INTRODUCTION TO PARI

KEITH CONRAD

Introduction

From a terminal window, start PARI by typing `gp`, and exit it with `quit`.

In order to multiply 13 and 51, type `13*51`. The answer is `663`. You must *always* remember to write `*` for multiplication. Try computing `(12+4)(8-3)`, without the `*`.

To define the polynomial $f(x) = x^2+x-1$, type `f(x) = x^2 + x - 1`. Then, to evaluate this $f(x)$ at $x = 3$, enter the command `f(3)`. If, in the course of a PARI session, some polynomial appears on an earlier command line, say line 20, and you want to compute its value at $x = 3$ without typing the polynomial all over again, you can use the `subst` command (substitution) with a reference to the relevant line, namely `subst(%20,x,3)`. Alternatively, if you have already defined some polynomial $f(x)$ and you want to substitute for x a number appearing on line 20, you can enter the PARI command `f(%20)`.

Example. Here is a (somewhat random) PARI session. Can you figure out what each line means?

```
> 3*4
%1 = 12
> f(x) = x^2 - x + 5
> f(3)
%2 = 11
> f(x)^2
%3 = x^4 - 2*x^3 + 11*x^2 - 10*x + 25
> subst(%3,x,3)
%4 = 121
> f(%1)
%5 = 137
> f(%5)
%6 = 18637
```

Here are two URLs with information about PARI. The main PARI web site is

`http://mahery.math.u-psud.fr/~belabas/pari/`.

An online page describing PARI commands is

`http://pari.math.u-bordeaux.fr/dochtml/html.stable/`.

To find the meaning of a PARI command, precede it with `?`. Try `?factor` and `?isprime`.

Division

When a and b are integers, with $b \neq 0$, we can divide a by b to get a quotient and a remainder. The quotient and remainder are computed in PARI as `divrem(a,b)`.

Example: Input `divrem(26,7)` and the answer is `[3,5]`, which means $26 = 7 \cdot \mathbf{3} + \mathbf{5}$. (The output will include a tilde after the vector, which means it is viewed by PARI as a column vector.)

To find quotients alone, we could compute the ratio a/b as a real number and extract the integer part. For instance, let's say we want to know the quotient when 934234 is divided by 2755. If you type `934234/2755`, you might be surprised at the answer: it's exactly what you typed! (Do it.) The reason is that PARI is meant for number theorists, so it will not convert fractions into real number decimals automatically. At most it will convert a non-reduced fraction into reduced form (try `4275/589`), but otherwise it does not simplify. To force PARI to treat rational numbers as real numbers, simply multiply by 1.0 like this: `1.0*934234/2755`. Or enter the numerator or denominator as a real number with a decimal point, *e.g.*, `934234/2755.0`. Either way, the output has integer part `339`.

To output only the quotient with the `divrem` command, you only want the first component of `divrem(a,b)`. This can be done by appending `[1]` after the command: `divrem(a,b)[1]` is just the quotient, and similarly `divrem(a,b)[2]` is just the remainder. Try an example.

There are actually three ways to compute the remainder when a is divided by b in PARI:

`divrem(a,b)[2]` `a%b` `lift(Mod(a,b))`.

Sums, binomial coefficients, and complex numbers

Sums in PARI are entered like this: $\sum_{n=a}^{b} f(n)$ is `sum(n=a,b,f(n))`. (You could use other letters in place of `n`.) To figure out how to compute a sum like $\sum_{d|n} f(d)$ in PARI, enter `?sumdiv` and experiment.

Binomial coefficients occur in the binomial theorem:

$$(x+y)^n = \sum_{k=0}^{n} \binom{n}{k} x^k y^{n-k}.$$

Algebraically,

$$\binom{n}{k} = \frac{n!}{k!(n-k)!} = \frac{n(n-1)(n-2)\cdots(n-k+1)}{k!}.$$

This binomial coefficient is entered in PARI as `binomial(n,k)`. The last expression for $\binom{n}{k}$ has the advantage (by comparison with the middle expression) that it makes sense for negative n. It is the formula PARI uses for binomial coefficients. Input, say, `binomial(-3,7)` and `binomial(-3,8)`, and PARI returns meaningful answers rather than error messages. Try inputting `binomial(9,-5)` and see what PARI does.

To write complex numbers in PARI, type i as `I`, not as `i`. (This frees `i` to be used as a summation index, say.)[1] For instance, `(3+4*I)^2` gives the square of $3+4i$. (Remember, PARI will return an error message if you type `3+4I`; don't forget the `*`.)

