S1/S TEÓRICA

est de primalidad

Wilson

-1)! ≡ -1 (n) ⟺ n es primo

multiplicaciones)

complejidad de un test se mide en
cant. de dígitos del nº
test de Wilson necesita 10^m
tiplicaciones para saber si el nº de
itos es primo (Entonces es exponencial
m)

) Test de Fermat

siendo $a^p \equiv a\ (p)$ cuando p es primo
test es dado un $m \in \mathbb{N}$, elijo
) entre 1 y m-1 al azar
se calcula $a^m \equiv ?\ (m)$

$? \neq a \Rightarrow$ no es compuesto

jado a, la complejidad es a lo
sumo logarítmica en la cant.
de dígitos de m.

roblema: nº de Carmichel
nº compuestos que pasan el test de
Fermat para cualquier a. Hay ∞ tales
nº $(cX) > X^{2/7}$ si X es grande

) Test de Miller-Rabin

Se basa en la sig. proposición

Prop Sea p primo $p>2$

$p-1 = 2^1 \cdot d$ d es impar

Sea $a \in \mathbb{N}$ $1 \leq a < p$

Entonces, o bien $a^d \equiv -1\ (p)$ para algún
$0 \leq r \leq s-1$ o bien

$a^d \equiv 1\ (p)$

Dem: $1 \geq 1$

por Fermat $a^{p-1} \equiv 1\ (p)$

Entonces $a^{2^1 \cdot d} \equiv 1\ (p)$

$p \mid a^{2^1 \cdot d} - 1$ ← DIFERENCIA DE CUA

como $a^{2^1 \cdot d} - 1 = (a^{2^{1-1} \cdot d} + 1) \cdot (a^{2^{1-1} \cdot d} -$

Como p es primo, entonces

$p \mid a^{2^{1-1} \cdot d} + 1$ ó $p \mid a^{2^{1-1} \cdot d} - 1$

Si ocurre esto, listo.

Si ocurre esto, repetimos el proceso

$a^{2^{1-1} \cdot d} - 1 = (a^{2^{1-2} \cdot d} + 1) \cdot (a^{2^{1-2} \cdot d} -$

$\Rightarrow$ o bien $\exists r,\ 1 \leq r < 1$ /p

o bien, luego de 1-1 pasos queda
que $p \mid a^{2^1} - 1$

Entonces $p \mid (a^d + 1) \cdot (a^d - 1)$

como p primo $\Rightarrow p \mid a^d + 1 \Rightarrow$ caso r=
$p \mid a^d - 1 \Rightarrow$ (el segundo o bi

Asamblea

Scanned by CamScanner

Test de M.-Rabin: dado m impar, (queremos ver si m es primo)

$m-1 = 2^s d$ $\quad s \geq 1$ d impar

Se elige a al azar $1 < a < m$ y se calcula $a^{2^r d} \equiv c_r \ (m)$

para cada $0 \leq r < s$

$a^d \equiv c \ (m)$

Si $c_r \neq -1$ o $c \neq +1$ (para c/r)

$\Rightarrow$ m es compuesta

▶ Este test es concluyente, es decir, si m es compuesto, $\exists$ (muchos) "testigos" (a) que "fallan" el test, es decir, detectan que m es compuesto

Dificultad: no se sabe como elegir los testigos que detecten m compuesto

∴ Se eligen valores de "a" al azar y se demuestra que si se corre el test k veces, la probabilidad que m pase el test y sea compuesto es $\frac{1}{4}^k$.

La complejidad del test es

$\sim k \cdot (\log(m))^3$

(es cúbico en la cant. de dígitos de m)

4) test AKS (Agrawal, Kayal, Saxena)

"PRIMES is in P"

Teo: Hay un algoritmo, determinístico polinomial en la cant. de dígitos de n, para decidir si un nº es primo

(Es "fácil")

Volviendo a congruencias

El anillo $\mathbb{Z}/m\mathbb{Z}$

En el conjunto $\{0, 1, 2, \ldots, m-1\}$ (las clases de congruencia módulo m)

Se puede sumar con una suma

$\dot{+}$) $a \dot{+} b = r_m(a+b)$

(Sumamos a con b y tomamos $\equiv$ mod (m))

Esta suma tiene las prop.: (saco el punto en la notación)

1) $a+b = b+a$ (conmutativa)

2) $a+0 = a$ (elemento neutro)

3) $(a+b)+c = a+(b+c)$ (asociativa)

4) Dado $a \in \{0, \ldots, m-1\}$

$\exists \tilde{a} \in \{0, \ldots, m-1\}$ (congruencia)

