Assignment 3 Questions 1, 2, 3, 4

Queston 1 (a)

```
> r := n-1;
  re := M(n) = M(n-1)+r+(r-1)*(r^2+r)+sum(sum(1,j=0..r-k),k=1..r);
```

$$r := n - 1$$

$$re := M(n) = M(n-1) + \frac{n}{2} - 1 + (n-2)\left((n-1)^2 + n - 1\right) + \frac{n^2}{2} \quad \textbf{(1)}$$

```
> expand( rsolve( {re,M(1)=0}, M(n) ) );
```

$$\frac{1}{4} n^2 - \frac{1}{6} n + \frac{1}{4} n^4 - \frac{1}{3} n^3 \quad \textbf{(2)}$$

So its O(n^4)

```
> re := T(n)=2*T(n/2)+n/2;
```

$$re := T(n) = 2\,T\left(\frac{n}{2}\right) + \frac{n}{2} \quad \textbf{(3)}$$

```
> rsolve( {re,T(1)=0}, T(n) );
```

$$\frac{n \ln(n)}{2 \ln(2)} \quad \textbf{(4)}$$

```
> n*log[2](n);
```

$$\frac{n \ln(n)}{\ln(2)} \quad \textbf{(5)}$$

Question 2 (a)

```
> p := 3*2^5+1;
```

$$p := 97 \quad \textbf{(6)}$$

```
> alpha := numtheory[primroot](p);
```

$$\alpha := 5 \quad \textbf{(7)}$$

```
> omega8 := alpha ^ iquo(p-1,8) mod p;
```

$$\omega 8 := 64 \quad \textbf{(8)}$$

```
> seq( omega8 &^ i mod p, i=0..8 );
```

$$1, 64, 22, 50, 96, 33, 75, 47, 1 \quad \textbf{(9)}$$

Question 3(a)

```
> FFT1 := proc(n::posint,
               A::Array,k::integer,
               W::Array,l::integer,p,
               T::Array,j::integer)
  # k is the index (initially 0) into where A starts
  # l is the index (initially 0) into W where the powers of omega
  start
  # j is the index (initially 0) into where T starts
  local n2,i,s,t;
     if n=1 then return; fi;
     n2 := n/2;
```

```
    for i from 0 to n2-1 do
        T[j+i] := A[k+2*i];
        T[j+i+n2] := A[k+2*i+1];
    od;
    FFT1(n2,T,j,   W,l+n2,p,A,k);
    FFT1(n2,T,j+n2,W,l+n2,p,A,k+n2);
    for i from 0 to n2-1 do
        s := T[j+i];
        t := W[l+i]*T[j+i+n2] mod p;
        A[k+i] := s+t mod p;
        A[k+i+n2] := s-t mod p;
    od;
    return;
end:
```

```
> p := 97;
  n := 8;
  alpha := numtheory[primroot](p);
  omega8 := alpha^iquo(p-1,n) mod p;
  omega8inv := 1/omega8 mod p;
  seq( omega8inv^i mod p, i=0..n );
```

$$p := 97$$

$$n := 8$$

$$\alpha := 5$$

$$\omega 8 := 64$$

$$omega8inv := 47$$

$$1, 47, 75, 33, 96, 50, 22, 64, 1 \quad \textbf{(10)}$$

```
> W := Array(0..n-1):
  for i from 0 to 3 do W[i] := omega8^i mod p; od:
  W[4] := 1: W[5] := W[2]: W[6] := 1:
  W;
  Winv := Array(0..n-1):
  for i from 0 to 3 do Winv[i] := omega8inv^i mod p; od:
  Winv[4] := 1: Winv[5] := Winv[2]: Winv[6] := 1:
  Winv;
```

$$[1, 64, 22, 50, 1, 22, 1, 0, \cdots 0 .. 7 \text{ Array}]$$

$$[1, 47, 75, 33, 1, 75, 1, 0, \cdots 0 .. 7 \text{ Array}] \quad \textbf{(11)}$$

```
> A := Array(0..n-1,[1,2,3,4,3,2,1,0]);
  a := add(A[i]*x^i,i=0..n-1);
  p := 97;
  T := Array(0..n-1);
  FFT1(n,A,0,W,0,p,T,0);
```

$$A := [1, 2, 3, 4, 3, 2, 1, 0, \cdots 0 .. 7 \text{ Array}]$$

$$a := x^6 + 2x^5 + 3x^4 + 4x^3 + 3x^2 + 2x + 1$$

$$p := 97$$

$$T := [0, 0, 0, 0, 0, 0, 0, 0, \cdots \ 0 .. 7 \text{ Array}] \quad \textbf{(12)}$$

```
> A;
  seq( eval(a,x=omega8^i mod p) mod p, i=0..n-1 );
```

