Fundamentos de teoría de números

Introducción a la Criptografía y a la Seguridad de la Información

Iván Castellanos

Departamento de ingeniería de sistemas e industrial
Universidad Nacional de Colombia

31 de octubre de 2019

Algoritmo de la división

Teorema

Dados $a, b \in \mathbb{Z}$ *con* $b > 0$, $\exists!\ q, r$ *con* $0 \leq r < b$ *tal que* $a = q * b + r$

Demostración.

Se demuestra probando que $S = \{a - x * b \mid x \in \mathbb{Z}, a - x * b \geq 0\}$ es no vacio y r es el mínimo de S □

Corolario

Dados $a, b \in \mathbb{Z}$ *con* $b \neq 0$, $\exists!\ q, r$ *con* $0 \leq r < |b|$ *tal que* $a = q * b + r$

Demostración.

Considerar $a = q' * |b| + r$ y notar que si $b < 0$ entonces $b = -|b|$ □

Algoritmo de la división

Ejemplo

$8 = 1 * 5 + 3$

$30 = 6 * 5 + 0$

Definición (Cociente)

Del teorema del algoritmo de la división q se llama *cociente* y en programación es el resultado de la *división entera piso* $\lfloor \frac{a}{b} \rfloor$

Definición (Residuo)

Del teorema del algoritmo de la división r se llama *módulo* o *resíduo* y en programación es el resultado de la operación *módulo*, se denota como a mod b

Algoritmo de la división

Ejemplo

$8 = 1 * 5 + 3$

$30 = 6 * 5 + 0$

Definición (Cociente)

Del teorema del algoritmo de la división q se llama *cociente* y en programación es el resultado de la *división entera piso* $\lfloor \frac{a}{b} \rfloor$

Definición (Residuo)

Del teorema del algoritmo de la división r se llama *módulo* o *resíduo* y en programación es el resultado de la operación *módulo*, se denota como a mod b

Ejercicio

¿Cuál es el cociente y el módulo de *-13* dividido entre *5*?

Congruencia modular

Definición (Congruencia modular)

Decimos que a es *congruente* con b módulo n, notado $a \equiv b (\text{mod } n)$ si el residuo de a entre n es igual al residuo de b entre n

Nota

Si $a \text{ mod } n \neq b \text{ mod } n$ decimos que a no es congruente con b modulo n y se denota $a \not\equiv b (\text{mod } n)$

Ejemplo

$7 \equiv 11 (\text{mod } 2)$
$40 \equiv 60 (\text{mod } 10)$
$14 \not\equiv 7 (\text{mod } 3)$

Divisibilidad

Definición (Divisibilidad)

Sean $a, b \in \mathbb{Z}$, a es *divisible* por b si $\exists k \in \mathbb{Z}$, tal que $a = b * k$.
b se dice que es un *divisor* de a y a es un *múltiplo* de b

Lema

para $b \neq 0$, a es divisible por b si y solo si el a módulo b es igual a 0

Nota

Notamos b es divisor de a o b divide a a como $b \mid a$ y b no divide a a como $b \nmid a$

Ejemplo

$4 \mid -12$, pues $-12 = 4 * (-3)$
$4 \nmid 10$, pues $10 = 4 * 2 + 2$

Propiedades divisibilidad

Sean $a, b, c, d \in \mathbb{Z}$ se cumple lo siguiente:

- $a \mid 0$ (múltiplo trivial)
- $\pm 1 \mid a$ y $\pm a \mid a$ (divisores triviales)
- $a \mid 1$ si y solo si $a = \pm 1$
- Si $a \mid b$ y $b \mid c$ entonces $a \mid c$
- Si $a \mid b$ y $c \mid d$ entonces $ac \mid bd$
- $a \mid b$ y $b \mid a$ si y solo si $a = \pm b$
- Si $a \mid b$ y $b \neq 0$ entonces $|a| \leq |b|$
- Si $a \mid b$ y $a \mid c$ entonces $\forall x, y \in \mathbb{Z}$ $a \mid (bx + cy)$

Nota

La ultima propiedad se puede generalizar por inducción:
Si $a \mid b_k$ para $k = 1, \ldots, n$ entonces para $\forall x_k \in \mathbb{Z}$, $a \mid \sum_{k=1}^{n} b_k * x_k$

Divisores de un número

- Podemos encontrar todos los divisores positivos de $n \in \mathbb{Z}^+$ en $O(n)$ iterando por todos los $a \in \mathbb{Z}^+$, $a \leq n$ revisando si $a \mid n$

Lema

Si $a \mid n$ *entonces* $a \leq \sqrt{n}$ *o* $\frac{n}{a} \leq \sqrt{n}$

- Por el lema anterior podemos calcular todos los divisores de n en $O(\sqrt{n})$

