Universität Wien
Prof. Dr. D. Burde

Computeralgebra
— PARI —

---

1. Eine kleine Einführung in PARI-GP. PARI-GP ist ein Computeralgebrasystem (CAS), das hauptsächlich für Berechnungen in der Zahlentheorie entworfen wurde. Wir starten das Programm mit dem Befehl "gp". Dann erscheint die folgende Meldung:

```
PARI/GP is free software, covered by the GNU General Public License, and
comes WITHOUT ANY WARRANTY WHATSOEVER.

Type ? for help, \q to quit.
Type ?12 for how to get moral (and possibly technical) support.

   realprecision = 28 significant digits
   seriesprecision = 16 significant terms
   format = g0.28

parisize = 4000000, primelimit = 500000
```

Wir wollen jetzt ein paar einfache Befehle ausprobieren:

```
? 13*51
%1 = 663
? gcd(360,336)
%2 = 24
? print("gcd(360,336) = ",gcd(360,336))
gcd(360,336) = 24
? 2^(2^8+1)
%4 = 231584178474632390847141970017375815706539969331281128078915168015826259279872
? primes(100)
%6 = [2, 3, 5, 7, 11, 13, 17, 19, 23, 29, 31, 37, 41, 43, 47, 53, 59, 61, 67,
71, 73, 79, 83, 89, 97, 101, 103, 107, 109, 113, 127, 131, 137, 139, 149,
151, 157, 163, 167, 173, 179, 181, 191, 193, 197, 199, 211, 223, 227, 229,
233, 239, 241, 251, 257, 263, 269, 271, 277, 281, 283, 293, 307, 311, 313,
317, 331,337, 347, 349, 353, 359, 367, 373, 379, 383, 389, 397, 401, 409,
419, 421, 431, 433, 439, 443, 449, 457, 461, 463, 467, 479, 487, 491, 499,
503, 509, 521, 523, 541]
? \q
Good bye!
```

primes(n) gibt die ersten n Primzahlen aus. PARI hat standardmäßig schon die ersten 500000 Primzahlen vorberechnet. Der Neustart-Befehl "gp -p 1000000" startet PARI mit 1000000 vorberechneten Primzahlen. Die Funktion prime(n) gibt die n-te Primzahl aus. Mit factor(n) kann man eine ganze Zahl n faktorisieren:

```
? prime(100)
%1 = 541
? factor(160688361)
%2 =
[3 1]
[181 1]
[541 1]
[547 1]
```

Es gibt auch einen Befehl, mit dem man entscheiden kann, ob eine ganze Zahl n prim ist: isprime(n)

```
? isprime(2958270619)
%1 = 0
? factor(2958270619)
%2 =
[1117 2]
[2371 1]
? isprime(650051333)
%3 = 1
```

Hier sind noch weitere Befehle. Mit deriv(f) kann man die Ableitung von f bestimmen.

```
? binomial(120,71)
%1 = 129308059588415138973375479913618 00
? deriv(1/x)
%2 = -1/x^2
? sin(x)
%3 = x - 1/6*x^3 + 1/120*x^5 - 1/5040*x^7 + 1/362880*x^9 - 1/39916800*x^11
+ 1/6227020800*x^13 - 1/1307674368000*x^15 + O(x^16)
? \p 1000
   realprecision = 1001 significant digits (1000 digits displayed)
? Pi
%4 = 3.14159265358979323846264338327950288419716939937510582097494459230781640
628620899862803482534211706798214808651328230664709384460955058223172535940812
848111745028410270193852110555964462294895493038196442881097566593344612847564
823378678316527120190914564856692346034861045432664821339360726024914127372458
700660631558817488152092096282925409171536436789259036001133053054882046652138
414695194151160943305727036575959195309218611738193261179310511854807446237996
274956735188575272489122793818301194912983367336244065664308602139494639522473
719070217986094370277053921717629317675238467481846766940513200056812714526356
082778577134275778960917363717872146844090122495343014654958537105079227968925
892354201995611212902196086403441815981362977477130996051870721134999999837297
804995105973173281609631859502445945534690830264252230825334468503526193118817
101000313783875288658753320838142061717766914730359825349042875546873115956286
```

```
38823537875937519577818577805321712268066130019278766111959092164201 99
```

Mit PARI kann man wie folgt Summen berechnen. Wir wollen die Reihe der reziproken Primzahlwerte bis $p \leq n$ ausrechen, d.h.,

$$\sum_{p \leq n} \frac{1}{p}$$

```
? sum(n=1,100,isprime(n)*1.0/n)
%1 = 1.80281720104887093987161582 5
? sum(n=1,1000,isprime(n)*1.0/n)
%2 = 2.19808012717508754158847678 5
? sum(n=1,10000,isprime(n)*1.0/n)
%3 = 2.48305994723356063609961130 6
```

