(III.E) INTRODUCTION TO PARI

Besides the huge, expensive packages like Mathematica, Maple, and MAGMA, there are a number of free "calculators" which are useful in a particular area of mathematics: e.g. LiE and ATLAS for representation theory; the SAGE cloud for algebra, combinatorics, and number theory; and Wolfram Alpha for quick online computations across a wide range. PARI/GP is a computer algebra system for fast computations in number theory. It was originally designed by Henri Cohen, who literally wrote the book\(^1\) on computational number theory. You will want to install it on your computer from

http://pari.math.u-bordeaux.fr/

in order to do some of the exercises.

Below I have copied some commands and very simple “programs” to illustrate how PARI is used. You will also want to have a look at

- K. Conrad, “Introduction to PARI”,
- W. Stein, “Elementary number theory” (Lectures 3 and 16), and
- the official PARI tutorial and reference card.

The “?” (or “gp >”) is GP’s command prompt. Outputs are not displayed below (only the inputs). Expressions enclosed in brackets “[]” are not PARI code.

Checking the prime number theorem:

```gp
? pi(x,c=0) = forprime(p=2,x,c++);c;
? for(n=1,10,print(n*1000, ,pi(n*1000), ,n*1000/(log(n*1000)-1)))
```

Primality testing: Wilson’s theorem:

```gp
? Wilson(n) = Mod((n-1)!,n) == Mod(-1,n)
? Wilson(5)
```

Primality testing: Fermat’s theorem:

```plaintext
probprime(n,a) = Mod(a,n)^(n-1) == Mod(1,n)
```

```plaintext
x = [huge odd number]
```

```plaintext
for(i=0,100,if(probprime(x+2*i,2),print(i))
```

[do some with a=3, 4, etc.]

Discrete log:

```plaintext
dislog(x,g,s)=s=g; for(n=1,znorder(g),if(x==s,return(n),s=s*g));0;
dislog(18,Mod(5,23))
p=nextprime(9048610000)
g=Mod(5,p)
a=g^948603
dislog(a,g) [takes a moment]
znlog(a,g) [much faster, built-in optimized version]
```

Primitive roots:

```plaintext
roots(p) = for(n=1,p-1,if(znorder(Mod(n,p))==(p-1),print1(n, ))
roots(17)
roots(19)
```

Diffie-Hellman key exchange:

[Notes: in $a = qb + r$, “a\b” is the $q$, and “a\b” is the $r$; “!” means “not”; and “?***” explains the command “***”.]

```plaintext
p=nextprime([huge 30 digit number])
isprime((p-1)/2)
nextgoodprime(p) = while(!isprime((p-1)/2),p=nextprime(p+1));p
nextgoodprime(p)
g=2
znorder(Mod(g,p))
?random
Alice=random(p)
Bob=random(p)
Alice_say = Mod(g,p)^Alice
Bob_say = Mod(g,p)^Bob
```
secret = Alice\_say\^Bob

Bob\_say\^Alice

**RSA Attack 2: factoring a product of “close” primes:**

? n=1692209

? for(i=0,10,print(i," ",sqrt((floor(sqrt(n))+i+1)^2 - n)))