Assignment 5 Question 1 (factorization in Zp).

```
> restart;
  p := 11; `mod` := mods;
```

$$p := 11$$

$$mod := mods$$

```
> a1 := x^4+8*x^2+6*x+8;
```

$$a1 := x^4 + 8\,x^2 + 6\,x + 8$$

```
> Gcd(a1, diff(a1,x)) mod p;
```

$$1$$

The polynomial is square-free so there are no repeated factors so we use the Cantor-Zassenhaus method.

```
> g := Gcd( a1, x^p-x ) mod p;
```

$$g := x^4 - 3\,x^2 - 5\,x - 3$$

So g is a product of 4 linear factors. Splitting

```
> h := Gcd( g, x^( (p-1)/2 ) - 1 ) mod p;
```

$$h := x + 2$$

```
> f1 := h;
```

$$f1 := x + 2$$

```
> g := Quo( g, h, x ) mod p;
```

$$g := x^3 - 2\,x^2 + x + 4$$

It remains to split g which is a product of three linear factors.

```
> h := Gcd( g, (x+1)^((p-1)/2)-1 ) mod p;
```

$$h := x + 3$$

```
> f2 := h;
```

$$f2 := x + 3$$

```
> g := Quo( g, f2, x ) mod p;
```

$$g := x^2 - 5\,x + 5$$

```
> h := Gcd( g, (x-1)^5-1 ) mod p;
```

$$h := x^2 - 5\,x + 5$$

```
> h := Gcd( g, (x+2)^5-1 ) mod p;
```

$$h := x + 1$$

```
> f3 := x+1;
```

$$f3 := x + 1$$

```
> f4 := Quo( g, f3, x ) mod p;
```

$$f4 := x + 5$$

We are done. The factorization is

```
> a1 = f1*f2*f3*f4;
```

$$x^4+8x^2+6x+8=(x+2)(x+3)(x+1)(x+5)$$

Problem 2

```
> a2 := x^6+3*x^5-x^4+2*x^3-3*x+3;
```

$$a2 := x^6+3x^5-x^4+2x^3-3x+3$$

```
> Gcd(a2, diff(a2,x)) mod p;
```

$$1$$

```
> g := Gcd( a2, x^p-x ) mod p;
```

$$g := x+2$$

So a2 has one linear factor.

```
> f1 := g;
```

$$f1 := x+2$$

```
> h := Quo(a2,g,x) mod p;
```

$$h := x^5+x^4-3x^3-3x^2-5x-4$$

```
> g := Gcd( h, x^(p^2) - x ) mod p;
```

$$g := 1$$

If h has no linear and quadratic factors of a, there cannot be any cubics, so we can stop. We have

```
> a2 = f1*h;
```

$$x^6+3x^5-x^4+2x^3-3x+3=(x+2)\left(x^5+x^4-3x^3-3x^2-5x-4\right)$$

Problem 3

```
> a3 := x^8+x^7+x^6+2*x^4+5*x^3+2*x^2+8;
```

$$a3 := x^8+x^7+x^6+2x^4+5x^3+2x^2+8$$

```
> Gcd(a3,diff(a3,x)) mod p;
```

$$1$$

This time I will use Powmod.

```
> w := Powmod(x,p,a3,x) mod p;
```

$$w := -3x^7-4x^6+3x^5-2x^3-5x^2+3$$

```
> g := Gcd( a3, w-x ) mod p;
```

$$g := 1$$

```
> w := Powmod(w,p,a3,x) mod p;
```

$$w := -5x^7-2x^6-3x^5-3x^3+2x^2+5x+4$$

```
> g := Gcd( a3, w-x ) mod p;
```

$$g := x^2+x+1$$

So a3 has one irreducible quadratic factor.

```
> f1 := g;
```

$$f1 := x^2+x+1$$

```
> h := Quo(a3,g,x) mod p;
```

$$h := x^6 + 2\,x^2 + 3\,x - 3$$

Now the next computation of gcd(h, $x^{p^3} - x$) with p=11 is quite large so we'll do it more carefully.

```
> w := Powmod( w, p, h, x ) mod p;
```