The absolute value of a complex number $a+bi$ is $|a+bi| = \sqrt{a^2+b^2}$. This is computed in PARI as `abs(a+b*I)`. In particular, when `a` is a real number in PARI, `abs(a)` is its absolute value.

Modular arithmetic

PARI does modular arithmetic using the command `Mod`. For instance, 2 mod 7 is entered as `Mod(2,7)`. If you try `mod(2,7)`, you'll get an error message. Use the capital M.

Example: To compute 2^{100} mod 81, input `Mod(2,81)^100`. Try `Mod(2^100,81)`, and the answer will be the same. (Do it.)

What is the difference between `Mod(a^d,m)` and `Mod(a,m)^d`? In the first case, PARI computes a^d as an ordinary integer and *then* reduces mod m. In the second case, by making

[1]The number π in PARI is `Pi`, not `pi`. So compute $e^{2\pi i/5}$ as `exp(2*Pi*I/5)`.

the base for the exponentiation an intrinsic "modular" number, `Mod(a,m)`, PARI knows from the start to carry out all operations modulo m. This is more efficient.

Example: Try `Mod(100,242437)^32354543534` and `Mod(100^32354543534,242437)`. The final answers must be the same, but there is a noticeable difference in the run time of these two calculations. Thus, when you work mod m in PARI, it is to your advantage to put (large) exponents outside the `Mod` command.

How do we turn a modular integer into a plain integer? Use `lift`. For instance, `lift(Mod(9,31))` returns the value `9`. Also, `lift(Mod(2343423,31))` has value `9`. The command `lift` returns the least non-negative remainder as an ordinary integer. (So `lift(Mod(a,m))` is the same as `divrem(a,m)[2]` and `a%m`.)

`znorder(Mod(a,m))` computes the order of a mod m. The order is the smallest exponent $n \geq 1$ such that $a^n \equiv 1 \bmod m$. For instance, the input `znorder(Mod(2,23))` has output `11`. That means $2^{11} \equiv 1 \bmod 23$ and 11 is the smallest $n \geq 1$ for which $2^n \equiv 1 \bmod 23$.

`eulerphi(m)` computes the number of invertible integers modulo m.

`znprimroot(m)` will return a generator (also called a primitive root) modulo m if there is one. It is always the smallest possible generator of the invertible numbers modulo m.

`chinese(Mod(a,m),Mod(b,n))` finds the solution to $x \equiv a \bmod m$ and $x \equiv b \bmod n$ when there is one. For instance, `chinese(Mod(3,8),Mod(12,45))` has output `Mod(147,360)`. (If you enter incompatible input, such as `chinese(Mod(1,3),Mod(2,3))`, you'll get an error message that betrays PARI's French origins. Try it.)

gcd, divisors

Compute a gcd using `gcd`.

Example: Compute `gcd(2479,1739)`.

`lcm(a,b)` is, of course, the least common multiple of a and b.

Given integers a and b, PARI can solve $ax+by = (a,b)$ as `bezout(a,b)`. The answer will be a vector triple `[x,y,d]`, where d is the gcd of a and b and $ax + by = d$. (There is not a unique integer solution (x, y); PARI simply gives *one* solution, based on Euclid's algorithm I presume.)

Example: Input `bezout(74,91)` and the answer is `[16,-13,1]`. Check this is correct. What is `bezout(91,74)`? Compute `bezout(2479,1739)` and check the result is correct.

All the positive integer divisors of n (even when $n < 0$) can be found with `divisors(n)`.

Example: Compute `divisors(342)`.

Primes

`primes(n)` is a vector listing the first n primes.
`precprime(x)` is the largest (*i.e.*, preceding) prime $\leq x$ (for real x).
`nextprime(x)` is the first prime $\geq x$ (for real x).
`numdiv(n)` is the number of (positive) divisors of the integer n.

For instance, `precprime(11)` and `nextprime(11)` are both `11`. While the largest prime PARI seems to have stored in the `prime` command is `prime(41561)`, which is 500257 (try inputting `prime(41562)` and see what happens), PARI has no problem using the command `nextprime` beyond this range.

Example: Compute `nextprime(10^10)`.

Sometimes we may want to know how many times a prime p shows up in the prime factorization of n. When $n = 45 = 3^2 \cdot 5$, the prime 3 shows up two times. The relevant command for the exponent of p in the factorization of n is `valuation(n,p)`.

Example: Check `valuation(45,3)` is `2` and `valuation(45,7)` is `0`. Try computing this function for nonprime `p`, such as `valuation(45,15)` and `valuation(45,10)`. What do the answers mean?

