Assignment 5 Question 2 (factorization problems in Z[x])

p1

```
> p1 := x^10-6*x^4+3*x^2+13;
```

$$p1 := x^{10} - 6\,x^4 + 3\,x^2 + 13$$

```
> gcd( diff(p1,x), p1 );
```

$$1$$

So p1 is square-free, and because it is monic, it is also primitive. So we proceed to factor p1 modulo the given primes.

```
> Factor(p1) mod 13;
```

$$(x^2 + 2\,x + 7)\,(x^2 + 11\,x + 7)\,(x^2 + 8)^2\,x^2$$

```
> Factor(p1) mod 17;
```

$$(x^5 + 12\,x^4 + 4\,x^3 + x^2 + 4\,x + 15)\,(x^5 + 5\,x^4 + 4\,x^3 + 16\,x^2 + 4\,x + 2)$$

```
> Factor(p1) mod 19;
```

$$(x^6 + x^4 + 6\,x^2 + 5)\,(x^4 + 18\,x^2 + 14)$$

The prime p=19 tells us that the degrees of the factors over Z must be 4 & 6 or 10. The prime p=17 tells us that the possible degrees are 5 & 5, or 10. Hence, intersecting these possible degrees the only possible degree is 10 hence this polynomial is irreducible over Z. So we are done with p1.

p2

```
> p2 := 8*x^7+12*x^6+22*x^5+25*x^4+84*x^3+110*x^2+54*x+9;
```

$$p2 := 8\,x^7 + 12\,x^6 + 22\,x^5 + 25\,x^4 + 84\,x^3 + 110\,x^2 + 54\,x + 9$$

```
> content(p2,x);
```

$$1$$

```
> gcd( p2, diff(p2,x) );
```

$$4\,x^2 + 4\,x + 1$$

Okay, so p4 is not square-free. We need to first find the square-free factorization.

```
> g1 := gcd(p2,diff(p2,x),'abar');
```

$$g1 := 4\,x^2 + 4\,x + 1$$

```
> h1 := gcd(abar,g1,'f1');
```

$$h1 := 1 + 2\,x$$

```
> f1;
```

$$x^4 + 2\,x^2 + 9$$

```
> g2 := gcd(g1,diff(g1,x),'g1bar');
```

$$g2 := 1 + 2\,x$$

```
> h2 := gcd(g1bar,g2,'f2');
```

$$h2 := 1 + 2\,x$$

```
> f2;
```

$$1$$

Now, clearly the square-free rfactorization of g2 is g2. The square-free factorizatoin of g1 is

```
> f2*g2^2;
```

$$(1 + 2\,x)^2$$

The square-free factorization of p2 is

```
> s2 := f1*f2^2*g2^3;
```

$$s2 := (x^4 + 2\,x^2 + 9)\,(1 + 2\,x)^3$$

```
> expand( p2-s2 );
```

$$0$$

Now, to complete the factorization we need to factor the quartic polynomial f1 which is primitive and square-free.

```
> f13 := Factor(f1) mod 13;
```

$$f13 := (x^2 + 2\,x + 3)\,(x^2 + 11\,x + 3)$$

```
> f17 := Factor(f1) mod 17;
```

$$f17 := (x + 8)\,(x + 6)\,(x + 11)\,(x + 9)$$

```
> f19 := Factor(f1) mod 19;
```

$$f19 := (x + 12)\,(x + 7)\,(x + 14)\,(x + 5)$$

So if f1 factors, it does so into two quadratics. The coefficient bound is $2^3 \cdot 9 = 72$. We can use p=13 and p=19

```
> 13*19 > 2*72;
```

$$144 < 247$$

We need to guess the right pair of linear factors to combine from f19

```
> c13 := x^2+2*x+3;
```

$$c13 := x^2 + 2\,x + 3$$

```
> c19 := Expand( (x+7)*(x+12) ) mod 19;
```

$$c19 := x^2 + 8$$

```
> tf := chrem([c13,c19],[13,19]);
```

$$tf := x^2 + 171\,x + 198$$

```
> tf := mods(tf,13*19);
```

$$tf := x^2 - 76\,x - 49$$

```
> divide(f1,tf);
```

$$\mathit{false}$$

Trying again with x+5 instead of x+12 for the second factor

```
> c19 := Expand( (x+7)*(x+5) ) mod 19;
```

$$c19 := x^2 + 12\,x + 16$$

```
> tf := chrem([c13,c19],[13,19]);
```

$$tf := x^2 + 145\,x + 16$$

```
> tf := mods(tf,13*19);
```

$$tf := x^2 - 102\,x + 16$$

```
> divide(f1,tf);
```

$$\mathit{false}$$

Trying again with x+14 instead of x+12 for the second factor

```
> c19 := Expand( (x+7)*(x+14) ) mod 19;
```