Die Reihe divergiert bekanntermaßen für $n \to \infty$, aber sehr langsam. Man teste dagegen die folgende Reihe, wobei F_k die k-te Fibonacci-Zahl ist:

$$\sum_{k=1}^{\infty} \frac{1}{F_k} = 1 + 1 + \frac{1}{2} + \frac{1}{3} + \frac{1}{5} + \frac{1}{8} + \cdots +$$

```
? sum(n=1,100,1.0/fibonacci(n))
%8 = 3.35988566624317755316720113029189271796889051337319684864955538153251303
? sum(n=1,1000,1.0/fibonacci(n))
%9 = 3.35988566624317755317201130291892717968890513373196848649555381532513 03
? sum(n=1,10000,1.0/fibonacci(n))
%10 = 3.35988566624317755317201130291892717968890513373196848649555381532513 03
```

Wir vermuten, daß die Reihe gegen eine Konstante, die mit 3.35988566 beginnt, konvergiert. In der Tat, die Reihe konvergiert gegen die Prévost Konstante:

```
3.35988566624317755317201130291892717968890513373196848649555381532513 03
18996683383615416216456790087297045342928853913304136789017100883679 59
13517330771190785803335503325077531875998504871797778970060395645092 15
37589277526567335402403316944179929393461099262625796464765186865944 97
10216558984360881472693249591079473873673378523326877499762727757946 85
36769185419814676687429987673820969139012177220244052081510942649349 51
37454166727895534447077777584780259634076907484741555791042006750152 03
41070533528512979263524206226753756805576195566972084884385440798332 42
92851368070827522662579751188646464096737461572387236295562053612203 02 ...
```

Prévost hatte 1977 bewiesen, daß diese Konstante irrational ist. Vorher hatte Apéry bewiesen, daß $\zeta(3)$ irrational ist:

$$\zeta(s) = \sum_{n=1}^{\infty} \frac{1}{n^s}, \quad \mathrm{Re}(s) > 1$$

```
? \p 100
   realprecision = 105 significant digits (100 digits displayed)
? zeta(3)
%2 = 1.20205690315959428539973816151144999076498629234049888179227155 5
```

```
341838205786313090186455873609335258
```

Kommen wir nochmal zum ggt zweier ganzer Zahlen a, b zurück, der mit gcd(a,b) berechnet wird. (lcm(a,b) berechnet das kgv von a und b). Mit bezout(a,b) kann PARI sogar die lineare diophantische Gleichung $ax + by = (a, b)$ lösen. Wir machen ein Beispiel und rechnen gleich die Probe dazu. PARI benutzt den Euklidischen Algorithmus dazu, und gibt nur eine Lösung aus, auch wenn es mehrere gibt.

```
? gcd(2479,1739)
%4 = 37
? bezout(2479,1739)
%5 = [-7, 10, 37]
? -7*2479+10*1739
%6 = 37
```

Der Befehl funktioniert nicht nur in $\mathbb{Z}$, sondern auch in $\mathbb{Z}[x]$:

```
? gcd(x^2-1,x^2+x+3)
%7 = 1
? gcd(x^4+x^3-x-1,2*x^3+5*x^2+5*x+3)
%8 = x^2 + x + 1
? bezout(x^4+x^3-x-1,2*x^3+5*x^2+5*x+3)
%9 = [4/5, -2/5*x + 3/5, x^2 + x + 1]
```

Das gilt auch für den Befehl factor:

```
? factor(x^5-1)
%10 =
[x - 1 1]
[x^4 + x^3 + x^2 + x + 1 1]
```

Die Teiler einer ganzen Zahl n findet man wie folgt:

```
? divisors(111111)
%15 = [1, 3, 7, 11, 13, 21, 33, 37, 39, 77, 91, 111, 143, 231, 259, 273, 407,
429, 481, 777, 1001, 1221, 1443, 2849, 3003, 3367, 5291, 8547, 10101, 15873,
37037, 111111]
? numdiv(111111)
%16 = 32
? factor(111111)
%17 =
[3 1]
[7 1]
[11 1]
[13 1]
[37 1]
```

Auch Vektoren und Matrizen sind in PARI vorgesehen. Wir berechnen die Inverse von $\begin{pmatrix} 1 & 2 \\ 3 & 4 \end{pmatrix}$:

```
? [1,2,3]+[4,5,6]
%1 = [5, 7, 9]
? [1,2;3,4]^(-1)
%2 =
[-2     1]
[3/2 -1/2]
```

Was ist $2^{100} \mod 81$?

```
? Mod(2,81)^100
%3 = Mod(25, 81)
```

Man kann Polynome auch modulo p faktorisieren:

```
? factor(x^2-5)
%4 =
[x^2 - 5 1]
? factor(Mod(1,11)*(x^2-5))
%5 =
[Mod(1, 11)*x + Mod(4, 11) 1]
[Mod(1, 11)*x + Mod(7, 11) 1]
```