Nota

Si un numero n tiene β bits entonces $O(n) = O(2^{\beta})$ y $O(\sqrt{n}) = O(2^{\frac{\beta}{2}})$

Nota

Veremos mas adelante que es muy dificil encontrar una solución con menor complejidad a este problema

GCD

Definición (Máximo común divisor)

Sean $a, b \in \mathbb{Z}$ con $a \neq 0$ o $b \neq 0$, el *máximo común divisor (Greatest Common Divisor)* de a y b notado como $gcd(a, b)$ es un entero positivo d tal que:

- $d \mid a$ y $d \mid b$
- Si $c \mid a$ y $c \mid b$ entonces $c \mid d$

Definición (Coprimo)

Sean $a, b \in \mathbb{Z}$, a y b son *coprimos* si $gcd(a, b) = 1$

GCD

Sean $a, b, c \in \mathbb{Z}$ se cumple lo siguiente:

1. $gcd(a, b) = gcd(|a|, |b|) = gcd(b, a)$
2. $gcd(a, gcd(b, c)) = gcd(gcd(a, b), c)$
3. $gcd(a, a) = |a|$, $gcd(a, 0) = |a|$, $gcd(a, 1) = 1$
4. Si $gcd(a, b) = 1$ y $c \mid a$ entonces $gcd(a, c) = 1$
5. Si $gcd(a, b) = 1$ entonces $gcd(ac, b) = gcd(c, b)$
6. $gcd(a, b) = gcd(a - b, b)$ si $a > b$
7. $gcd(a, b) = gcd(a, b - a)$ si $b > a$
8. $gcd(a, b) = gcd(b, a \bmod b)$

GCD

Para calcular $gcd(a, b)$ podríamos calcular todos los divisores de a y b y tomar el mínimo que tengan en común

Nota

Gracias a las propiedades 3 y 8 podemos hacerlo mas eficiente

GCD(a, b):

if $b = 0$ **then**
  return a
else
  return $GCD(b, a \bmod b)$
end if

Nota

Este es el *algoritmo de euclides*, cuya complejidad es $O(\beta^3)$ para numeros de β bits

Algoritmo extendido de Euclides

El *algoritmo extendido de euclides* encuentra no solo $gcd(a, b)$ sino además $x, y \in \mathbb{Z}$ tal que $gcd(a, b) = a * x + b * y$

EEA(a, b):

if $b = 0$ **then**
  return $(a, 1, 0)$
else
  $(d', x', y') \leftarrow EEA(b, a \bmod b)$
  $q \leftarrow \lfloor \frac{a}{b} \rfloor$
  $(d, x, y) \leftarrow (d', y', x' - q * y')$
  return
end if

Algoritmo extendido de Euclides

El *algoritmo extendido de euclides* encuentra no solo $gcd(a, b)$ sino además $x, y \in \mathbb{Z}$ tal que $gcd(a, b) = a * x + b * y$

EEA(a, b):

if $b = 0$ **then**
  return $(a, 1, 0)$
else
  $(d', x', y') \leftarrow EEA(b, a \bmod b)$
  $q \leftarrow \lfloor \frac{a}{b} \rfloor$
  $(d, x, y) \leftarrow (d', y', x' - q * y')$
  return
end if

Ejercicio

calcule EEA(508, 103)

Ecuaciones diofantinas

Definición (Ecuación diofantina)

Una ecuación diofantina es una ecuación polinomial de una o mas variables donde se buscan unicamente *soluciones enteras*

Ejemplo

- $ax + by = c$ es una ecuación diofantina lineal
- $x^n + y^n = z^n$ es una ecuación muy conocida gracias a Pitágoras $(n = 2)$ y a Fermat $(n > 2)$

Nota

El nombre de estas ecuaciones viene del matemático Diophantus de Alenxadria quien estudió este tipo de ecuaciones en el siglo III

Ecuaciones diofantinas

Definición (Ecuación diofantina)

Una ecuación diofantina es una ecuación polinomial de una o mas variables donde se buscan unicamente *soluciones enteras*

Ejemplo

- $ax + by = c$ es una ecuación diofantina lineal
- $x^n + y^n = z^n$ es una ecuación muy conocida gracias a Pitágoras $(n = 2)$ y a Fermat $(n > 2)$

Nota

El nombre de estas ecuaciones viene del matemático Diophantus de Alenxadria quien estudió este tipo de ecuaciones en el siglo III

Ejercicio

Escriba 2 soluciones de la ecuación diofantina $508x + 103y = 4$

Ecuaciones diofantinas

Teorema

Sean $a, b \in \mathbb{Z}$, la ecuación diofantina $a*x+b*y=d$ tiene solucion(es) si y solo si $gcd(a,b) \mid d$

Ejemplo

Una solución de la ecuación diofantina de $2*x+6*y=14$ es $x=1,\ y=2$. Otra es $x=10,\ y=-1$