$$c19 := x^2 + 2\,x + 3$$

```
> tf := chrem([c13,c19],[13,19]);
```

$$tf := x^2 + 2\,x + 3$$

```
> divide(f1,tf,'q');
```

$$\mathit{true}$$

Notice that the coefficients are really small, in fact we could have managed with just c13. Hence the factorization is

```
> f1 = c19*q;
```

$$x^4 + 2\,x^2 + 9 = \left(x^2 + 2\,x + 3\right)\left(x^2 - 2\,x + 3\right)$$

p3

Now, the third polynomial is not monic.

```
> p3 := 9*x^7+6*x^6-12*x^5+14*x^4+15*x^3+2*x^2-3*x+14;
```

$$p3 := 9\,x^7 + 6\,x^6 - 12\,x^5 + 14\,x^4 + 15\,x^3 + 2\,x^2 - 3\,x + 14$$

```
> content(p3,x);
```

$$1$$

```
> gcd(p3,diff(p3,x));
```

$$1$$

```
> f13 := Factor(p3) mod 13;
```

$$f13 := 9\left(x^2 + 7\,x + 4\right)\left(x + 6\right)\left(x^4 + 5\,x^3 + 9\,x^2 + 9\,x + 5\right)$$

```
> f17 := Factor(p3) mod 17;
```

$$f17 := 9\left(x + 12\right)\left(x + 13\right)\left(x + 8\right)\left(x^2 + 5\,x + 12\right)\left(x^2 + 8\,x + 6\right)$$

```
> f19 := Factor(p3) mod 19;
```

$$f19 := 9\left(x^3 + 11\,x + 15\right)\left(x^4 + 7\,x^3 + 13\,x^2 + 13\,x + 7\right)$$

We have for p=13, and p=17, the possible degrees of the factors over Z are D = {1,2,3,4,5,6,7}, but for p=19 the possible degrees are D = {3,4,7}. So let's look for a cubic factor and a quartic factor. The Mignotte bound on p3 is 2^6 15 = 32*15 = 480. However, probably, if there is a cubic factor, it's coefficients will be much less than this bound. We'll try that. If we can't find a cubic factor using the primes we have, to prove that p3 is irreducible, we'd need another prime. Modulo 13 we have only one possible choice for the cubic factor, namely

```
> c13 := expand( (x+6)*(x^2+7*x+4) ) mod 13;
```

$$c13 := x^3 + 7\,x + 11$$

Modulo 19 there is only one choice, namely

```
> c19 := (x^3+11*x+15);
```

$$c19 := x^3 + 11\,x + 15$$

Modulo 17 there are many choices. Let's try with just the two primes 13, 19 to see if that's sufficient first.

```
> c := chrem( [c13,c19], [13,19] );
```

$$c := x^3 + 163\,x + 167$$

```
> c := mods(c,13*19);
```

$$c := x^3 - 84\,x - 80$$

```
> divide(p3,c);
```

$$\mathit{false}$$

Okay, this didn't work, but that could be bacause the leading coefficient of the cubic factor is not 1, it could be 3 or 9 - since the leading coefficient of p3 is 9. We don't, in general, want to factor this integer, so let's multiply through by 9

```
> c := mods( 9*c, 13*19 );
```

$$c := 9\,x^3 - 15\,x + 21$$

```
> c := primpart(c,x);
```

$$c := 3\,x^3 - 5\,x + 7$$

```
> divide(p3,c,'q');
```

$$\mathit{true}$$

```
> q;
```

$$3\,x^4 + 2\,x^3 + x^2 + x + 2$$

Thus the factorization is

```
> p3 = c*q;
```

$$9\,x^7 + 6\,x^6 - 12\,x^5 + 14\,x^4 + 15\,x^3 + 2\,x^2 - 3\,x + 14 = \left(3\,x^3 - 5\,x + 7\right)\left(3\,x^4 + 2\,x^3 + x^2 + x + 2\right)$$

Note, if c didn't divide p3, this would not mean that we've proven that there is no cubic factor of p3. Because Mignottes bound gives us 480 but we have to allow for a factor of 2 for positive and negative coefficients, and we also have to allow for multiplying by a factor of 3 too much when trying to attach the leading coefficient, i.e. we need that the product of the primes (= 13*19=247) is greater than 2*3*480 = 2880 which is definitely not the case. Hence we would definitely need to use p=17 as well.

