Pontificia Universidad Católica de Chile
Escuela de Ingeniería
Departamento de Ciencias de la Computación

Ayudante: Nicholas Mc-Donnell
Email: namcdonnell@uc.cl

Ayudantía 10

Test de Miller-Rabin

IIC3253 – Criptografía

Fecha: 2021-06-02

Historia

Un poco de historia sobre el algoritmo, en 1976 Miller invento una versión determinista del test, pero la correctitud del test dependía en una extensión de la Hipótesis de Riemann[1], por lo tanto tenía un uso limitado. Luego, en 1980 Rabin modifico el test para que fuera probabilista, pero que su correctitud no dependiera de alguna extensión de la Hipótesis de Riemann. Este último es el test moderno, y el que principalmente tratará la ayudantía.

1. Notación y Definiciones Preliminares

Definición 1.1 (Enteros Modulo n)**.** Se define $\mathbb{Z}/n\mathbb{Z}$, como las clases de equivalencia de los enteros respecto a la relación de congruencia modulo n.

$$\mathbb{Z}/n\mathbb{Z} = \{\overline{a}_n \mid a \in \mathbb{Z}\} = \{\overline{0}_n, \ldots, \overline{n-1}_n\}$$

Además, se suma y multiplicación de la siguiente forma[2]:

$$\overline{a}_n + \overline{b}_n = \overline{a+b}_n$$
$$\overline{a}_n \cdot \overline{b}_n = \overline{a \cdot b}_n$$

[1] https://www.claymath.org/millennium-problems/riemann-hypothesis

[2] Se deja como ejercicio verificar que todo está bien definido (i.e. son funciones bien definidas, y no dependen del representante de la clase de equivalencia).

Definición 1.2 (Invertibles Modulo n)**.** Se define $(\mathbb{Z}/n\mathbb{Z})^\times$ como los elementos de $\mathbb{Z}/n\mathbb{Z}$ que tienen inverso.

$$(\mathbb{Z}/n\mathbb{Z})^\times = \{a \in \mathbb{Z}/n\mathbb{Z} \mid \exists b \in \mathbb{Z}/n\mathbb{Z}\, ab = \overline{1}_n\}$$

Definición 1.3 (Orden)**.** Dado $x \in (\mathbb{Z}/n\mathbb{Z})^\times$ se define $\text{ord}(x)$ como el menor entero positivo k tal que $x^k = \overline{1}_n$.

$$\text{ord}(x) = \text{mín}\{k > 0 \mid x^k = \overline{1}_n\}$$

Definición 1.4 (Función Phi)**.** Se tiene que $\varphi(n) = \left|(\mathbb{Z}/n\mathbb{Z})^\times\right|$[3].

Nota. *Se usará un abuso de notación, donde $x \in \mathbb{Z}/n\mathbb{Z}$ se usará intercambiablemente con $x \in \mathbb{Z}$, donde x es un representante de la clase de equivalencia.*

2. Resultados sin Demostración

Los siguientes resultados se darán sin demostración, o con un esbozo de demostración (terminar las demostraciones es un ejercicio **bonus**).

Teorema 2.1 (Teorema Chino del Resto (CRT))**.** *Dado $n, m \in \mathbb{N}$ tal que $\gcd(n, m) = 1$ existe una biyección natural que preserva suma y multiplicación entre $\mathbb{Z}/nm\mathbb{Z}$ y $\mathbb{Z}/n\mathbb{Z} \times \mathbb{Z}/m\mathbb{Z}$*[4]*.*

Demostración. La siguiente función[5] cumple lo pedido:

$$\begin{aligned} f :&\mathbb{Z}/nm\mathbb{Z} \to \mathbb{Z}/n\mathbb{Z} \times \mathbb{Z}/m\mathbb{Z} \\ &x \mapsto (x \mod n, x \mod m) \end{aligned}$$

□

Teorema 2.2 (Lagrange (en $(\mathbb{Z}/n\mathbb{Z})^\times$))**.** *Para todo $x \in (\mathbb{Z}/n\mathbb{Z})^\times$ se tiene que $ord(x) \mid \varphi(n)$.*

Teorema 2.3 ($(\mathbb{Z}/p^\alpha\mathbb{Z})^\times$ es Ciclico)**.** *Dado p primo impar, existe $g \in (\mathbb{Z}/p^\alpha\mathbb{Z})^\times$ tal que para todo $y \in (\mathbb{Z}/p^\alpha\mathbb{Z})^\times$ $y = g^k$ para algún $k \in \mathbb{Z}$. Se dice que g genera $(\mathbb{Z}/p^\alpha\mathbb{Z})^\times$, o que g es un generador.*

Corolario. *Las soluciones de la ecuación $x^k = 1$ con $x \in (\mathbb{Z}/n\mathbb{Z})^\times$ y $n = p^\alpha$ corresponden naturalmente a soluciones de la congruencia $ak \equiv 0 \mod \varphi(n)$.*

[3]Está definición es equivalente a la dada anteriormente. Queda como ejercicio demostrar eso.

