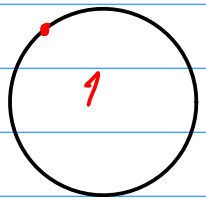
Notas de Clase 01 - Manuel Loaiza Vasquez 02/09/2020

Problema: Con n puntos en una circunferencia que están unidos por cuerdas, ¿en cuántas piezas está dividido el círculo?

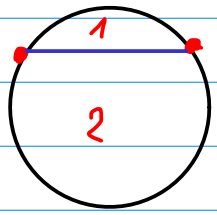
$n = 1$

1



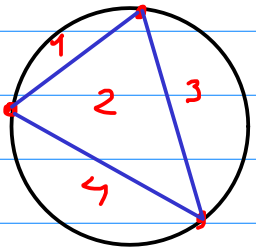
$n = 2$

2



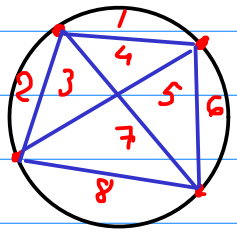
$n = 3$

4



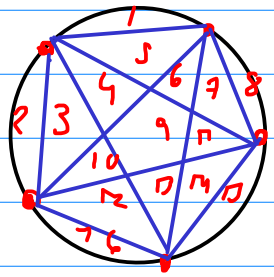
$n = 4$

8



$n = 5$

16



Aparentemente la respuesta es 2^{n-1}, sin embargo, para $n = 6$ obtenemos 31 piezas, lo cual destruye nuestra hipótesis.

- El incremento de una pieza al añadir una cuerda.
  = una cuerda divide cada pieza en dos.
- La cantidad de piezas divididas por la cuerda
  = cada pieza se divide por un segmento de la cuerda.
- La cantidad de segmentos en la cuerda
  = la cantidad de puntos internos que son intersección con otros segmentos.
- Observamos que [1 + cantidad puntos de intersección interna] es la cantidad de piezas que un segmento dividirá en dos.
- El incremento al añadir c cuerdas
  = c + [cantidad total de puntos de intersección interna en las nuevas cuerdas].

Sea $f :=$ cantidad de piezas

$c :=$ cantidad de cuerdas

$p :=$ cantidad de puntos de intersección interna

Comenzando con cero puntos, tenemos una pieza, luego

$$f = 1 + C + P.$$

Sea $n \in \mathbb{N}$ la cantidad de puntos que tenemos de entrada, sabemos que cada cuerda se forma con 2 puntos

$$f(n) = 1 + \binom{n}{2} + P(n)$$

y cada punto de intersección interna se forma con 4 puntos

$$f(n) = 1 + \binom{n}{2} + \binom{n}{4}$$

$$= 1 + \frac{n!}{2!(n-2)!} + \frac{n!}{4!(n-4)!}$$

$$= 1 + \frac{n(n-1)}{2} + \frac{n(n-1)(n-2)(n-3)}{24}$$

$$= 1 + \frac{12(n^2-n)}{24} + \frac{n^4 - 6n^3 + 11n^2 - 6n}{24}$$

$$= 1 + \frac{n^4 - 6n^3 + 23n^2 - 18n}{24}$$

∎

$\therefore$ Con n puntos en una circunferencia que están unidos por cuerdas, el círculo puede ser dividido en $1 + \frac{n^4 + 6n^3 + 23n^2 - 18n}{24}$ piezas.

Problema: ¿Cómo calculamos el máximo común divisor de A y B?

- Solución trivial pero ineficiente:

Hallamos los divisores de A y B

$$\text{div}A = \{ d_1, d_2, \dots, d_n \} \quad \wedge \quad \text{div}B = \{ e_1, e_2, \dots, e_m \}.$$

d_1 ... d_n: A veces; e_1 ... e_m: B veces

El cálculo de cada lista sería en $O(\max(A,B))$, para cada factor en $\text{div}A$ realizaría una búsqueda binaria en $\text{div}B$ para saber si aparece. De

esta manera la complejidad en tiempo sería // Notación Manuel

$T(A,B) = O(A + B + A \lg B)$ // $\lg := \log_2$

$= O(\max(A,B) \lg(\max(A,B)))$.

- Solución eficiente: Algoritmo de Euclides

```
GCD(A, B)
  if (B == 0) return A;
  else return GCD(B, A mod B)
```

Analicemos la corrección del algoritmo provisto.

Teorema. Para todo $A \in \mathbb{N} \cup \{0\}$, $B \in \mathbb{N}$ tenemos que

$GCD(A,B) = GCD(B, A \bmod B)$.