Corolario

Sean $a, b \in \mathbb{Z}$, la ecuación diofantina $a*x+b*y=1$ tiene solucion(es) si y solo si a y b son coprimos

Ejemplo

$2*x+6*y=1$ no tiene soluciones enteras

Teorema chino del resíduo

Considere el siguiente acertijo de Brahmagupta:

> *Una anciana va al mercado y un caballo se tropieza con ella y rompe su canasta de huevos. El jinete le ofrece pagar por los daños y le pregunta cuantos huevos tenía, ella no recuerda el numero exacto, pero cuando ella tomaba de a 2 huevos le sobraba uno. Lo mismo pasó cuando ella tomaba de a 3, 4, 5 o 6 al tiempo, pero cuando ella tomaba de a 7 huevos al tiempo no le sobraban. ¿Cuál es el menor numero de huevos que podía tener?*

Teorema chino del resíduo

Teorema (Chino del residuo)

Sean $n_1, n_2, ..., n_k \in \mathbb{Z}^+$ *donde cada pareja son coprimos y* $a_1, a_2, ..., a_k \in \mathbb{Z}$, *entonces el sistema de congruencias* $x \equiv a_i (mod\ n_i)\ \forall i \in \{1, ..., k\}$ *tiene una única solución módulo* $N = n_1 n_2 ... n_k$

$x = \sum_{i=1}^{k} N_i y_i a_i\ mod\ N$ *donde* $N_i = \frac{N}{n_i}$ *y* $y_i = N_i^{-1}\ mod\ n_i$

Demostración.

Considerar el caso para 2 ecuaciones, es decir, $x \equiv a_1 (\text{mod } n_1)$ y $x \equiv a_2 (\text{mod } n_2)$. Con este caso se puede generalizar □

Teorema chino del resíduo

Teorema (Chino del residuo)

Sean $n_1, n_2, ..., n_k \in \mathbb{Z}^+$ *donde cada pareja son coprimos y* $a_1, a_2, ..., a_k \in \mathbb{Z}$, *entonces el sistema de congruencias* $x \equiv a_i (mod\ n_i)\ \forall i \in \{1, ..., k\}$ *tiene una única solución módulo* $N = n_1 n_2 ... n_k$

$x = \sum_{i=1}^{k} N_i y_i a_i\ mod\ N$ *donde* $N_i = \frac{N}{n_i}$ *y* $y_i = N_i^{-1}\ mod\ n_i$

Demostración.

Considerar el caso para 2 ecuaciones, es decir, $x \equiv a_1 (\text{mod } n_1)$ y $x \equiv a_2 (\text{mod } n_2)$. Con este caso se puede generalizar □

Ejercicio

Encontrar $x \in \mathbb{Z}$ tal que $x \equiv 1 (\text{mod } 5)$ y $x \equiv 2 (\text{mod } 7)$

Primalidad

Definición (Numeros primos)

Un número $p \in \mathbb{Z}^+$, $p > 1$ es un número *primo* si sus únicos divisores positivos son 1 y p, en caso contrario se dice que el número es *compuesto*

Ejemplo

2, 11, 1000000007 son algunos números primos

Lema

Sea p primo, p es coprimo con todos los números $a \in \mathbb{Z}$, $1 \leq a < p$

Nota

Podemos calcular si un numero n es primo o no mirando los divisores de n en $O(\sqrt{(n)})$

Factorización prima

Teorema (Fundamental de la aritmética)

Todo $n \in \mathbb{Z}^+$ con $n > 1$ puede ser expresado como un producto de primos, esta representación es única aparte del orden en el que ocurren los factores

Definición (Factorización prima)

La factorización prima de $n \in \mathbb{Z}$, $n > 1$ la notamos como $n = p_1^{q_1} p_2^{q_2} ... p_k^{q_k}$ con $p_1 < p_2 < ... < p_k$ primos y $q_1, q_2, ..., q_k > 0$

Nota

Podemos calcular la factorización prima de un número n en $O(\sqrt{(n)})$

Distribución de primos

Definición ($\pi(n)$)

$\pi(n)$ es la función que cuenta el numero de primos menores a n

Ejemplo

$\pi(10) = 4$, $\pi(100) = 25$

Teorema (Distribución de los números primos)

$\pi(n) \sim \frac{n}{\ln n}$

Nota

Podemos calcular todos los primos menores a n con la criba de Eratóstenes en $O(n)$ (en tiempo y memoria)

Phi de Euler

Definición ($\phi(n)$)

Para $n \in \mathbb{Z}$, $n > 1$ la función $\phi(n)$ (Phi de Euler) denota el número de enteros positivos menores o iguales a n que son coprimos con n

