

Generalização

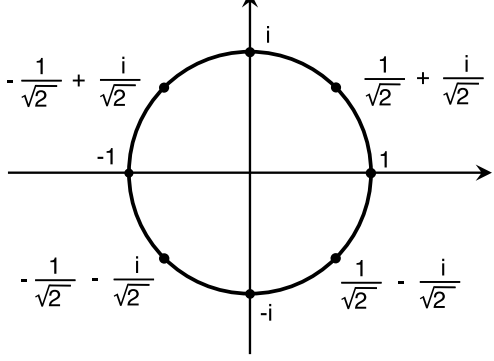
Uma propriedade importante da coleção de pontos com que trabalhamos na seção anterior é que

$$1 \quad = \quad 1^4 \quad = \quad (-1)^4 \quad = \quad i^4 \quad = \quad (-i)^4$$

Logo, para fazer a coisa funcionar, digamos, com 8 pontos, nós precisamos encontrar uma coleção com a seguinte propriedade:

$$1 \quad = \quad p_1^8 \quad = \quad p_2^8 \quad = \quad \dots \quad = \quad p_8^8$$

Mas, isso não é uma tarefa difícil no plano complexo: basta pegar 8 pontos equidistantes no círculo unitário, começando com o 1.



(Verifique isso!)

Em geral, para formar uma coleção de tamanho 2^m , nós pegamos 2^m pontos equidistantes no círculo unitário (começando no 1).

Nós vamos chamar essa coleção de U_m .^a

- para todo ponto p em U_m , o ponto $-p$ também está em U_m — pois, p e $-p$ ficam em extremos opostos no círculo
- para todo ponto p em U_m , o ponto p^2 também está em U_m — (porque?)

Essas duas propriedades tem uma consequência interessante:

- quando nós elevamos todos os elementos de U_m ao quadrado — denote isso por $(U_m)^2$ — nós obtemos um subconjunto de U_m com a metade do tamanho (i.e., 2^{m-1} pontos).

E o mais interessante de tudo é que

$$(U_m)^2 \quad = \quad U_{m-1}$$

Isso já estava acontecendo na seção anterior, veja só

$$U_1 \quad = \quad \{1, -1\} \qquad U_2 \quad = \quad \{1, -1, i, -i\}$$

e

$$(U_2)^2 \quad = \quad U_1$$

Agora nós estamos prontos para fazer as coisas funcionarem recursivamente.

O nosso problema consiste em calcular o valor do polinômio $A(x)$ em todos os pontos da coleção U_m .

Como já sabemos, a ideia consiste em separar as potências pares e ímpares de $A(x)$

$$A(x) \quad = \quad \underbrace{a_0 + a_2x^2 + \dots + a_nx^n}_{\text{par}} + \underbrace{a_1x + a_3x^3 + \dots + a_{n-1}x^{n-1}}_{\text{ímpar}}$$

e, a seguir, nós fatoramos o termo x na parte ímpar, para obter

$$A(x) \quad = \quad \underbrace{a_0 + a_2x^2 + \dots + a_nx^n}_{A_2(x)} + \underbrace{\left[a_1 + a_3x^2 + \dots + a_{n-1}x^{n-2} \right]}_{A_1(x)} \cdot x$$

de modo que

$$A(x) \quad = \quad A_2(x) + A_1(x) \cdot x$$

Essa decomposição permite que os termos $A_2(x)$ e $A_1(x)$ sejam calculados apenas sobre a metade dos pontos — digamos, a metade de cima do círculo.

Isto é, nós estamos calculando valores de polinômios com a metade do tamanho de $A(x)$ (i.e., a metade dos termos), para uma coleção de pontos com a metade do tamanho de U_m .

No entanto, a recursão ainda não está perfeita porque $A_2(x)$ e $A_1(x)$ não são polinômios comuns, mas polinômios que só possuem potências pares.

Mas, isso é um problema fácil de resolver.

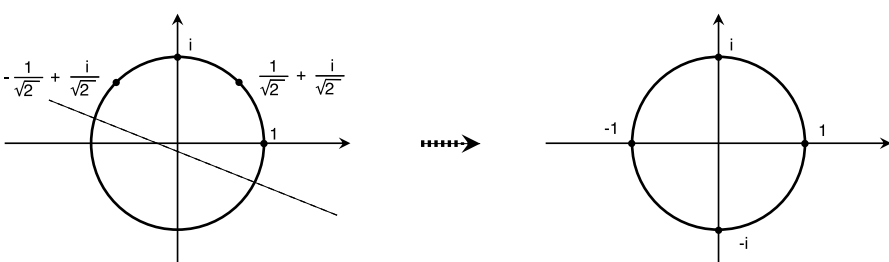
Basta escrever

$$\begin{aligned} A_2(x) &= a_0 + a_2(x^2) + a_4(x^2)^2 + a_6(x^2)^3 + \dots + a_n(x^2)^{n/2} \\ A_1(x) &= a_1 + a_3(x^2) + a_5(x^2)^2 + a_7(x^2)^3 + \dots + a_{n-1}(x^2)^{(n-2)/2} \end{aligned}$$

Isto é, nós podemos ver $A_2(x)$ e $A_1(x)$ como polinômios (comuns) de graus $n/2$ e $(n-2)/2$, sobre o parâmetro x^2 .

Isso significa que nós vamos calcular os valores $A_2(x)$ e $A_1(x)$ (na versão acima) sobre os quadrados dos pontos na metade de cima do círculo.

O passo final consiste em observar o que acontece quando nós elevamos os pontos na metade de cima do círculo ao quadrado:^b



É isso mesmo! nós obtemos a coleção U_{m-1} !

Resumindo tudo o que nós acabamos de fazer:

- para calcular o valor do polinômio $A(x)$ sobre a coleção U_m
- nós decompomos $A(x)$ nos polinômios $A_2(x)$ e $A_1(x)$ (como indicado acima)
- calculamos os valores de $A_2(x)$ e A_1 sobre a coleção U_{m-1}
- e depois calculamos os valores de $A(x)$ a partir dos valores obtidos para $A_2(x)$ e $A_1(x)$

Essas observações já são suficientes para construir um algoritmo de divisão e conquista para a etapa 1:

```
Procedimento  ConversãoR1R2-DC  ( A(x), U_m )
{
    Se ( m = 0 )    Retorna A(1)

    (A2,A1) <--  Quebra ( A(x) )

    V2 <--  ConversãoR1R2-DC ( A2(x), U_{m-1} )
    V1 <--  ConversãoR1R2-DC ( A1(x), U_{m-1} )

    Para cada par de pontos (p,-p) em U_m
    {
        V(p)  <--  V2(p)  +  V1(p)
        V(-p) <--  V2(p)  +  V1(p) * -p
    }
    Retorna (V)
}
```

Examinando o pseudo-código desse procedimento, não é difícil chegar à seguinte equação de recorrência para o seu tempo de execução:^c

$$T(n) \quad = \quad 2 \cdot T(n/2) \quad + \quad O(n)$$

Essa é uma equação de recorrência bem conhecida, que possui solução

$$T(n) \quad = \quad \Theta(n \log n)$$

^aEsse nome é duplamente apropriado: de um lado, U e m se referem ao fato de que são 2^m pontos no círculo unitário, e de outro U_m é parecido com Um.

^bNa realidade, isso funciona para qualquer metade de pontos consecutivos no círculo — (porque?)

^cAqui, nós estamos assumindo que $2^m = O(n)$, o que é o caso para a nossa aplicação de multiplicação de polinômios.