Mathematics 566 **Homework (due Dec 5th)** A. Hulpke

D&F;9.2: 3,5,9

D&F;9.3: 2,4*

D&F;9.4: 1,2,3*,5,14*,18,19*

D&F;9.5: 5*,6,7*

In the problems that ask to factor a polynomial or to prove its irreducibility, you may use GAP for polynomial and field arithmetic. You may use `IsIrreducible` or `Factors` only if the problem is over $\mathbb{Q}$ or $\mathbb{Z}$ and then only to study factorization over finite fields.

Polynomials in GAP**:** GAP implements a polynomial ring in countably many indeterminates. If R is a ring you can get indeterminates in the following way:

```
gap> x:=X(Rationals,"x");
x
gap> y:=X(Rationals,"y");
y
gap> 5*x+3*y^4*x^2+y;
5*x+y+3*x^2*y^4
```

Note that the variable name and the way the variable is printed (the string) are different things, though it is convenient to use the variable name also as name for printing. (You can also use an integer for the second argument and then get the indeterminate with this internal number, printed by default as `x_i`.) For univariate polynomials the standard operations for euclidean rings are available:

```
gap> QuotientRemainder(p,q);
[ 2-3*x+x^2, -14+21*x-7*x^2 ]
gap> p:=-10+23*x-17*x^2+6*x^3-3*x^4+x^5;
-10+23*x-17*x^2+6*x^3-3*x^4+x^5
gap> q:=x^3+4*x+2;
2+4*x+x^3
gap> Gcd(p,q);
1
gap> GcdRepresentation(p,q);
[ -17/441-2/441*x-11/882*x^2,
  271/882-19/98*x+22/441*x^2-29/882*x^3+11/882*x^4 ]
```

GAP can factor univariate polynomials over finite fields and over the rationals:

```
gap> pol:=-10+23*x-17*x^2+6*x^3-3*x^4+x^5;
-10+23*x-17*x^2+6*x^3-3*x^4+x^5
gap> Factors(PolynomialRing(Rationals),pol);
[ -2+x, -1+x, -1+x, 5+x+x^2 ]
gap> pol:=1+z+z^2+z^3+z^4+z^5;
```

```
Z(2)^0+z+z^2+z^3+z^4+z^5
gap> Factors(PolynomialRing(GF(2)),pol);
[ Z(2)^0+z, Z(2)^0+z+z^2, Z(2)^0+z+z^2 ]
gap> Factors(PolynomialRing(GF(4)),pol);
[ Z(2)^0+z, Z(2^2)+z, Z(2^2)+z, Z(2^2)^2+z, Z(2^2)^2+z ]
```

(`Factors(pol)` alone factorizes over the smallest ring that contains the polynomials coefficients.)
To convert a univariate polynomial with integer coefficients to a polynomial over a finite field, proceed as follows:

```
gap> pol:=x^5+3*x+2;
2+3*x+x^5
gap> cof:=CoefficientsOfUnivariatePolynomial(pol);
[ 2, 3, 0, 0, 0, 1 ]
gap> f:=GF(5);
GF(5)
gap> UnivariatePolynomial(f,cof*One(f));
Z(5)+Z(5)^3*x_1+x_1^5
```

Experiment: Let $pol = x^5 + 3x^4 - 2x^2 + x - 2$ (this is not special – the result will be the same for almost any random polynomial). The following commands will factors pol modulo the first 1000 primes and collect the degree distribution in the variable `cnt` and returns the (rounded) frequencies of the degree distributions multiplied by $|S_5|$.

```
gap> pol:=x^5+3*x^4-2*x^2+x-2;;p:=1;;
gap> cof:=CoefficientsOfUnivariatePolynomial(pol);;
gap> part:=Partitions(5);
[ [ 1, 1, 1, 1, 1 ], [ 2, 1, 1, 1 ], [ 2, 2, 1 ], [ 3, 1, 1 ], [ 3, 2 ],
  [ 4, 1 ], [ 5 ] ]
gap> cnt:=List(part,i->0);
[ 0, 0, 0, 0, 0, 0, 0 ]
gap> for i in [1..1000] do
> p:=NextPrimeInt(p);f:=GF(p);;pred:=UnivariatePolynomial(f,cof*One(f));;
> l:=List(Factors(pred),Degree);Sort(l);
> l:=Position(part,Reversed(l));cnt[l]:=cnt[l]+1;
> od;
gap> List(cnt,i->Int(i/1000*120+1/2));
```

Can you relate the result in any way to the structure of S_5?
Can you formulate a conjecture about the distribution of factors of a random polynomial modulo different primes?