Ejemplo

$\phi(16) = 8$, $\phi(5) = 4$

Lema

Si p es primo y $k \in \mathbb{Z}$, $k > 1$ entonces
$\phi(p^k) = p^k - p^{k-1} = p^k(1 - \frac{1}{p})$

Nota

Podemos calcular $\phi(n)$ en $O(n \log n)$ mirando el *gcd* para todos los numeros enteros menores o iguales a n

Phi de Euler

Teorema

$\phi(n)$ es una función multiplicativa para coprimos, es decir, si $gcd(n,m) = 1$ entonces $\phi(nm) = \phi(n)\phi(m)$

Corolario

Sea $n = p_1^{q_1} p_2^{q_2} ... p_k^{q_k}$, $\phi(n) = n(1 - \frac{1}{p_1})(1 - \frac{1}{p_2})...(1 - \frac{1}{p_k})$

Nota

Con lo anterior podemos reducir el problema de calcular $\phi(n)$ al de la factorización prima de n

Congruencia modular

Teorema

Sea $n \in \mathbb{Z}^+$ la congruencia modulo n es una relación de equivalencia sobre $\mathbb{Z}$

Nota

Una relación de equivalencia es una relación *reflexiva*, *simétrica* y *transitiva*

Definición (Clases de equivalencia)

Dada una relacion de equivalencia $\sim$ en S, la clase de equivalencia de un elemento $a \in S$ es el conjunto $[a] = \{x \in S \mid x \sim a\}$

Ejemplo

Sobre la congruencia modulo 2 tenemos 2 clases de equivalencia: $[0] =$ numeros pares y $[1] =$ numeros impares

$\mathbb{Z}_n$

Definición ($\mathbb{Z}_n$)

Sea $n \in \mathbb{Z}^+$, $\mathbb{Z}_n = \{[x]_n \mid x = 0, \ldots, n-1\}$ donde $[x]_n$ corresponde a la clase de equivalencia de x con la congruencia módulo n

Definición (Operaciones en $\mathbb{Z}_n$)

En $\mathbb{Z}_n$ definimos $+$ y $*$ como $[a]_n + [b]_n = [a+b]_n$ y $[a]_n * [b]_n = [a*b]_n$

Teorema

Las operaciones $+$ y $*$ en $\mathbb{Z}_n$ están bien definidas

Nota

Por simplicidad podemos notar $[x]_n$ como x si sabemos que $x \in \mathbb{Z}_n$

Grupos

Definición (Grupo)

Un grupo $\langle G, \cdot \rangle$ es un conjunto G con una operación binaria cerrada $\cdot$ con las siguientes propiedades:

- $\forall a, b, c \in G,\ (a \cdot b) \cdot c = a \cdot (b \cdot c)$ (asociatividad de $\cdot$)
- $\exists e \in G$ tal que $\forall x \in G,\ e \cdot x = x \cdot e = x$ (elemento neutro de $\cdot$)
- $\forall x \in G\ \exists x' \in G,\ x \cdot x' = x' \cdot x = e$ (inverso de x)

Definición (Grupo Abeliano)

Sea $\langle G, \cdot \rangle$ un grupo, decimos que es un *grupo abeliano* o conmutativo si:

- $\forall a, b \in G,\ a \cdot b = b \cdot a$ (conmutatividad de $\cdot$)

Ejemplo

$\langle \mathbb{Z}, + \rangle$, $\langle \mathbb{Z}_n, + \rangle$ y $\langle \mathbb{Q}^+, * \rangle$ son grupos abelianos.

Anillos

Definición (Anillo)

Un *anillo* $\langle A, +, \cdot \rangle$ es un conjunto A con dos operaciones binarias cerradas $+$ y $\cdot$ con las siguientes propiedades:

- $\langle A, + \rangle$ es un grupo abeliano
- $\cdot$ es asociativa
- $\forall a, b, c \in A,\ a \cdot (b + c) = (a \cdot b) + (a \cdot c)$ (distributividad por izquierda) y $(a + b) \cdot c = (a \cdot c) + (b \cdot c)$ (distributividad por derecha)

Definición (Anillo conmutativo)

Un anillo $\langle A, +, \cdot \rangle$ es conmutativo si $\cdot$ es conmutativo

Definición (Anillo con unidad)

Un anillo $\langle A, +, \cdot \rangle$ tiene unidad si $\cdot$ tiene elemento neutro

Anillos

Ejemplo

- $\langle \mathbb{Z}, +, * \rangle, \langle \mathbb{Q}, +, * \rangle \langle \mathbb{R}, +, * \rangle$ y $\langle \mathbb{C}, +, * \rangle$ son anillos conmutativos con unidad
- $\langle n\mathbb{Z}, +, * \rangle$ es un anillo conmutativo sin unidad
- $\langle \mathbb{R}^{n \times n}, +, * \rangle$ es un anillo no conmutativo con unidad
- $\langle \mathbb{Z}_n, +, * \rangle$ es un anillo conmutativo con unidad