Mit dem Befehl polisirreducible kann man testen, ob ein Polynom irreduzibel über $\mathbb{Q}[x]$ bzw. $\mathbb{F}_p[x]$ ist. Es wird 1 oder 0 ausgegeben. 1 meint irreduzibel.

```
? polisirreducible(x^2-5)
%6 = 1
? polisirreducible(Mod(1,11)*(x^2-5))
%7 = 0
```

Die prime Restklassengruppe $(\mathbb{Z}/n\mathbb{Z})^*$ hat ja bekanntlich $\varphi(n)$ Elemente. Die Funktion $\varphi(n)$ heißt die Eulersche φ-Funktion. Falls die Gruppe $(\mathbb{Z}/n\mathbb{Z})^*$ zyklisch ist, so heißt ein Erzeuger eine *Primitivwurzel modulo n*. Gauß hat bewiesen, daß es genau dann Primitivwurzeln modulo n gibt, wenn $n = 2, 4, p^\ell, 2p^\ell$ gilt für eine Primzahl $p > 2$ und ein $\ell \in \mathbb{N}$.

```
? eulerphi(43)
%8 = 42
? znprimroot(43)
%9 = Mod(3, 43)
? eulerphi(4489)
%10 = 4422
? znprimroot(4489)
%11 = Mod(2, 4489)
? znstar(4489)
%12 = [4422, [4422], [Mod(2, 4489)]]
```

Hierbei gibt znprimroot(n) die kleinste Primitivwurzel modulo n aus, sofern es überhaupt Primitivwurzeln modulo n gibt. Mit znstar(n) wird die Struktur von $(\mathbb{Z}/n\mathbb{Z})^*$ nochmal zusammengefaßt. Der Befehl chinese(Mod(a,m),Mod(b,n)) findet eine Lösung zu den Kongruenzen

$$x \equiv a \mod m, \quad x \equiv b \mod n$$

falls es eine gibt:

```
? chinese(Mod(3,8),Mod(12,45))
%1 = Mod(147, 360)
```

2. Übungen: Der Primzahlsatz. Schreiben Sie ein PARI Programm pnt.gp, das die folgende Funktion berechnet:

$$\pi(x) = \sum_{p \le x} 1$$

Die Summe geht über alle Primzahlen $p \le x$. Der Primzahlsatz, der 1896 unabhängig von Hadamard und de la Vallée Poussin bewiesen wurde, besagt

$$\pi(x) \sim \frac{x}{\log x} \quad \text{für } x \to \infty$$

Berechnen Sie die Zahlen $\pi(1000), \pi(2000), \ldots, \pi(10000)$ und vergleichen Sie die Werte mit der Näherung $x/(\log x - 1)$.

3. Der Dirichletsche Primzahlsatz. Seien a und q zwei teilerfremde ganze Zahlen. Schreiben Sie ein PARI Programm dirichlet.gp, das die folgende Funktion berechnet:

$$f(n) = f(n, a, q) = \sum_{\substack{p \le n \\ p \equiv a(q)}} 1$$

Der Wert $f(n)$ ist gleich der Anzahl der Primzahlen $p \le n$, die in der arithmetischen Folge $qx+a$ vorkommen. Der Satz von Dirichlet besagt, daß $\lim_{n\to\infty} f(n) = \infty$ gilt. Genauer gilt:

$$f(x, q, a) \sim \frac{\pi(x)}{\varphi(q)} \sim \frac{x}{\varphi(q) \log x}, \quad \text{für } x \to \infty$$

Berechnen Sie für $a = 7$ und $q = 16$ die Zahlen $f(1000), f(2000), \ldots, f(10000)$.

4. Faktorisierung mit PARI. Faktorisieren Sie mit PARI die Zahl

$$2^{227} - 1 = 21567957333720511835733612069615704538909715538032457984882888199372 7$$

Je nach Rechnergeschwindigkeit sollten Sie schon einige Minuten auf die Antwort warten. Berechnen Sie die Faktoriserung mit anderen CAS und vergleichen Sie die Zeit. Sollten Sie zu lange warten, dann brechen Sie besser ab, und versuchen Sie es mit $2^{211} - 1$ oder $2^p - 1$ für kleinere Primzahlen p.

Lösung: Es gilt

$$\begin{aligned} 2^{227} - 1 &= 26986333437777017 \\ &\quad \times 799217773820597962649150695086772095345660121688631 \end{aligned}$$

5. PARI Online. Die Homepage von PARI ist zu finden unter

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

William Stein hat einen Online PARI Calculator eingerichtet. Er findet sich unter

`http://modular.fas.harvard.edu/calc`