Pontificia Universidad Católica de Chile
Departamento de Ciencia de la Computación
IIC2283 - Diseño y Análisis de Algoritmos

Ayudantía 11 - Testeo de primalidad

27 de noviembre de 2020

Profesor Marcelo Arenas

Bernardo Barías y Ricardo Rodríguez

Repaso

Recordemos el test de primalidad visto en clase, compuesto por una función principal **TestPrimalidad**(n, k) y dos funciones auxiliares **EsPotencia**(n) y **TieneRaízEntera**(n, k, i, j)

TestPrimalidad(n, k)
- $n = 2$ PRIMO
- n es par COMPUESTO
- **EsPotencia**(n) COMPUESTO

  sea $a_1, \ldots, a_k$ una secuencia de números elegidos de manera uniforme e independiente desde $\{1, \ldots, n-1\}$
  - $i := 1$ k
    - **MCD**$(a_i, n) > 1$ COMPUESTO
    - $b_i := \textbf{Exp}(a_i, \frac{n-1}{2}, n)$
  - $neg := 0$
  - $i := 1$ k
    - $b_i \equiv -1n$ $neg := neg + 1$
    - $b_i \not\equiv 1n$ COMPUESTO
  - $neg = 0$ COMPUESTO
  - PRIMO

TieneRaízEntera(n, k, i, j)
- $i = j$
  - **Exp**$(i, k) = n$ sí
  - no
- $i < j$
  - $p := \lfloor \frac{i+j}{2} \rfloor$
  - $val := \textbf{Exp}(p, k)$
  - $val = n$ sí
  - $val < n$ **TieneRaízEntera**(n, k, $p+1$, j)
  - **TieneRaízEntera**(n, k, i, $p-1$)
- no

EsPotencia(n)
- $n \leq 3$ no

$k := 2$ $\lfloor \log_2(n) \rfloor$
    TieneRaízEntera(n, k, 1, n) sí
no

Pregunta 1

Ejecute calculando a mano el algoritmo **TestPrimalidad**(n, k) con los siguientes parámetros

1. **TestPrimalidad**(57, 3)
2. **TestPrimalidad**(2021, 5)
3. **TestPrimalidad**(40548895045822167299, 5)

Pregunta 2: Aplicaciones del test en criptografía

El algoritmo criptográfico RSA requiere para su inicialización de números primos generados aleatoriamente, cuyo tamaño sea de 1024 bits, es decir, de 308 o 309 dígitos al representarlos en base 10. Por el teorema de los números primos, probado por Hadamard y de la Vallée Poussin en 1896, para un valor n grande, la probabilidad de que el número n sea primo es aproximadamente $\frac{1}{ln(n)}$.

Al implementar este algoritmo, se suele utilizar el test de primalidad anterior usando $k = 20$ para declarar si un número es primo o no.

1. Calcule el valor esperado de números de 309 cifras a probar hasta conseguir 2 primos, ¿Como distribuye esta variable aleatoria?
2. ¿Cuál es el tiempo esperado de ejecución de este procedimiento para generar 2 primos?
3. Suponga que debido al descubrimiento de un ataque criptográfico y mejoras en la capacidad de cómputo usted debe ahora utilizar 2 primos de 618 dígitos, ¿Cuál es el valor esperado de números de ese largo a testear hasta conseguir 2 primos?