$a + \tilde{a} = 0$ (inverso)

$\mathbb{Z}/m\mathbb{Z}$ es el conjunto

$\{0, 1, \ldots, m-1\}$ → la suma tomando congruencias es

$(\mathbb{Z}/m\mathbb{Z}, \dot{+})$ un grupo abeliano

(Verifica 2, 3, 4)

(Verifica 1)

Ejemplo: $\mathbb{Z}/7\mathbb{Z}$

es el conj $\{0, 1, 2, 3, 4, 5, 6\}$

Ej: congruencia

$1+2 = 3$ (7)

$3+5 = 1$ (7)

$6+4 = 3$ ⋮

$2+5 = 0$ (5 es el inverso aditivo de 2 en $\mathbb{Z}/7\mathbb{Z}$)

En $\mathbb{Z}/m\mathbb{Z}$ se define un producto

$a \cdot b = r_m(a \cdot b)$

Scanned by CamScanner

Ej: en $\mathbb{Z}/7\mathbb{Z}$ (como si fuese $=$)

$2.3 = 6 \ (7)$

$2.4 = 1 \ (7)$

$3.5 = 1 \ (7)$

$6.4 = 3 \ (7)$

Prop del producto:

I) $a.b = b.a$ (conmutativo)

II) $a.1 = a$ (neutro)

III) $a(b.c) = (a.b)c$ (asociativo)

IV)

V) $a(b+c) = a.b + a.c$ (Distributiva)

El anillo $\mathbb{Z}/m\mathbb{Z}$

es el conjunto $\{0, 1, \dots, m-1\}$ con las operaciones $+, \cdot$

$(\mathbb{Z}/m\mathbb{Z}, +, \cdot)$ (verifica lo anterior)

En verdad se tiene anillo, conmutativo (I) con unidad (II)

Def Un cuerpo es un anillo conmutativo con unidad / $\forall a \neq 0$ $\exists \tilde{a} / a.\tilde{a} = 1$

(o sea $\forall$ elemento $\neq 0$ $\exists$ inverso multiplicativo)

Ej: En $(\mathbb{Z}/10\mathbb{Z}, +, \cdot)$

$4.5 = 0$

$2.10 = 0$

Entonces $\mathbb{Z}/10\mathbb{Z}$ no es un cuerpo

10, 4, 5 no tienen inverso multiplicativo

ya que si por ej. 2 tuviese inverso multiplicativo $\exists \tilde{a} / 2.\tilde{a} = 1$

multiplicando por lo que sea

$10.2.\tilde{a} = 10$

$0\tilde{a} = 10$

$0 = 10$ (Abs)

¿Cuándo $\mathbb{Z}/m\mathbb{Z}$ es un cuerpo?

Rta: $\iff$ m es primo

Dem

Dado $a \neq 0$, si q.v.q. a es invertible, hay que resolver la ecuación de congruencia

$aX \equiv 1 \ (m)$

Esta ecuación tiene sol $\iff$

$(a:m) \mid 1 \iff (a:m) = 1$

Teorema:

$\mathbb{Z}/m\mathbb{Z}$ es un cuerpo $\iff$ m es primo

Dem $\mathbb{Z}/m\mathbb{Z}$ es cuerpo si, por definición la ec. $aX \equiv 1 \ (m)$ tiene solución $\forall$ $1 \leq a < m$

Por la observación de recién esta ecuación tiene solución $\iff (a:m) = 1$

Si m no es primo:

$\exists \ 1 < a_0 < m \ / \ a_0 \mid m$

En cuyo caso $(a_0 : m) \neq a_0$

$\Rightarrow a_0 X \equiv 1 \ (m)$ no tiene solución

Si m es primo:

Entonces todo $1 \leq a < m$ verifica que $(a:m) = 1$

$\Rightarrow$ la ec. $aX \equiv 1 \ (m)$ tiene solución $\forall \ 1 \leq a < m$

Obs: Lema

En $\mathbb{Z}/m\mathbb{Z}$ los elementos que tienen inverso multiplicativo son los de $\mathbb{Z}/m\mathbb{Z}$ tales que $(a:m) = 1$

Estos elementos se llaman los unidades de $\mathbb{Z}/m\mathbb{Z}$ y se denota

$\mathcal{U}(\mathbb{Z}/m\mathbb{Z})$ por def de la φ de Euler, hay $\varphi(m)$ elementos en $\mathcal{U}(\mathbb{Z}/m\mathbb{Z})$

Asamblea

Scanned by CamScanner