Dominios enteros

Definición (Divisores no triviales de cero)

En un anillo $\langle A, +, \cdot \rangle$ hay *divisores no triviales* de 0, si $\exists a, b \in A$, $a \neq 0$, $b \neq 0$ y $a \cdot b = 0$

Definición (Domino entero)

Un *dominio de integridad* o *dominio entero* $\langle I, +, \cdot \rangle$ es un anillo conmutativo con unidad, que no tiene divisores no triviales de cero

Ejemplo

- $\langle \mathbb{Z}, +, * \rangle, \langle \mathbb{Q}, +, * \rangle \langle \mathbb{R}, +, * \rangle$ y $\langle \mathbb{C}, +, * \rangle$ son dominios enteros
- $\langle \mathbb{Z}_{50}, +, * \rangle$ no es un dominio entero

Cuerpos

Definición (Inverso multiplicativo)

Sea $\langle A, +, \cdot \rangle$ un anillo con unidad, decimos que $x \in A$ tiene inverso multiplicativo si $\exists x' \in A$ tal que $x \cdot x' = x' \cdot x = 1$, donde 1 es la unidad. Notamos al inverso multiplicativo de x como x^{-1}

Definición ($\mathbb{Z}_n^*$)

$\langle \mathbb{Z}_n^*, * \rangle$ es el *grupo* de los elementos con inverso multiplicativo de $\mathbb{Z}_n$

Cuerpos

Definición (Inverso multiplicativo)

Sea $\langle A, +, \cdot \rangle$ un anillo con unidad, decimos que $x \in A$ tiene inverso multiplicativo si $\exists x' \in A$ tal que $x \cdot x' = x' \cdot x = 1$, donde 1 es la unidad. Notamos al inverso multiplicativo de x como x^{-1}

Definición ($\mathbb{Z}_n^*$)

$\langle \mathbb{Z}_n^*, * \rangle$ es el *grupo* de los elementos con inverso multiplicativo de $\mathbb{Z}_n$

Ejercicio

Calcule los elementos de $\langle \mathbb{Z}_9^*, * \rangle$

Cuerpos

Definición (Inverso multiplicativo)

Sea $\langle A, +, \cdot \rangle$ un anillo con unidad, decimos que $x \in A$ tiene inverso multiplicativo si $\exists x' \in A$ tal que $x \cdot x' = x' \cdot x = 1$, donde 1 es la unidad. Notamos al inverso multiplicativo de x como x^{-1}

Definición ($\mathbb{Z}_n^*$)

$\langle \mathbb{Z}_n^*, * \rangle$ es el *grupo* de los elementos con inverso multiplicativo de $\mathbb{Z}_n$

Ejercicio

Calcule los elementos de $\langle \mathbb{Z}_9^*, * \rangle$

Teorema

$a \in \mathbb{Z}_n^*$ si y solo si $gcd(a, n) = 1$

Cuerpos

Definición (Cuerpo)

$\langle A, +, \cdot \rangle$ es un *cuerpo* o *campo* si es $\langle A, +, \cdot \rangle$ un anillo conmutativo con unidad que tiene inversos multiplicativos $\forall x \in A,\ x \neq 0$, donde 0 es el elemento neutro de $+$

Ejemplo

- $\langle \mathbb{Z}, +, * \rangle$ no es un cuerpo
- $\langle \mathbb{Q}, +, * \rangle, \langle \mathbb{R}, +, * \rangle$ y $\langle \mathbb{C}, +, * \rangle$ son cuerpos

Teorema

Sea p primo, $\mathbb{Z}_p$ es un cuerpo

Teorema

Todo cuerpo es un dominio entero

$F[x]$

Definición (Polinomio)

Sea $\mathbb{F}$ un cuerpo, un polinomio $f(x) : \mathbb{F} \to \mathbb{F}$ de define como $f(x) = \sum_{i=0}^{\infty} a_i x^i$ donde $a_i \in \mathbb{F}$ y $a_i \neq 0$ para un numero finito de valores

Definición

$\mathbb{F}[x]$ es el conjunto de todos los polinomios sobre $\mathbb{F}$

Definición (Grado)

Sea $f(x) = \sum_{i=0}^{\infty} a_i x^i \in \mathbb{F}[x]$, el *grado del polinomio* $f(x)$ es el valor $n \in \mathbb{Z}$ tal que $a_n \neq 0$ y $a_i = 0 \ \forall i > n$