$$w := x$$

```
> g := Gcd( h, w-x ) mod p;
```

$$g := x^6 + 2\,x^2 + 3\,x - 3$$

Therefore we have two cubic factors (and nothing left). To split them we try

```
> RandomZ11 := rand(p):
> r := x^3+add( RandomZ11()*x^i, i=0..2 );
```

$$r := x^3 + 5\,x^2 + 9\,x + 6$$

```
> w := Powmod( r, (p^3-1)/2, g, x ) mod p;
```

$$w := 5\,x^5 - x^4 - 2\,x^3 - x + 2$$

```
> h := Gcd( g, w-1 ) mod p;
```

$$h := x^3 - 3\,x - 5$$

```
> f2 := h;
```

$$f2 := x^3 - 3\,x - 5$$

```
> f3 := Quo(g,h,x) mod p;
```

$$f3 := x^3 + 3\,x + 5$$

So the factorization of a3 is

```
> f1*f2*f3;
```

$$(x^2 + x + 1)\,(x^3 - 3\,x - 5)\,(x^3 + 3\,x + 5)$$

```
> Expand(a3-f1*f2*f3) mod p;
```

$$0$$

For the second part of the question we need to factor the polynomial

```
> x^2-a;
```

$$x^2 - a$$

modulo the following prime p

```
> p := 10^20+129;
```

$$p := 100000000000000000129$$

for a = 3, 5 and 7. We cannot compute gcd($x^2 - a, x^p - x$) mod p without using binary powering with remainder this time. We compute the remainder of x^p divided $h(x) = x^2 - a$ using powmod.

```
> for a in [3,5,7] do
      h := x^2-a;
      w := Powmod( x, p, h, x ) mod p;
      g := Gcd(h,w-x) mod p;
```

```
        print( x^2-a, degree(g,x) );
  od:
```

$$x^2-3,\ 2$$

$$x^2-5,\ 2$$

$$x^2-7,\ 0$$

Since for a=3 and a=5 the degree of the gcd is 2, we have square roots for a=3 and a=5.

```
> a := 3; h := x^2-a;
  for alpha do
      w := Powmod( x+alpha, (p-1)/2, h, x ) mod p;
      g := Gcd( h, w-1 ) mod p;
      print('alpha' = alpha, deg=degree(g,x) );
      if degree(g,x) = 1 then S := -coeff(g,x,0); break fi;
  od:
```

$$a := 3$$

$$h := x^2-3$$

$$\alpha = 1,\ deg = 0$$

$$\alpha = 2,\ deg = 2$$

$$\alpha = 3,\ deg = 0$$

$$\alpha = 4,\ deg = 1$$

```
> S;
```

$$2828774567150416084 8$$

```
> a - S^2 mod p;
```

$$0$$

```
> a := 5; h := x^2-a;
  for alpha from 1 do
      w := Powmod( x+alpha, (p-1)/2, h, x ) mod p;
      g := Gcd( h, w-1 ) mod p;
      print('alpha' = alpha, deg=degree(g,x) );
      if degree(g,x) = 1 then S := -coeff(g,x,0); break fi;
  od:
```

$$a := 5$$

$$h := x^2-5$$

$$\alpha = 1,\ deg = 0$$

$$\alpha = 2,\ deg = 0$$

$$\alpha = 3,\ deg = 2$$

$$\alpha = 4,\ deg = 0$$

$$\alpha = 5,\ deg = 0$$

$$\alpha = 6,\ deg = 1$$

```
> S;
```

$$14339274750131571137$$

```
> 5-S^2 mod p;
```

$$0$$

The cost of computing $gcd(x^2 - a, x^p \textbf{ mod } a - x)$ is $\mathrm{O}(\log_2 p\, d^2)$ for $d = 2$ so $\mathrm{O}(\log_2 p)$ aritmetic operations in Zp. For the split the expected number of tries is 2. So this cost is also $\mathrm{O}(\log_2 p)$ arithmetic operations in $\mathbb{Z}_p$.