

### Heurística 1

$$n = a^b \mid a \in \mathbb{N}, b > 1 \Rightarrow n \text{ es compuesto}$$

### Heurística 2

$$\exists a \leq r \mid 1 < \text{mcd}(n, a) < n \Rightarrow n \text{ es compuesto}$$

### Calculo de r

r es el  $\min r \mid \text{Or}(n) > \log_2 n$

$\text{Or}(n)$  es el orden de  $n$  módulo r y representa el menor k tal que  $n^k \equiv 1 \pmod{r}$

$\xrightarrow{\text{mínimo } k} \text{Ejemplo } \text{Or}_3(5) = 2 \leftarrow \text{mínimo } k$

ya que  $\frac{5^2 - 1}{3}$  da resto 0

Vamos a calcular  $r$  si  $n=5$

Empezamos con  $k=1$

$\frac{5^1 - 1}{2}$  es exacta  $\Rightarrow O_2(5) = 1$   
pero  $1 < \log_2 5 \Rightarrow$  No vale  
empezamos  
con  $r=2$

Probamos  $r=3$

$$\frac{5^2 - 1}{3} \text{ no exacta} \quad \frac{5^3 - 1}{3} = 8 \Rightarrow O_3(5) = 2$$

pero  $2 < \log_2 5 \Rightarrow$  no vale

Seguimos probando  $r=4, r=5, r=6$ , que no valen

Probamos  $r=7$

este vale

$$\frac{5^k - 1}{7}$$

nos probar  $k=1, k=2, k=3, k=4, k=5$   
tenemos divisiones no exactas, pero

$$\frac{5^6 - 1}{7} = 2232 \Rightarrow O_7(5) = 6 > \log_2 5$$

¿Para qué sirve r?

- ① Establece un límite para el cálculo del mcd
- ② Permite determinar primalidad  
 $n \leq r \Rightarrow n$  es primo
- ③ Establece un límite en el bucle con el que verificamos la condición suficiente en AKS

Cálculo del mcd

Algoritmo

```
while (a != 0) {  
    temp = a;  
    a = b % a;  
    b = temp;  
}
```

## Peor instancia

a, b son dos números consecutivos en la sucesión de Fibonacci

1, 1, 2, 3, 5, 8, 13, 21, ...

$f_1, f_2, f_3, f_4, f_5, f_6, f_7, f_8, \dots$

Número de iteraciones del bucle:

*Índice del término en la sucesión*

Fórmula de E. Lucas

$$\phi = \frac{1+\sqrt{5}}{2}$$

$$f_n = \frac{\phi^n - (1-\phi)^n}{\sqrt{5}}$$

Transformando  $f_n$  y tomando logaritmos en base  $\phi$  para despejar n. se concluye que la complejidad es  $O(\log f_n)$