Nota

Si n es el grado de $f(x)$, podemos escribir $f(x) = \sum_{i=0}^{n} a_i x^i$

Dominio entero $F[x]$

Ejercicio

Sea $f(x) = 4x^3 + 2x + 1$, $p(x) \in \mathbb{Z}_5[x]$. Calcule $f(3)$

Dominio entero $F[x]$

Ejercicio

Sea $f(x) = 4x^3 + 2x + 1$, $p(x) \in \mathbb{Z}_5[x]$. Calcule $f(3)$

Sean $f(x) = \sum_{i=0}^{\infty} a_i x^i, g(x) = \sum_{i=0}^{\infty} b_i x^i \in \mathbb{F}[x]$ definimos la suma y multiplicación como:

- $f(x) + g(x) = \sum_{i=0}^{\infty} c_i x^i$ donde $c_i = a_i + b_i$
- $f(x) * g(x) = \sum_{i=0}^{\infty} c_i x^i$ donde $c_i = \sum_{j+k=i} a_j * b_k$

Teorema

$\langle \mathbb{F}[x], +, * \rangle$ *es un dominio entero, pero no es un cuerpo*

Nota

Note que $\mathbb{F}[x]$ y $\mathbb{Z}$ son dominios enteros, pero no son cuerpos. Comparten varias similitudes algebráicas

Algoritmo de la división

Teorema

Sean $f(x), g(x) \in \mathbb{F}[x]$ *polinomios de grado* n *y* m *respectivamente, con* $m > 0$, $\exists!\ q(x), r(x) \in \mathbb{F}[x]$ *tal que* $f(x) = g(x) * q(x) + r(x)$ *donde el grado de* $r(x)$ *es estrictamente menor a* m

Nota

$q(x)$ se llama *cociente*, $r(x)$ se llama *residuo* o *módulo*

Algoritmo de la división

Teorema

Sean $f(x), g(x) \in \mathbb{F}[x]$ *polinomios de grado* n *y* m *respectivamente, con* $m > 0$, $\exists!\ q(x), r(x) \in \mathbb{F}[x]$ *tal que* $f(x) = g(x) * q(x) + r(x)$ *donde el grado de* $r(x)$ *es estrictamente menor a* m

Nota

$q(x)$ se llama *cociente*, $r(x)$ se llama *residuo* o *módulo*

Ejercicio

Sean $f(x) = 3x^3 - 3x^2 + 3x + 1$ y $g(x) = 2x^2 - 2x - 4$, $f(x), g(x) \in \mathbb{Z}_5[x]$ calcular $q(x)$ y $r(x)$

Polinomios irreducibles

Definición (Polinomio irreducible)

Sea $p(x) \in \mathbb{F}[x]$ un polinomio de grado n, $p(x)$ es un *polinomio irreducible* si $\forall g(x), h(x) \in \mathbb{F}[x]$ con $h(x)$ y $g(x)$ polinomios de grado menor a n, $p(x) \neq g(x) * h(x)$

Ejemplo

$p(x) = x^3 + 3x + 2 \in \mathbb{Z}_5[x]$ es irreducible

Ejemplo

$p(x) = x^8 + x^4 + x^3 + x + 1 \in \mathbb{Z}_2[x]$ es irreducible

Nota

Note que la definición de polinomio irreducible en $\mathbb{F}[x]$ es muy similar a la de números primos en $\mathbb{Z}$

Campos finitos

Teorema

Sea $\mathbb{F}$ un campo finito, entonces $\forall n \in \mathbb{Z}^+$, $\exists p(x) \in \mathbb{F}[x]$ polinomio irreducible de grado n

Nota

Al igual que a partir de un número primo p podemos construir el campo $\mathbb{Z}_p$, con un polinomio irreducible $p(x) \in \mathbb{F}[x]$ podemos construir el campo $\mathbb{F}[x]_{p(x)}$ tomando las clases de equivalencia de la congruencia modular con $p(x)$

Teorema

Si el campo $\mathbb{F}$ tiene a elementos, el campo $\mathbb{F}[x]_{p(x)}$ donde $p(x)$ es polinomio irreducible de grado n tiene a^n elementos

Campos de Galois

Teorema

Si $\mathbb{F}$ es un campo finito entonces $|\mathbb{F}| = p^n$ donde p es un numero primo y $n \in \mathbb{Z}^+$, además $\mathbb{F}$ es el único campo (salvo isomorfismos) de tamaño p^n

Definición (Campo de Galois)

El campo de Galois de tamaño p^n notado $GF(p^n)$ es el campo de tamaño p^n

Nota

Estos campos son llamados así por el matemático Evariste Galois

Campos de Galois

Teorema

Si $\mathbb{F}$ es un campo finito entonces $|\mathbb{F}| = p^n$ donde p es un numero primo y $n \in \mathbb{Z}^+$, además $\mathbb{F}$ es el único campo (salvo isomorfismos) de tamaño p^n

Definición (Campo de Galois)

