```
> a1 := x^10-6*x^4+3*x^2+13;
  a2 := 8*x^7+ 12*x^6+ 22*x^5+ 25*x^4+ 84*x^3+ 110*x^2+ 54*x+9;
  a3 := 9*x^7+ 6*x^6-12*x^5+ 14*x^4+ 15*x^3+ 2*x^2-3*x+ 14;
  a4 := 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;
```

$$a1 := x^{10} - 6x^4 + 3x^2 + 13$$

$$a2 := 8x^7 + 12x^6 + 22x^5 + 25x^4 + 84x^3 + 110x^2 + 54x + 9$$

$$a3 := 9x^7 + 6x^6 - 12x^5 + 14x^4 + 15x^3 + 2x^2 - 3x + 14$$

$$a4 := x^{11} + 2x^{10} + 3x^9 - 10x^8 - x^7 - 2x^6 + 16x^4 + 26x^3 + 4x^2 + 51x - 170 \quad \textbf{(1)}$$

```
> SQRFREE := proc(a)
      local g, h, f, a_bar;
      if degree(a) <= 1 then return a; fi;
      g := gcd(a, diff(a, x));
      if g = 1 then return a; fi;
      a_bar := quo(a, g, x);
      h := gcd(g, a_bar);
      f := quo(a_bar, h, x);
      return f, SQRFREE(g);
> end:
> DiophantSolve := proc(a,b,c,x,p)
  local g,sigma,tau,q,s,t;
      g := Gcdex(a,b,x,'s','t') mod p;
      if g <> 1 then error "a and b are not relatively prime!" fi;
      sigma := Rem(c*s,b,x,'q') mod p;
      tau := Expand(c*t+q*a) mod p;
      return (sigma, tau);
  end:
> MignotteBound := proc(f,x)
      local d;
      d := degree(f,x);
      return 2^d*ceil(sqrt(d+1))*maxnorm(f);
  end:
> UniHenselLifting := proc(input_a, x, input_u0, input_w0, p)
  local alpha, a, u0, w0, u, w, B, e_k, c, k, u_k, w_k, s, t, r, q;
  `mod` := mods;
      alpha := lcoeff(input_a, x);
      a := alpha * input_a;
      B := alpha * MignotteBound(input_a, x);
      u0 := alpha * (input_u0 / lcoeff(input_u0, x)) mod p;
      w0 := alpha * (input_w0 / lcoeff(input_w0, x)) mod p;
      print(a mod p, u0 mod p, w0 mod p);
      print(expand(a-u0*w0) mod p);
      k := 1;
      u := u0; w := w0;
      s, t := DiophantSolve(w, u, 1, x, p);

      while (a - u*w) <> 0 do
          e_k := expand(a - u*w);
          if e_k = 0 then return (primpart(u), primpart(w)); fi;
          if p^k > 2*B then return FAIL; fi;
          c := (e_k / (p^k)) mod p;
          u_k, w_k := DiophantSolve(w0, u0, c, x, p);
          u := u + u_k * (p^k);
```

```
        w := w + w_k * (p^k);
        u := expand(alpha * u / lcoeff(u, x)) mod (p^(k+1));
        w := expand(alpha * w / lcoeff(w, x)) mod (p^(k+1));
        k := k + 1;
    od:
end:
```

```
> P := [13, 17, 19, 23];
```

$$P := [13, 17, 19, 23] \tag{2}$$

```
> `mod` := mods;
```

$$mod := mods \tag{3}$$

```
> factor_in_p := proc(sqrf, P)
    local f, p, degrees, add_f, fmodp;
    for f in sqrf do
        if degree(f) <= 1 then next; fi;
        for p in P do
            fmodp := Factor(f) mod p;
            print(fmodp, p);
            degrees := map(degree, convert(fmodp, list));
            degrees := combinat[choose](degrees);
            add_f := `+`@op:
            print(ListTools[MakeUnique](map(add_f, degrees)));
        od;
    od;
end:
```

```
> factor(a1);
a1;
a1_SQRF := [SQRFREE(a1)];
factor_in_p(a1_SQRF, P);
```

$$x^{10} - 6x^4 + 3x^2 + 13$$

$$x^{10} - 6x^4 + 3x^2 + 13$$

$$a1\_SQRF := [x^{10} - 6x^4 + 3x^2 + 13]$$

$$(x^2 - 2x - 6)\, x^2\, (x^2 - 5)^2\, (x^2 + 2x - 6), 13$$

$$[0, 2, 4, 6, 8, 10]$$

$$(x^5 + 5x^4 + 4x^3 - x^2 + 4x + 2)\, (x^5 - 5x^4 + 4x^3 + x^2 + 4x - 2), 17$$

$$[0, 5, 10]$$

$$(x^4 - x^2 - 5)\, (x^6 + x^4 + 6x^2 + 5), 19$$

$$[0, 4, 6, 10]$$

$$(x^6 - 7x^4 - 5x^2 - 7)\, (x^2 - 6x + 10)\, (x^2 + 6x + 10), 23$$

$$[0, 2, 6, 8, 4, 10] \tag{4}$$

```
> a2;
a2_SQRF := [SQRFREE(a2)];
```

$$8x^7 + 12x^6 + 22x^5 + 25x^4 + 84x^3 + 110x^2 + 54x + 9$$

$$a2\_SQRF := [x^4 + 2x^2 + 9, 1, 1 + 2x] \tag{5}$$

```
> factor(a2);
factor_in_p(a2_SQRF, P);
```

