7 = 2
? W[1..2]
%8 = [4,5]~
? M[2,2]
%9 = 5
? M[1,]
%10 = [1,2,3]
? M[,2]
%11 = [2,5]~
? M[1..2,1..2]
%12 = [1,2;4,5]
```

```
? [n^2|n<-[1..10]]
%5 = [1,4,9,16,25,36,49,64,81,100]
? [n^2|n<-[1..10],isprime(n)]
%6 = [4,9,25,49]
? [a,b] = [1,2];
? print("a=",a," b=",b)
% a=1 b=2
```

PROGRAMMING

Control structures :

(See also : forsubset, forperm, forpart, forsubgroup, forell, forfactored, fordivfactored. . .)

```
if(cond,expr_true{,expr_false})  
while(cond, expr)  
for(var=start,end,expr(var))  
forstep(var=start,end,step,expr(var))  
forprime(var=start,end,expr(var))  
fordiv(N,var,expr(var))
```

$$\sum_{d|N} f(d)$$

```
forvec(var=[[a,b], [c,d]],expr(var))
```

$f(a, c), f(a, c + 1), \dots, f(a, d)$

$f(a + 1, c), f(a + 1, c + 1), \dots, f(a + 1, d)$

\vdots

$f(b, c), f(b, c + 1), \dots, f(b, d)$

To configure the memory used by PARI, In the file `.gprc` (`orgprc.txt` under windows) add

```
parisizemax=1G
```

or do

```
default(parisizemax,"1G");
```

if the message 'the PARI stack overflows!' appears

Galois extensions
Finite fields
Number fields
Class field theory
Elliptic curves
L-functions
Modular forms