El campo de Galois de tamaño p^n notado $GF(p^n)$ es el campo de tamaño p^n

Nota

Estos campos son llamados así por el matemático Evariste Galois

Ejercicio

Calcule $GF(2^2)$. Note que debe tener el conjunto junto a las operaciones $+$ y $*$. Utilice el polinomio irreducible $x^2 + x + 1$

Exponenciación

Definición (Exponenciación)

Dado un anillo con unidad $\langle A, +, * \rangle$ podemos definir la operación exponenciación, dado $a \in A$ y $n \in \mathbb{N}$, como $a^0 = 1$ y $a^n = a^{n-1} * a$

Nota

Podemos calcular a^n haciendo $O(n)$ multiplicaciones

Existen ciertas propiedades que nos ayudarán a calcular exponenciaciones de manera eficiente

- $a^{n_0} * a^{n_1} * \ldots * a^{n_k} = a^{n_0 + n_1 + \ldots + n_k}$
- $(a^n)^2 = a^{2n}$
- si $n \in \mathbb{N}$ entonces $n = \sum_{i=0}^{k} b_i * 2^i$ (n en binario)

Exponenciación modular

Utilizando lo anterior podremos resolver a^b en $\mathbb{Z}_n$ eficientemente ***PowerMod(a, b, n):***

$curr \leftarrow a \bmod n$, $res \leftarrow 1$
while $b > 0$ **do**
  if $b \bmod 2 = 1$ **then**
    $res \leftarrow (res * curr) \bmod n$
  end if
  $curr \leftarrow (curr * curr) \bmod n$
  $b \leftarrow \lfloor \frac{b}{2} \rfloor$
end while
return res

Complejidad

Si a y b son numeros de β bits la complejidad es $O(\beta^3)$

Teorema de Euler

Teorema (de Euler)

Dados $a, n \in \mathbb{Z}$ *coprimos,* $a^{\phi(n)} \equiv 1 (mod\ n)$

Corolario (Teorema pequeño de Fermat)

Dados $a, p \in \mathbb{Z}$, *con* p *primo,* $a^{p-1} \equiv 1 (mod\ p)$

Nota

El inverso multiplicativo de a en $\mathbb{Z}_p$ es a^{p-2}

Teorema de Euler

Teorema (de Euler)

Dados $a, n \in \mathbb{Z}$ *coprimos,* $a^{\phi(n)} \equiv 1 (mod\ n)$

Corolario (Teorema pequeño de Fermat)

Dados $a, p \in \mathbb{Z}$, *con* p *primo,* $a^{p-1} \equiv 1 (mod\ p)$

Nota

El inverso multiplicativo de a en $\mathbb{Z}_p$ es a^{p-2}

Ejercicio

Calcule $2019^{987654321}$ mod 22

Elementos primitivos

Definición (Orden de un entero)

Sea A un anillo con unidad, si a tiene inverso multiplicativo en A, el orden de $a \in A$ es define como $ord_A(a) = min\{k \in \mathbb{Z}^+ \mid a^k = 1\}$

Teorema

Sea $k = ord_A(a)$, $a^h = 1$ *si y solo si* $k \mid h$

Corolario

$a^x = a^y$ *si y solo si* $x \equiv y (mod\ ord_A(a))$

Corolario

Si $a \in \mathbb{Z}_n^*$, *entonces* $ord_{\mathbb{Z}_n}(a) \mid \phi(n)$

Elementos primitivos

Definición (Elemento primitivo)

Sea $\mathbb{F}$ un cuerpo finito, $\alpha \in \mathbb{F}$ es un elemento primitivo de $\mathbb{F}$ si $\{\alpha^i \mid i \in \mathbb{N}\} = \mathbb{F} - \{0\}$

Ejemplo

$x+1$ o 00000011 (03) es un elemento primitivo de $GF(2^8)$

Teorema

La cantidad de elementos primitivos en un cuerpo finito $\mathbb{F}$ *es* $\phi(|\mathbb{F}|-1)$

Elementos primitivos

Definición (Elemento primitivo)

Sea $\mathbb{F}$ un cuerpo finito, $\alpha \in \mathbb{F}$ es un elemento primitivo de $\mathbb{F}$ si $\{\alpha^i \mid i \in \mathbb{N}\} = \mathbb{F} - \{0\}$

Ejemplo

$x+1$ o 00000011 (03) es un elemento primitivo de $GF(2^8)$

Teorema

La cantidad de elementos primitivos en un cuerpo finito $\mathbb{F}$ *es* $\phi(|\mathbb{F}|-1)$

Ejercicio

¿Cuantos elementos primitivos tiene $GF(2^8)$?