Prueba: Sabemos que si $n \mid m$ y $m \mid n$, entonces $m = n$, donde $x \mid y$ significa que x divide a y, $m, n, x, y \in \mathbb{N} \cup \{0\}$.

($\Rightarrow$) Comencemos probando que $GCD(A,B) \mid GCD(B, A \bmod B)$.

Aplicando el teorema de representación única de la división tenemos

$A = Bk + r$, $0 \le r < B$ ∧ $r = A \bmod B$

$r = A - Bk$ y como $GCD(A,B)$ es un divisor de A y B,

tenemos que $\left.\begin{array}{l} GCD(A,B) \mid A \\ GCD(A,B) \mid Bk \end{array}\right\} GCD(A,B) \mid (A - Bk)$

$\Downarrow$

$GCD(A,B) \mid (A \bmod B)$

Por lo tanto, $GCD(A,B) \mid B$, $GCD(A,B) \mid (A \bmod B)$

$\Rightarrow GCD(A,B) \mid GCD(B, (A \bmod B))$.

($\Leftarrow$) Probemos que $GCD(B, A \bmod B) \mid GCD(A,B)$.

Análogamente a la prueba anterior, tenemos que

$GCD(B, A \bmod B) \mid B$ ∧ $GCD(B, A \bmod B) \mid A \bmod B$

$A \bmod B = A - Bk \Rightarrow A = Bk + A \bmod B$

Como $GCD(B, A \bmod B) \mid (A \bmod B)$ y $GCD(B, A \bmod B) \mid Bk$

entonces $GCD(B, A \bmod B) \mid A$.

Como también $GCD(B, A \bmod B) \mid B$, tenemos $GCD(B, A \bmod B) \mid GCD(A,B)$

∴ Concluimos que $GCD(A,B) = GCD(B, A \bmod B)$ ∎

Teorema. $GCD(A,B)$ tiene complejidad en tiempo $O(\lg(\max(A,B)))$.

Prueba: Sin pérdida de generalidad, asumamos que $A \geq B$. En caso no sea hacemos un swap entre las dos variables. Analicemos dos casos:

i) $B \leq \frac{A}{2}$: En este caso, si $B \neq 0$ tenemos que resolver

$$GCD(A,B) = GCD(B, \underbrace{A \bmod B}_{\leq \frac{A}{2} \; < \frac{A}{2}})$$

ii) $B > \frac{A}{2}$:

$$-B < -\frac{A}{2}$$

$$\underbrace{A-B}_{A \bmod B \text{ pues } A \geq B} < \frac{A}{2}$$

$$GCD(A,B) = GCD(B, \underbrace{A \bmod B}_{< \frac{A}{2}})$$

Notamos que en el caso (i) ambos se reduces al menos en su mitades, mientras que en el caso (ii) solo uno de ellos se reduce al menos a su mitad. Asimismo sabemos que cuando uno de ellos llegue a cero, el programa empieza a retornar, por lo cual tenemos que $T(A,B) \leq 1 + T(A, \frac{B}{2})$

$$\leq 1 + 1 + T(A, \tfrac{B}{4})$$

$$\vdots$$

$$\leq 1 + 1 + \ldots + 1 + T\left(A, \frac{B}{2^{\lfloor \lg B \rfloor}}\right)$$

$\vdash \lfloor \lg B \rfloor$ veces $\dashv$

$\vdots$ Análogamente con A

$$\leq \underbrace{1+\ldots+1}_{\lfloor \lg B \rfloor \text{ veces}} + \underbrace{1+\ldots+1}_{\lfloor \lg A \rfloor \text{ veces}} + \underbrace{T\left(\frac{A}{2^{\lfloor \lg A \rfloor}}, \frac{B}{2^{\lfloor \lg B \rfloor}}\right)}_{C}$$

$$\leq C + \lfloor \lg B \rfloor + \lfloor \lg A \rfloor$$

$$\leq C \lfloor \lg \max(A,B) \rfloor + \lfloor \lg \max(A,B) \rfloor + \lfloor \lg \max(A,B) \rfloor$$

$$\leq (2+C) \lfloor \lg(\max(A,B)) \rfloor$$

$$\leq (2+C)(\lg(\max(A,B)) + 1)$$

$$\leq 2(2+C) \lg(\max(A,B))$$

$$\leq K \lg(\max(A,B))$$

$\therefore GCD(A,B) \in O(\lg(\max(A,B)))$. ∎