p4

```
> p4 := x^11+2*x^10+3*x^9-10*x^8-x^7-2*x^6+16*x^4+26*x^3+4*x^2+51*
  x-170;
```

$$p4 := x^{11} + 2\,x^{10} + 3\,x^9 - 10\,x^8 - x^7 - 2\,x^6 + 16\,x^4 + 26\,x^3 + 4\,x^2 + 51\,x - 170$$

```
> gcd( p4, diff(p4,x) );
```

$$1$$

So p4 is square-free also, and also primitive. So we proceed to factor p4 modulo the given primes.

```
> f17 := Factor(p4) mod 17;
```

$$f17 := (x^3 + 2\,x^2 + 3\,x + 7)\,(x^6 + 16\,x^2 + 3)\,x^2$$

```
> f19 := Factor(p4) mod 19;
```

$$f19 := (x + 8)\,(x^2 + 13\,x + 13)\,(x^4 + 6\,x^3 + 18\,x^2 + 17\,x + 6)\,(x^4 + 13\,x^3 + 18\,x^2 + 2\,x + 6)$$

```
> f23 := Factor(p4) mod 23;
```

$$f23 := (x^4 + 13\,x^2 + 14)\,(x^2 + 18\,x + 15)\,(x + 7)\,(x^2 + 8)\,(x^2 + 2)$$

Chinese remaindering is not efficient in general because we have to consider too many combinations of factors if there are many primes. That's the main reason by Hensel lifting is needed.

We cannot do Hensel lifting using p=17 because the polynomial is not square-free modulo 17.
The prime p=19 is more attractive than p=23 because there are fewer factors.

```
> p := 19;
```

$$p := 19$$

```
> MonicHenselLift := proc(a,u0,w0,p,B)
  local k,U,W,ek,s,t,ck,sigma,tau;
      `mod` := mods;
      U := Expand(u0) mod p;
      W := Expand(w0) mod p;
      Gcdex( w0, u0, x, 's', 't' ) mod p;
      for k do
          ek := expand(a-U*W);
          if ek=0 then return(U,W); fi;
          if p^k>2*B then return FAIL fi;
          ck := ek/p^k;
          if not type(ck,polynom(integer)) then ERROR("bug") fi;
          sigma := Rem(ck*s,u0,x,'q') mod p;
          tau := Expand(w0*q+ck*t) mod p;
          U := U + sigma*p^k;
          W := W + tau*p^k;
      od;
  end:
```

```
> B := maxnorm(p4)*2^degree(p4,x);
```

$$B := 348160$$

First we will lift all the factors of p4 modulo 19, so u0 = the i'th factor, and w0 is the product of the remaining factors..

```
> found := false:
  for i to 4 while not found do
      u0 := op(i,f19); # the i'th factor
      w0 := Quo(p4,u0,x) mod p;
      R := MonicHenselLift(p4,u0,w0,p,B);
      print(Lifting(u[0]=u0),Result=R);
      if R <> FAIL then found := true fi;
  od:
```

$$\mathit{Lifting}(u_0 = x + 8),\ \mathit{Result} = \mathit{FAIL}$$

$$\mathit{Lifting}(u_0 = x^2 + 13\,x + 13),\ \mathit{Result} = \mathit{FAIL}$$

$$\mathit{Lifting}(u_0 = x^4 + 6\,x^3 + 18\,x^2 + 17\,x + 6),\ \mathit{Result} = \mathit{FAIL}$$

$$\mathit{Lifting}(u_0 = x^4 + 13\,x^3 + 18\,x^2 + 2\,x + 6),\ \mathit{Result} = \mathit{FAIL}$$

None of these work so we now have to consider all pairs of factors from p4 modulo 19.

```
> for i to 4 while not found do
    for j from i+1 to 4 while not found do
      u0 := Expand( op(i,f19)*op(j,f19) ) mod p;
      w0 := Quo(p4,u0,x) mod p;
      R := MonicHenselLift(p4,u0,w0,p,B);
      print(Lifting(u[0]=u0),Result=R);
      if R <> FAIL then found := true fi;
    od
  od:
```

$$\mathit{Lifting}(u_0 = x^3 + 2\,x^2 + 3\,x + 9),\ \mathit{Result} = (x^3 + 2\,x^2 + 3\,x - 10,\ x^8 - x^4 + 3\,x^2 + 17)$$

Got it! The factors are

```
> R;
```

$$x^3 + 2\,x^2 + 3\,x - 10,\ x^8 - x^4 + 3\,x^2 + 17$$

Check

```
> expand( p4-R[1]*R[2] );
```

$$0$$