$$(x^2+2x+3)\ (x^2-2x+3)\ (1+2x)^3$$
$$(x^2+2x+3)\ (x^2-2x+3), 13$$
$$[0, 2, 4]$$
$$(x-8)\ (x-6)\ (x+8)\ (x+6), 17$$
$$[0, 1, 2, 3, 4]$$
$$(x+5)\ (x-7)\ (x-5)\ (x+7), 19$$
$$[0, 1, 2, 3, 4]$$
$$(x^2+2x+3)\ (x^2-2x+3), 23$$
$$[0, 2, 4] \quad \textbf{(6)}$$

```
> chrem([x^2+2*x+3, x^2+2*x+3], [13, 23]);
  quo(a2, x^2+2*x+3, x, 'r');
  r;
```

$$x^2+2x+3$$
$$8x^5-4x^4+6x^3+25x^2+16x+3$$
$$0 \quad \textbf{(7)}$$

```
> a3;
  a3_SQRF := [SQRFREE(a3)];
```

$$9x^7+6x^6-12x^5+14x^4+15x^3+2x^2-3x+14$$
$$a3\_SQRF := [9x^7+6x^6-12x^5+14x^4+15x^3+2x^2-3x+14] \quad \textbf{(8)}$$

```
> factor_in_p(a3_SQRF, P);
```

$$-4\ (x^2-6x+4)\ (x^4+5x^3-4x^2-4x+5)\ (x+6), 13$$
$$[0, 2, 4, 6, 1, 3, 5, 7]$$
$$-8\ (x-4)\ (x^2+8x+6)\ (x^2+5x-5)\ (x-5)\ (x+8), 17$$
$$[0, 1, 2, 3, 4, 5, 6, 7]$$
$$9\ (x^3-8x-4)\ (x^4+7x^3-6x^2-6x+7), 19$$
$$[0, 3, 4, 7]$$
$$9\ (x^3+x^2-7x-2)\ (x^3+6x+10)\ (x-8), 23$$
$$[0, 3, 6, 1, 4, 7] \quad \textbf{(9)}$$

```
> primpart(chrem([9*(x^4+5*x^3-4*x^2-4*x+5), 9*(x^4+7*x^3-6*x^2-6*
  x+7)], [13, 19]), x);
```

$$3x^4+2x^3+x^2+x+2 \quad \textbf{(10)}$$

```
> quo(a3, 3*x^4+2*x^3+x^2+x+2, x, 'r');
  r;
```

$$3x^3-5x+7$$
$$0 \quad \textbf{(11)}$$

```
> expand((3*x^4+2*x^3+x^2+x+2) * (3*x^3-5*x+7));
```

$$9x^7+6x^6-12x^5+14x^4+15x^3+2x^2-3x+14 \quad \textbf{(12)}$$

```
> a4;
  a4_SQRF := [SQRFREE(a4)];
```

$$x^{11}+2x^{10}+3x^9-10x^8-x^7-2x^6+16x^4+26x^3+4x^2+51x-170$$
$$a4\_SQRF := [x^{11}+2x^{10}+3x^9-10x^8-x^7-2x^6+16x^4+26x^3+4x^2+51x-170] \quad \textbf{(13)}$$

```
> factor_in_p(a4_SQRF, P);
```

$$(x^4 - 6x^3 + 5x^2 - 4x - 2)\,(x^3 + 2x^2 + 3x + 3)\,(x^4 + 6x^3 + 5x^2 + 4x - 2),\ 13$$

$$[0, 4, 8, 3, 7, 11]$$

$$x^2\,(x^3 + 2x^2 + 3x + 7)\,(x^6 - x^2 + 3),\ 17$$

$$[0, 2, 3, 5, 6, 8, 9, 11]$$

$$(x^4 + 6x^3 - x^2 - 2x + 6)\,(x^2 - 6x - 6)\,(x^4 - 6x^3 - x^2 + 2x + 6)\,(x + 8),\ 19$$

$$[0, 4, 8, 2, 6, 10, 1, 5, 9, 3, 7, 11]$$

$$(x^4 - 10x^2 - 9)\,(x^2 + 8)\,(x^2 - 5x - 8)\,(x^2 + 2)\,(x + 7),\ 23$$

$$[0, 2, 4, 6, 8, 10, 1, 3, 5, 7, 9, 11] \quad \textbf{(14)}$$

```
> u0 := x^3+2*x^2+3*x+7; w0 := Quo(a4, u0, x) mod 17;
```

$$u0 := x^3 + 2x^2 + 3x + 7$$

$$w0 := x^8 - x^4 + 3x^2 \quad \textbf{(15)}$$

```
> UniHenselLifting(a4, x, u0, w0, 17);
```

$$x^{11} + 2x^{10} + 3x^9 + 7x^8 - x^7 - 2x^6 - x^4 - 8x^3 + 4x^2,\ x^3 + 2x^2 + 3x + 7,\ x^8 - x^4 + 3x^2$$

$$0$$

$$x^3 + 2x^2 + 3x - 10,\ x^8 - x^4 + 3x^2 + 17 \quad \textbf{(16)}$$

```
> factor(a4);
```

$$(x^3 + 2x^2 + 3x - 10)\,(x^8 - x^4 + 3x^2 + 17) \quad \textbf{(17)}$$