[4]Aquí la suma y multiplicación son componente a componente.

[5]Hay un inverso explicito de la función, ver `https://en.wikipedia.org/wiki/Chinese_remainder_theorem#Case_of_two_moduli`.

Demostración. Dado g generador y a solución de la congruencia, ver que g^a corresponde a una solución de la ecuación original. □

Teorema 2.4 (φ es Multiplicativa)**.** *Dado $n, m \in \mathbb{Z}$ tales que $\gcd(n, m) = 1$ se tiene que $\varphi(nm) = \varphi(n)\varphi(m)$.*

Demostración. Usar CRT. □

Corolario. *Se tiene la siguiente igualdad $\varphi(n) = \prod_{p|n} p^{\alpha_p - 1}(p-1)$.*

Demostración. Usar el teorema anterior y calcular $\varphi(p^\alpha)$. □

3. Test de Miller-Rabin

Test de Miller-Rabin D

La entrada es $n \in \mathbb{Z}$ tal que $n > 1$ y $k \in \mathbb{N}$.

1) Si $n \leq 9$ se revisa si $n \in \{2, 3, 5, 7\}$, y se retorna "primo" o "compuesto" correspondientemente.
2) Si $n > 9$ y n es par, retornar es "compuesto".
3) Se escribe $n = m2^k$, donde m es impar. Repetir lo siguiente t veces
   a) Se elige $x \in (\mathbb{Z}/n\mathbb{Z})^\times$ al azar[6].
   b) Se verifica que x cumple alguno de los siguientes, $x^m = 1$ o $x^{m2^i} = -1$ para algún $0 \leq i < k$.
   c) Si falla la verificación, se retorna "compuesto".
4) Se retorna "primo".

Nota. *La parte b) se puede hacer usando "binary exponentiation". Con lo anterior, se tiene que el test tiene complejidad $O\left(t \cdot (\log(n))^3\right)$*[7]

Teorema 3.1. *El test de Miller-Rabin no da falsos negativo.*

[6] Se elige $x \in \mathbb{Z}/n\mathbb{Z}$ distinto de 0 y se calcula $g = \gcd(x, n)$, si g no es 1 se retorna "compuesto".

[7] La complejidad de la multiplicación de números es considerada.

Demostración. Sea p primo. Si $p \leq 9$ es obvio que Miller-Rabin retorna "primo". Si $p > 9$ entonces es impar, se escribe $p - 1 = m2^k$, con m impar. Sea $x \in (\mathbb{Z}/p\mathbb{Z})^\times$[8]. Se nota que

$$x^{p-1} = 1$$

por el teorema de Euler-Fermat. Reescribiendo el exponente se tiene que

$$x^{m2^k} = 1.$$

Se usa el siguiente argumento recursivo para demostrar que $x^m = 1$ o $x^{m2^i} = -1$ para algún $0 \leq i < k$, se nota que $\left(x^{m2^{l-1}}\right)^2 - 1 = 0$ tiene dos soluciones $x^{m2^{l-1}} = \pm 1$, si $x^{m2^{l-1}} = -1$ se tiene lo pedido, si no se usa el argumento recursivo sobre $x^{m2^{l-1}} - 1 = 0$, para el caso base $x^m - 1 = 0$, se tiene que trivialmente se cumple lo pedido. □

Teorema 3.2. *Sea $n > 9$ entero compuesto impar. Se escribe $n - 1 = 2^k m$, con m impar. Dado*

$$B = \{x \in (\mathbb{Z}/n\mathbb{Z})^\times \mid x^m = 1 \text{ o } x^{m2^i} = -1 \text{ para algún } 0 \leq i < k\}$$

se tiene que

$$\frac{|B|}{\varphi(n)} \leq \frac{1}{4}$$

Demostración. Sea 2^l máximo tal que $\forall p \mid n$ se tiene $2^l \mid p - 1$. Se define

$$B' = \{x \in (\mathbb{Z}/n\mathbb{Z})^\times \mid x^{m2^{l-1}} = \pm 1\}$$

Se quiere ver que $B \subset B'$, dado $x \in B$, se tienen dos casos, $x^m = 1$ y $x^{m2^i} = -1$ para algún $0 \leq i < k$. En el primer caso trivialmente se tiene que $x \in B'$. Para el segundo caso, se ve que $x^{m2^i} \equiv -1 \mod p$ para todo primo $p \mid n$[9], por lo que $\text{ord}(x) = 2^{i+1}$ para todo $p \mid n$. Ahora, por Lagrange se tiene que $2^{i+1} \mid p - 1$, más específicamente $2^{i+1} \mid 2^l$, por lo que $l \geq i + 1$. Con lo anterior se ve que

$$x^{m2^{l-1}} = (-1)^{m2^{l-i-1}} = (-1)^{2^{l-i-1}}$$

Por lo que $x^{m2^{l-1}} = -1$ si y solo si $l = i + 1$ y es 1 si y solo si $l > i + 1$. Con lo que se tiene que $x \in B'$.