Factoring and primality testing

Type `factor(224467774227)` and press the PARI button. The answer comes out as a 3×2 matrix. In each row, the first term is a prime and the second term is its multiplicity as a prime factor. In the factorization of 224467774227, one prime factor appears twice and the two others each appear once. (Actually, there is an exception to this description of the matrix. If $n < 0$, then `factor(n)` will return a factorization matrix whose first row is `[-1  1]`, which indicates the negativity of the number. But -1 is *not* a prime number! Try `factor(-162)`.) PARI will also factor rational numbers. Compute `factor(5/9)` and decide what PARI must be doing when it factors rational numbers.

To decide if a number n is prime, the relevant command is `isprime(n)`, which returns the value 1 if n is prime and 0 if it is not. For instance, compute `isprime(2958270619)`. Then `factor(2958270619)`. You should find there is one prime factor appearing twice and another appearing once. Does PARI think 1 is prime? What about -1? Or -3? Or -11?

Vector and matrix operations

To enter a vector into PARI from scratch, simply use square brackets (*not* parentheses!) with terms separated by commas.

Example: `[3,4,5] + [5,8,9]` has value `[8,12,14]`.

Example:
```
> v = [1,2,3]
%1 = [1,2,3]
> 3*v
%2 = [3,6,9]
```

Example: Try entering `w = (1,2,3)` and see what happens.

When you are dealing with some vector `v` in PARI, you can find out how long it is by computing `length(v)`.

For instance, if you want to know the number of divisors of 342, you can ask PARI for the length of its vector of divisors: `length(divisors(342))` returns the answer `12`, so there are 12 divisors. Of course, the direct command `numdiv(342)` might appeal to you more. But you should know the `length` command is out there for general vectors.

The fifth coordinate of a vector `v` is `v[5]`. (Please note the square brackets. Typing `v(5)`, with parentheses, will not give an answer.)

The general PARI vector command is `vector(N,j,f(j))`, where this means a vector of length N, with j running from 1 to N, and in the j-th coordinate the number $f(j)$ is placed.

To enter a matrix, use commas to separate row entries and semi-colons to start a new row. The beginning and end of a matrix are indicated, as with vectors, by square brackets.

Example: The 3×3 identity matrix is `[1,0,0;0,1,0;0,0,1]`.

Example: Compute the inverse of $\left(\begin{smallmatrix} 3 & 5 \\ 1 & 2 \end{smallmatrix}\right)$ as `[3,5;1,2]^(-1)`.

The (i, j) entry of a matrix `A` is an obvious command: `A[i,j]`. Remember to use square brackets, not parentheses.

The size of matrix `A` is `matsize(A)`, which returns a 2-component vector, the *first* one giving the number of rows and the *second* giving the number of columns. For instance, `matsize(A)[1]` would tell you how many rows `A` has.

Example: When you compute `divrem(26,7)`, the answer `[3,5]` has a tilde after it, which means the answer is interpreted by PARI as a column vector, not as a row vector. Compute `matsize(divrem(26,7))` and see the answer is consistent with this column vector interpretation.

Example: Since `factor(n)` gives a matrix where each row corresponds to a separate prime, the number of prime factors of n can be computed as `matsize(factor(n))[1]`. Compute `matsize(factor(32211990))[1]`. Is this consistent with `factor(32211990)`?

PARI can work with vectors and matrices in modular arithmetic. Just give it a vector or matrix with modular entries. Or, just as rational numbers can be made real by multiplying by `1.0`, you can make a vector or matrix "modular" by writing it in its standard form and then multiplying the whole thing by `Mod(1,m)`, where m is your desired modulus. Thus, $[1, 2, 5]$ as a mod 3 vector could be entered as `Mod(1,3)*[1,2,5]`.

Polynomials

Many PARI calculations you do with integers can also be done with polynomials.

You can factor polynomials with rational coefficients by using the command `factor`. The answer always gives a factorization into irreducible polynomials with *integral* coefficients, and these factors might multiply back to the original polynomial *only* up to an overall scaling factor. To see what this means, do the next example.

Example: Compute `factor(x^2 - 1/9)`. Also try `factor(2*x)`, `factor(2*x^2-4)`, and `factor(2*x^2-8)`. In all cases, compare the product of the irreducible factors in the output with the original polynomial.

Example: Compute `bezout(x^2-1,x^2+x+3)`. Notice that although the inputs are integral polynomials, the outputs have rational coefficients. (The third entry you will see in the output is `1`, which means the polynomials are relatively prime.) Check the answer really works in Bezout's identity: $(x^2-1)a(x)+(x^2+x+3)b(x) = 1$, where PARI tells you the choices for $a(x)$ and $b(x)$.

