Assignment 3 Question 1 (on the FFT)

Part (a)

```
> p := 97;
```

$$p := 97$$

```
> ifactor(p-1);
```

$$(2)^5\,(3)$$

```
> primedivisors := [2,3];
```

$$primedivisors := [2, 3]$$

```
> alpha := 5;
```

$$\alpha := 5$$

```
> for q in primedivisors do modp( alpha^((p-1)/q), p ); od;
```

$$96$$

$$35$$

Neither power is 1 so $\alpha = 5$ is a primitive element.

```
> w := alpha^((p-1)/8) mod p;
```

$$w := -33$$

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

$$mod := mods$$

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

$$1, -33, 22, -47, -1, 33, -22, 47, 1$$

Part (b)

What is the Fourier transform of the polynomial $a(x) = 1 + x + x^2 + \ldots + x^{n-1}$. Well let's just try it

```
> a := add( x^i, i=0..7 );
```

$$a := x^7 + x^6 + x^5 + x^4 + x^3 + x^2 + x + 1$$

```
> F := [seq( eval(a,x=w^i) mod p, i=0..7 )];
```

$$F := [8, 0, 0, 0, 0, 0, 0, 0]$$

So the answer must be $[n, 0, 0, 0, \ldots 0]$. Obviously, for $\omega = 1$ we have $a(1) = n$. Recall that for $x \neq 1$, we have

$1 + x + x^2 + \ldots + x^{n-1} = \frac{(1 - x^n)}{1 - x}$ which Maple seems to "know".

```
> simplify( sum(x^i,i=0..n-1)*(1-x) );
```

$$-x^n + 1$$

So that the Fourier transform entry $F_i = \frac{(1 - \omega^{i \cdot n})}{(1 - \omega^i)}$ but the numerator is 0.

Part (c)

$M(n) = 2 \cdot M\left(\frac{n}{2}\right) + \frac{n}{2}$ hence

$2 \cdot M\left(\frac{n}{2}\right) = 4 \cdot M\left(\frac{n}{4}\right) + \frac{2 \cdot n}{4} = 4 \cdot M\left(\frac{n}{4}\right) + \frac{n}{2}$ hence

$4 \cdot M\left(\frac{n}{4}\right) = 4 \cdot M\left(\frac{n}{8}\right) + \frac{n}{2}$ hence ... hence

$2^{k-1} \cdot M\left(\frac{n}{2^k}\right) = 2^{k-1} \cdot M\left(\frac{n}{2^k}\right) + \frac{n}{2}$ and finally

$2^k \cdot M\left(\frac{n}{2^k}\right) = 2^k \cdot M(1) = 0.$

Adding both sides and cancelling equal terms we have $k = \log_2(n)$ lots of $\frac{n}{2}$ on the right and $M(n)$ on the left that don't cancel. Hence $M(n) = \frac{n}{2} \cdot \log_2(n)$.

Part (d)

Katatsuba recurrence

```
> simplify( rsolve( {T(1)=d, T(n)=3*T(n/2)+c*n}, T(n) ) );
```

$$(2\,c + d)\, n^{\frac{\ln(3)}{\ln(2)}} - 2\,c\,n$$

Optimized FFT recurrence (see code below)

```
> simplify( rsolve( {T(1)=0, T(n)=2*T(n/2)+n/2}, T(n) ) );
```

$$\frac{1}{2}\,\frac{n \ln(n)}{\ln(2)}$$

Gaussian elimination recurrence

```
> simplify( rsolve( {T(1)=0, T(n)=T(n-1)+(n-1)^2}, T(n) ) );
```

$$\frac{1}{6}\,n + \frac{1}{3}\,n^3 - \frac{1}{2}\,n^2$$

Part (e)

```
> unprotect(FFT):
  FFT := proc(n,A,p,w)
  local n2,B,C,i,wi,T;
    if n=1 then return; fi;
    n2 := n/2;
    B := Array(0..n2-1);
    C := Array(0..n2-1);
    for i from 0 to n2-1 do B[i] := A[2*i]; C[i] := A[2*i+1]; od;
    FFT(n2,B,p,w^2 mod p);
    FFT(n2,C,p,w^2 mod p);
    wi := 1;
    for i from 0 to n2-1 do
```

```
      T := wi*C[i] mod p;
      A[i] := B[i] + T mod p;
      A[n2+i] := B[i] - T mod p;
      wi := wi*w mod p;
    od;
    return;
  end:
> A := Array(0..7,[1,2,3,4,3,2,1,0]):
> FFT(8,A,p,w);
> convert(A,list);
```

$$[16, 48, 0, 16, 0, 36, 0, -11]$$

```
> FFT(8,A,p,1/w mod p);
> convert(A,list);
```

$$[8, 16, 24, 32, 24, 16, 8, 0]$$

```
> ninv := 1/8 mod p;
```

$$ninv := -12$$

```
> for i from 0 to 7 do A[i] := ninv*A[i] mod p; od:
> convert(A,list);
```

$$[1, 2, 3, 4, 3, 2, 1, 0]$$

Here is a version which stores the powers of ω in an array W and accesses them as needed.

```
> W := Array(0..3,[1,w,w^2,w^3] mod p):
> convert(W,list);
```

$$[1, -33, 22, -47]$$

```
> FFT := proc(n,A,p,W,stride)
  local n2,B,C,i,wi,temp;
    if n=1 then return; fi;
    n2 := n/2;
    B := Array(0..n2-1);
    C := Array(0..n2-1);
    for i from 0 to n2-1 do B[i] := A[2*i]; C[i] := A[2*i+1]; od;
    FFT(n2,B,p,W,2*stride);
    FFT(n2,C,p,W,2*stride);
    for i from 0 to n2-1 do
      temp := W[i*stride]*C[i] mod p;
      A[i] := B[i] + temp mod p;
      A[n2+i] := B[i] - temp mod p;
    od;
    return;
  end:
> A := Array(0..7,[1,2,3,4,3,2,1,0]):
> FFT(8,A,p,W,1);
> convert(A,list);
```

$$[16, 48, 0, 16, 0, 36, 0, -11]$$

Part (f)

Now let's multiply $a(x)\cdot b(x)$ using the FFT.

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

$$a := -x^3+3x+1$$

$$b := 2x^4-3x^3-2x^2+x+1$$

```
> A := Array(0..7,[1,3,0,-1]) mod p:
> B := Array(0..7,[1,1,-2,-3,2]):
> W := Array(0..3,[seq(w^i mod p,i=0..3)]):
> FFT(8,A,p,W,1);
> FFT(8,B,p,W,1);
> C := Array(0..7):
> for i from 0 to 7 do C[i] := A[i]*B[i] mod p: od:
> W := Array(0..3,[seq(1/w^i mod p,i=0..3)]):
> FFT(8,C,p,W,1);
> ninv := 1/8 mod p:
> for i from 0 to 7 do C[i] := ninv*C[i] mod p od:
> add( C[i]*x^i, i=0..7 );
```

$$-2x^7+3x^6+8x^5-8x^4-10x^3+x^2+4x+1$$

Let's check

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

$$-2x^7+3x^6+8x^5-8x^4-10x^3+x^2+4x+1$$