$$[16, 48, 0, 16, 0, 36, 0, 86, \cdots \ 0 .. 7 \text{ Array}]$$

$$16, 48, 0, 16, 0, 36, 0, 86 \quad \textbf{(13)}$$

We will apply the inverse transform to get back the original A

```
> FFT1(n,A,0,Winv,0,p,T,0);
> A;
```

$$[8, 16, 24, 32, 24, 16, 8, 0, \cdots \ 0 .. 7 \text{ Array}] \quad \textbf{(14)}$$

```
> A/n mod p;
```

$$[1, 2, 3, 4, 3, 2, 1, 0, \cdots \ 0 .. 7 \text{ Array}] \quad \textbf{(15)}$$

Question 3 (b)

```
> a := -x^3+3*x+1;
```

$$a := -x^3 + 3\,x + 1 \quad \textbf{(16)}$$

```
> b := 2*x^4-3*x^3-2*x^2+x+1;
```

$$b := 2\,x^4 - 3\,x^3 - 2\,x^2 + x + 1 \quad \textbf{(17)}$$

```
> A := Array(0..n-1):
  for i from 0 to degree(a,x) do A[i] := coeff(a,x,i) od:
  A;
```

$$[1, 3, 0, -1, 0, 0, 0, 0, \cdots \ 0 .. 7 \text{ Array}] \quad \textbf{(18)}$$

```
> B := Array(0..n-1):
  for i from 0 to degree(b,x) do B[i] := coeff(b,x,i) od:
  B;
```

$$[1, 1, -2, -3, 2, 0, 0, 0, \cdots \ 0 .. 7 \text{ Array}] \quad \textbf{(19)}$$

```
> FFT1(n,A,0,W,0,p,T,0):
> FFT1(n,B,0,W,0,p,T,0):
> C := Array(0..n-1):
  for i from 0 to n-1 do C[i] := A[i]*B[i] mod p od:
> FFT1(n,C,0,Winv,0,p,T,0); # inverse transform
> ninv := 1/n mod p;
  for i from 0 to 7 do C[i] := ninv*C[i] mod p od:
```

$$ninv := 85 \quad \textbf{(20)}$$

```
> add( C[i]*x^i, i=0..7 );
```

$$95\,x^7 + 3\,x^6 + 8\,x^5 + 89\,x^4 + 87\,x^3 + x^2 + 4\,x + 1 \quad \textbf{(21)}$$

```
> expand(a*b) mod p;
```

$$95\,x^7 + 3\,x^6 + 8\,x^5 + 89\,x^4 + 87\,x^3 + x^2 + 4\,x + 1 \quad \textbf{(22)}$$

Question 4

I found this easy compared with getting the FFT to work.

```
> FastNewton := proc(f,x,n,p) local a0,m,g,yk,y2k;
      if n=1 then
```

```
        a0 := coeff(f,x,0);
        if a0=0 then error "inverse does not exist" fi;
        return 1/a0 mod p;
     fi;
     m := iquo(n+1,2);
     g := convert(taylor(f,x,m+1),polynom); # g = f mod x^m
     yk := FastNewton(g,x,m,p);
     if degree(f,x)>=n then g := convert(taylor(f,x,n),polynom) else
 g := f fi;
     y2k := 2*yk-Expand(g*yk^2) mod p;
     convert(taylor(y2k,x,n),polynom);
 end:
```

```
> p := 11;
  f := 3+x+4*x^3+x^5;
```

$$p := 11$$

$$f := x^5 + 4\,x^3 + x + 3 \qquad \textbf{(23)}$$

```
> n := 6;
  b := FastNewton(f,x,n,p);
```

$$n := 6$$

$$b := 10\,x^5 + 7\,x^4 + 10\,x^3 + 9\,x^2 + 6\,x + 4 \qquad \textbf{(24)}$$

```
> Rem(b*f,x^n,x) mod p;
```

$$1 \qquad \textbf{(25)}$$

Here are two timings tests to show that with Maple's fast multiplication (the Expand call) we have a fast inverse

```
> f := Randpoly(10000,x) mod p:
```

```
> st := time():
  b := FastNewton(f,x,10001,p):
  time()-st;
```

$$0.030 \qquad \textbf{(26)}$$

```
> f := Expand(f^2) mod p:
```

```
> st := time():
  b := FastNewton(f,x,20001,p):
  time()-st;
```

$$0.058 \qquad \textbf{(27)}$$

```
> Rem(f*b,x^20001,x) mod p;
```

$$1 \qquad \textbf{(28)}$$