Con lo anterior se llega a que $|B| \leq |B'|$, y se quiere acotar $|B'|$. Notemos que $|B'|$ es la cantidad de soluciones de $x^{m2^{l-1}} = \pm 1$, para contar esto primero se contarán las soluciones

[8] Como p es primo $(\mathbb{Z}/p\mathbb{Z})^\times = \mathbb{Z}/p\mathbb{Z} \setminus \{0\}$

[9] $(a \equiv b \mod n \wedge d \mid n) \implies a \equiv b \mod d$

de $x^{m2^{l-1}} = 1$, usando CRT y contando las soluciones de $x^{m2^{l-1}} \equiv 1 \mod p^{\alpha_p}$ donde p^{α_p} es la potencia exacta que divide a n. Usando el corolario del Teorema 2.3, se tiene que las solución modulo p^{α_p} son $\gcd((p-1)p^{\alpha_p-1}, m2^{l-1})$, que es $\gcd(p-1,m)2^{l-1}$ ya que $2^{l-1} \mid p-1$ y $\gcd(p, m2^{l-1}) = 1$[10]. Por lo tanto se tiene que

$$\left|\{x \in (\mathbb{Z}/\ltimes\mathbb{Z})^\times \mid x^{m2^{l-1}} = 1\}\right| = \prod_{p|n} \gcd(p-1,m)2^{l-1},$$

y se puede usar el mismo argumento para ver que la cantidad de soluciones de $x^{m2^l} \equiv 1$ mód p^{α_p} es $\gcd(p-1,m)2^l$, y esa cantidad es el doble de la cantidad soluciones de $x^{m2^{l-1}} \equiv 1$ mód p^{α_p}, por lo que $x^{m2^l} \equiv -1 \mod p^{\alpha_p}$ tiene $\gcd(p-1,m)2^{l-1}$ soluciones, juntando todo se llega a

$$|B'| = 2\prod_{p|n} \gcd(p-1,m)2^{l-1}$$

con lo que

$$\frac{|B'|}{\varphi(n)} = 2\prod_{p|n} \frac{\gcd(p-1,m)2^{l-1}}{(p-1)p^{\alpha_p-1}}.$$

Ahora, por contradicción se asume que $\frac{|B|}{\varphi(n)} > \frac{1}{4}$, por lo tantos se tiene que $\frac{|B'|}{\varphi(n)} > \frac{1}{4}$. Se nota que $\gcd(p-1,m)2^{l-1} \mid (p-1)/2$, por lo que $\frac{(p-1)p^{\alpha_p-1}}{\gcd(p-1,m)2^{l-1}} \geq 2p^{\alpha_p-1}$, por lo que $\frac{|B'|}{\varphi(n)} \leq 2^{1-t}$, donde t es la cantidad de divisores primos de n. Esta desigualdad nos dice que $t \leq 2$[11], por lo que tomamos el caso donde $t = 2$ y $\alpha_p \geq 2$ para algún p, usando la cota anterior se tiene que $\frac{|B'|}{\varphi(n)} \leq 2 \cdot \frac{1}{3} \cdot \frac{1}{4} = \frac{1}{6}$, por lo que $\alpha_p = 1$ para todo p. Con lo anterior, y aún con $t = 2$, podemos reescribir la desigualdad a

$$1 \leq \frac{p-1}{\gcd(p-1,m)2^l} \cdot \frac{q-1}{\gcd(q-1,m)2^l} < 2$$

y como $\frac{p-1}{\gcd(p-1,m)2^l}$ y $\frac{q-1}{\gcd(q-1,m)2^l}$ son enteros, entonces $p-1 = \gcd(p-1,m)2^l$ y $q-1 = \gcd(q-1,m)2^l$. Denotando $m_p = \gcd(p-1,m)$ y $m_q = \gcd(p-1,m)$, se ve que

$$\begin{aligned} pq &= 1 + m2^l \\ pq &\equiv 1 + m2^l \mod m_p \\ -q &\equiv 1 \mod m_p \end{aligned}$$

[10]Notar que si $p \mid n-1$ se tiene que $p \mid 1$.
[11]Desarrollar $\frac{1}{4} < 2^{1-t}$.

con lo que se tiene que $m_p \mid q-1$, usando el mismo argumento con m_q, se tiene $m_q \mid p-1$, por lo que $m_p = m_q$, más aún $p = q$, pero eso contradice que $t = 2$.

Vemos el caso $n = p^\alpha$, y recordamos la desigualdad $\frac{(p-1)p^{\alpha_p - 1}}{\gcd(p-1,m)2^l} \geq p^{\alpha_p - 1}$, se nota entonces que $p^{\alpha-1} < 4$, por lo que $p = 3$ y $1 \leq \alpha \leq 2$, por lo que $n < 9$, lo que es una contradicción. $\square$