Finite fields & p-adic numbers

Marine Rougnant

Université Marie & Louis Pasteur (Besançon, France)

Algebraic Days of Gabon
École Normale Supérieure (ENS), Libreville, Gabon
10/03/25 – 14/03/25

Polynomials : factorisation

Over $\mathbb{F}_p$:

```
? factormod(pol,2)
% =
[Mod(1, 2)*x 4]

? factormod(pol,5)
% =
[Mod(1, 5)*x^2 + Mod(1, 5)*x + Mod(1, 5) 1]

[Mod(1, 5)*x^2 + Mod(4, 5)*x + Mod(1, 5) 1]
? lift(%)
% =
[  x^2 + x + 1 1]

[x^2 + 4*x + 1 1]
```

Elements in $\mathbb{F}_p$

```
? p = randomprime(2^100)
% = 792438309994299602682608069491
? a = Mod(2,p);
? type(a)
% = "t_INTMOD"
? a^(p-1)
% = Mod(1, 792438309994299602682608069491)
? a.mod == p
% = 1
? lift(a) \\lift to Z
% = 2
```

Elements in $\mathbb{F}_p(x)/(T)$

```
? T = x^2+1;
? b = Mod(x+a, T);
? type(b)
% = "t_POLMOD"
? b.pol
% = Mod(1, 79243...69491)*x + Mod(2,79243...69491)
? b.mod == T
% = 1
```

Finite fields and FFELT's

A finite field with p^n elements is defined by a monic polynomial of degree n over $\mathbb{F}_p$, p prime. There is no finite field structure, finite fields are represented only by elements.

```
? c = ffgen(3^8,'c) \\generator of F_3^8 as a field
% = c
? type(c)
% = "t_FFELT"
? c.p
% = 3
? c.mod \\defining polynomial, lifted to Z
% = c^8 + c^7 + 2*c^6 + c^3 + 2*c^2 + 2*c + 1
? polisirreducible(c.mod*Mod(1,3))
% = 1
? c.f \\degree over F_3
% = 8
```

Finite fields and FFELT's

```
? d = c^9+1
% = 2*c^7 + 2*c^6 + 2*c^4 + 2*c^3 + c + 2
? d.pol
% = 2*c^7 + 2*c^6 + 2*c^4 + 2*c^3 + c + 2
? type(d.pol)
% = "t_POL"
You can directly get an irreducible polynomial with ffinit.
? ffinit(3,5)
% = Mod(1,3)*x^5+Mod(1,3)*x^4+Mod(2,3)*x^3+Mod(1,3)
```

You can also supply your own defining polynomial. We do not check for irreducibility.

```
? ffgen(x^2+Mod(1,3))
% = x
```

You can use many generic functions with finite field elements.

```
? [c,c+1;2*c,1]^-1
% = [...]
? d = random(c) \\random element in the field
% = c^5 + 2*c^4 + c^3 + 2*c^2 + c
? issquare(d)
% = 1
? trace(d) \\over F_3
% = Mod(2, 3)
? norm(d)
% = Mod(1, 3)
? minpoly(d^82)
% = Mod(1,3)*x^4+Mod(1,3)*x^2+Mod(1,3)*x+Mod(1,3)
```

```
? factor(x^5+x^3+c)
% = [x + (2*c^5 + c^4 + 2*c) 1]
[x^2 + (c^7 + 2*c^6 + ... + c^2 + 2) 1]
[x^2 + (2*c^7 + c^6 + ... + 2*c^2 + 1) 1]
? polrootsmod(x^7+x+c)
% = [c^7 + 2*c^6 + c^5 + c^3 + 2*c + 2,
2*c^7 + c^6 + c^2 + 1]~
```

p-adic Numbers

A p-adic number has a unique representation in the form of a p-adic expansion. This representation defines it in PARI/GP. p-adic numbers are expressed as a series with a user-defined p-adic precision e.
Note : The p-adic zero with precision e is given by `O(p^e)`

```
? a=3+O(2^4)
% = 1 + 2 + O(2^4)
? type(a)
% = "t_PADIC"
? b=lift(a)
% = 3
? type(b)
% = "t_INT"
? valuation(a)
% = 0
? valuation(3,2)
% = 0
```

`factorpadic(pol, p, r)` : p-adic factorization of the polynomial pol to precision r
The factors are normalized so that their leading coefficient is a power of p.

```
? factorpadic(x^2 + 9, 3,5)
% =    []~
[(1 + O(3^5))*x^2 + O(3^5)*x + (3^2 + O(3^5)) 1]
? polrootspadic(x^2+9,3,5)
% =
? factorpadic(x^2 + 1, 5,3)
% =
[  (1 + O(5^3))*x + (2 + 5 + 2*5^2 + O(5^3)) 1]
[(1 + O(5^3))*x + (3 + 3*5 + 2*5^2 + O(5^3)) 1]
? polrootspadic(x^2+9,5,3)
% = [1 + 4*5 + 5^2 + O(5^3), 4 + 3*5^2 + O(5^3)]~
```