Метод множення Штрасена (за допомогою дискретного перетворення Фур'є)

Нехай $x=(x_0,...,x_{D-1})\in\mathbb{C}^D$, $y=(y_0,...,y_{D-1})\in\mathbb{C}^D$.

Означення. Циклічною згорткою x, y називається сигнал $z=x\times y$ довжини D:

$$z_n=\sum_{0\le i<D}\ \sum_{\substack{0\le j<D:\\ i+j\equiv n(\mathrm{mod}\,D)}} x_i y_j .$$

Означення. (Комплексне дискретне перетворення Фур'є (ДПФ)). Нехай $x=(x_0,...,x_{D-1})\in\mathbb{C}^D$ - сигнал довжини D, g - примітивний корінь ступеня D із одиниці, наприклад, $g=\exp(2\pi I/D)$, I - уявна одиниця, тоді дискретним перетворенням Фур'є сигналу x є сигнал

$$X=ДПФ(x)=(X_0,...,X_{D-1})\in\mathbb{C}^D:\ X_k=\sum_{j=0}^{D-1}x_j g^{-jk}\ .$$

Обернене перетворення Фур'є $ДПФ^{-1}(X)=x$ задається рівностями

$$x_j=\frac{1}{D}\sum_{k=0}^{D-1}X_k g^{jk}$$

Теорема про згортку *[1,теорема 9.5.12]. Нехай сигнали x, y мають однакову довжину D. Тоді циклічна згортка сигналів x, y задовольняє рівності*

$x\times y=ДПФ^{-1}(ДПФ(x)*ДПФ(y))$*, де '*' означає поелементне множення:*

$$(x\times y)_n=\frac{1}{D}\sum_{k=0}^{D-1}X_k Y_k g^{kn}\ .$$

Алгоритм обчислення ДПФ (швидке перетворення Фур'є).
Варіант Кулі-Тьюки з прорідженням за часом, $D=2^d$.

```
ШПФ(x){
   Перестановка(x);
   n=len(x);
   for(m=1;m<n; m=2m){
   for(j=0;j<m;j++){
      a = g^{-jn/(2m)} ;
      for(i=j; i<n; i=i+2m)
         (x_i, x_{i+m}) = (x_i + a x_{i+m}, x_i - a x_{i+m}) ;
   }
}
   return x;
}
```

```
ШПФ^-1(x){
   x=conjugate(x);// комплексно спряжене
   x=ШПФ(x);
   x=conjugate(x)/D;
   return x;
}

Перестановка(x){
   n=len(x);
   j=0;
   for(i=0;i<n-1;i++){
      if(i<j) (x_i, x_j)=(x_j, x_i);
      k=n>>1;
      while(k<=j){
         j=j-k;
         k=k>>1;
      }
      j=j+k;
   }
   return;
}
```

Алгоритм множення за допомогою ШПФ ([1] Алгоритм 9.5.12, стор.551)

1. [Початкова установка]
   Доповнити нулями x,y до тих пір, поки кожне з них не буде мати по 2D цифр
2. [Пряме перетворення Фур'є]
   X=ДПФ(x);
   Y=ДПФ(y);
3. [Покомпонентне множення]
   Z=X*Y;
4. [Обернене перетворення Фур'є]
   z=ДПФ$^{-1}$(Z);
5. [Заокруглення цифр результату]
   z=round(z);
6. [Переноси за основою *B*]
   carry=0;
   for(n=0; n<2D; n++){
      v=z_n+carry;
      z_n=v mod *B*;
      carry=$\lfloor v / B \rfloor$
   }
7. [Врахування останньої цифри]
   Вилучити нулі на початку послідовності. Якщо carry>0, то carry зробити старшою цифрою числа z;
   return z;

Приклад. 123456*123456

x = (6+I*0, 5+I*0, 4+I*0, 3+I*0, 2+I*0, 1+I*0, 0+I*0, 0+I*0, 0+I*0, 0+I*0, 0+I*0, 0+I*0, 0+I*0, 0+I*0, 0+I*0, 0+I*0, 0+I*0, 0+I*0)

y = (6+I*0, 5+I*0, 4+I*0, 3+I*0, 2+I*0, 1+I*0, 0+I*0, 0+I*0, 0+I*0, 0+I*0, 0+I*0, 0+I*0, 0+I*0, 0+I*0, 0+I*0, 0+I*0, 0+I*0, 0+I*0)

X=ДПФ(x) = (21+I*0, 14.2132-I*10.4374, 4.70711-I*8.94975, 3.23723-I*3.91709, 4-I*3, 3.10591-I*2.26024, 3.29289-I*0.949747, 3.44366-I*0.780508, 3+I*0, 3.44366+I*0.780508, 3.29289+I*0.949747, 3.10591+I*2.26024, 4+I*3, 3.23723+I*3.91709, 4.70711+I*8.94975, 14.2132+I*10.4374)

Y=ДПФ(y) = (21+I*0, 14.2132-I*10.4374, 4.70711-I*8.94975, 3.23723-I*3.91709, 4-I*3, 3.10591-I*2.26024, 3.29289-I*0.949747, 3.44366-I*0.780508, 3+I*0, 3.44366+I*0.780508, 3.29289+I*0.949747, 3.10591+I*2.26024, 4+I*3, 3.23723+I*3.91709, 4.70711+I*8.94975, 14.2132+I*10.4374)

Z=X*Y=(441+I*0, 93.0763+I*-296.696, -57.9411+I*-84.2548, -4.86394+I*-25.3611, 7+I*-24, 4.53804+I*-14.0402, 9.94113+I*-6.25483, 11.2496+I*-5.37561, 9+I*0, 11.2496+I*5.37561, 9.94113+I*6.25483, 4.53804+I*14.0402, 7+I*24, -4.86394+I*25.3611, -57.9411+I*84.2548, 93.0763+I*296.696)

z=ДПФ$^{-1}$(Z) = (36-I*5.32907e-15, 60-I*3.95846e-15, 73-I*1.52926e-16, 76+I*3.73641e-15, 70+I*3.18594e-15, 56+I*3.83476e-17, 35-I*1.62343e-15, 20-I*4.2572e-15, 10+I*1.77636e-15, 4+I*3.14697e-15, 1-I*1.52926e-16, 1.42109e-14+I*1.83697e-16, 0+I*3.66775e-16, 1.06581e-14+I*3.83476e-17, 0+I*1.92928e-15, 0+I*1.07188e-15)

z=round(z)=(36, 60, 73, 76, 70, 56, 35, 20, 10, 4, 1, 0, 0, 0, 0, 0)

Після переносів:

z=(0,0,0,0,0,1,5,2,4,1,3,8,3,9,3,6).

Відповідь:15241383936.

Літ.

Крэндал, Померанс. Простые числа. Стр. 550. (Алгоритм 9.5.12)

Кнут. Искусство программирования. 2 том, стр. 337