Example: Compute

```
bezout(x^4 + x^3 - x - 1, 2*x^3 + 5*x^2 + 5*x + 3)
```

and check the answer is correct. (The third entry of the output is not constant, indicating a nontrivial common divisor of the two polynomials.)

If you enter `binomial(x,k)` with a variable `x` rather than a particular number, then PARI interprets this as the binomial coefficient polynomial $\binom{x}{k}$. Try `binomial(x,3)`.

`poldegree(f)` is the degree of the polynomial f. (What is `poldegree(0)`?)

`polcoeff(f,j)` is the coefficient of x^j in f.

In addition to working with integers modulo integers, we can work with polynomials modulo other polynomials, and the `lift` command works there as well.

Example: `lift(Mod(x^3 - 2*x + 6,x^2 - x + 4))` returns value `-5*x + 2`, and indeed $x^3 - 2x + 6 \equiv -5x + 2 \bmod x^2 - x + 4$; check the difference $(x^3 - 2x + 6) - (-5x + 2)$ is divisible by $x^2 - x + 4$.

To turn a polynomial with integer coefficients into a polynomial with modular coefficients, multiply it by `Mod(1,m)` for a modulus m. Thus, the polynomial $x^2 - 5$ with coefficients interpreted mod 11 would be `Mod(1,11)*x^2 - Mod(5,11)` or could be entered as `Mod(1,11)*(x^2 - 5)`.

Example: Unlike the usual integer polynomial $x^2 - 5$, which does not factor further over the integers, the mod 11 polynomial $x^2 - 5$ factors over the integers mod 11. Indeed, type `factor(Mod(1,11)*(x^2-5))` and see what you get.

The polynomial analogue of `isprime` is `polisirreducible`. The output is `1` if the polynomial is irreducible and `0` otherwise. For instance, `polisirreducible(x^2-1)` is `0` while `polisirreducible(x^2+1)` is `1`. These refer to reducibility or irreducibility as polynomials with rational coefficients. The behavior with coefficients modulo p can be different. For instance, $x^2 + 1 = (x + 2)(x - 2)$ if we treat the coefficients as integers modulo 5 (since $1 \equiv -4 \bmod 5$), and if you enter `polisirreducible(Mod(1,5)*(x^2+1))` in PARI the output will be `0`, meaning the polynomial $x^2 + 1$ modulo 5 is not irreducible. Enter `factor(Mod(1,5)*(x^2+1))` to see how PARI exhibits the factorization.

The following table summarizes some PARI commands you have met.

Operation	Command
meaning of command "blah"	`?blah`
value of $f(x)$ at $x = 3$	`f(3)`
set $x = 3$ on line 20	`subst(%20,x,3)`
$\sum_{n=a}^{b} f(n)$	`sum(n=a,b,f(n))`
absolute value $\lvert a + bi \rvert$	`abs(a+b*I)` (can use $b = 0$)
convert to decimal	`*1.0`
making a vector with entries 1,2,3	`[1,2,3]`
$[a(1), \ldots, a(n)]$	`vector(n,j,a(j))`
length of vector v	`length(v)`
enter matrix $\left(\begin{smallmatrix} a & b \\ c & d \end{smallmatrix}\right)$	`[a,b;c,d]`
$\det(A)$	`matdet(A)`
$\binom{n}{k}$	`binomial(n,k)`
factor n	`factor(n)`
list divisors of n	`divisors(n)`
the n-th prime	`prime(n)`
list first n primes	`primes(n)`
is n prime?	`isprime(n)` (1 = yes, 0 = no)
(a, b)	`gcd(a,b)`
$[a, b]$	`lcm(a,b)`
solve $ax + by = (a, b)$ for x, y	`bezout(a,b)`
solve $a = bq + r$ for q, r	`divrem(a,b)`
solve $a = bq + r$ for r	`a%b`, `divrem(a,b)[2]`, or `lift(Mod(a,b))`
$a^b \bmod m$	`Mod(a,m)^b` (faster than `Mod(a^b,m)`)
order of $a \bmod m$	`znorder(Mod(a,m))`
$\varphi(m)$	`eulerphi(m)`
find generator modulo m	`znprimroot(m)`
$x \equiv a \bmod m$, $x \equiv b \bmod n$	`chinese(Mod(a,m),Mod(b,m))`
degree of f	`poldegree(f)`
coefficient of x^j in f	`polcoeff(f,j)`
is $f(x)$ irreducible?	`polisirreducible(f(x))` (1 = yes, 0 = no)