Elementos primitivos

Lema

a es elemento primitivo de $\mathbb{F}$ *si y solo si* $ord(a) = |\mathbb{F}| - 1$

Ejemplo

Encontrar los elementos primitivos de $\mathbb{Z}_7$

i	1	2	3	4	5	6	$ord_7(a)$
$a = 2, 2^i \mod 7$	2	4	1	2	4	1	3
$a = 3, 3^i \mod 7$	3	2	6	4	5	1	6
$a = 4, 4^i \mod 7$	4	2	1	4	2	1	3
$a = 5, 5^i \mod 7$	5	4	6	2	3	1	6
$a = 6, 6^i \mod 7$	6	1	6	1	6	1	2

Luego los elementos primitivos de $\mathbb{Z}_7$ son 3 y 5

Elementos primitivos

Teorema

Si $ord(a) = |\mathbb{F}| - 1$ *entonces* $a^{\frac{|\mathbb{F}|-1}{q}} \neq 1$ *para todo* q *primo divisor de* $|\mathbb{F}| - 1$

Nota

Por el lema anterior dado $a \in \mathbb{Z}_p^*$ podriamos saber si a es elemento primitivo de $\mathbb{Z}_p$ solo con pocas exponenciaciones

Lema

si tomamos de manera aleatoria $a \in \mathbb{Z}_p^*$ *la probabilidad de que a sea un elemento primitivo de* $\mathbb{Z}_p$ *es* $\frac{\phi(p-1)}{p-1}$

Nota

Tomando en cuenta lo anterior podemos encontrar elementos primitivos con un *algoritmo aleatorizado*

Logaritmo discreto

Definición (Problema del logaritmo discreto)

Sea p un número primo, $a \in \mathbb{Z}_p^*$ un elemento primitivo de $\mathbb{Z}_p$ y $b \in \mathbb{Z}_p^*$, el *problema del logaritmo discreto (DLP)* consiste en encontrar $x \in \mathbb{Z}_{\phi(p)}$ tal que $a^x \equiv b \pmod{p}$, denotamos x como $\log_a b \pmod{p}$

Nota

Podemos resolver el DLP en $O(p)$ haciendo busqueda exhaustiva o en $O(1)$ precomputando los valores usando $O(p)$ espacio. Si p tiene β bits $O(p) = O(2^\beta)$

Test de primalidad

- Ya mencionamos anteriormente que el problema de la primalidad (verificar si un número n es primo o no) es *dificil*
- Utilizando los teoremas anteriores veremos un enfoque *probabilístico* para resolver este problema

Definición (Pseudoprimo)

Un número n es *pseudoprimo base* a ($a \neq 0$), si n es compuesto y $a^{n-1} \equiv 1 (\text{mod } n)$

Nota

Note que si $a^{n-1} \not\equiv 1 (\text{mod } n)$ para $a \neq 0$ entonces n es compuesto

Test de primalidad de Fermat

Definición (Test de Fermat)

Dado n podemos calcular a^{n-1} para varios numeros $a \in \mathbb{Z}_n$ $(a > 1)$, si $a^{n-1} \not\equiv 1 (\text{mod } n)$ estamos 100 % seguros que n es compuesto. Si $a^{n-1} \equiv 1 (\text{mod } n)$, entonces n es primo o pseudoprimo base a. Este procedimiento es conocido como *test de Fermat*

Definición (Números de Carmichael)

n es un número de Carmichael si n es pseudoprimo base a $\forall a \in \mathbb{Z}_n^*$

Teorema

Existen infinitos números de Carmichael pero su distribución es muy baja

Ejemplo

El primer número de Carmichael es 561

Test de primalidad de Miller-Rabin

Teorema

Sea p primo y $x^2 \equiv 1 (mod\ p)$, entonces $x = 1$ o $x = p - 1$

Demostración.

Es inmediato considerando el hecho que $\mathbb{Z}_p$ es un campo y por ende no tiene divisores de 0 □

Nota

Note que si $x \not\equiv \pm 1 (\text{mod } n)$ y $x^2 \equiv 1 (\text{mod } n)$ entonces n es compuesto

Test de primalidad de Miller-Rabin

Definición (Witness)

Sea $n \in \mathbb{Z}^+$ impar, $n-1 = 2^k q$, con q impar, dado $a \in \mathbb{Z}_n$ si $a^{2^0 q} = a^q \equiv \pm 1 (\text{mod } n)$ entonces n es primo o pseudoprimo base a, en caso contrario procedemos a calcular $a^{2^1 q}, a^{2^2 q} ..., a^{2^k q}$. Si para algún $0 \leq i < k$, $a^{2^i q} \not\equiv \pm 1 (\text{mod } n)$ y $a^{2^{i+1} q} \equiv 1 (\text{mod } n)$ entonces estamos 100 % seguros que n numero es compuesto, en caso contrario n es *probablemnte primo*. Esto es conocido como la función *witness*

Definición (Test de Miller-Rabin)

Dado n, el *test de Miller-Rabin* consiste en aplicar la función *witness* para diferentes $a \in \mathbb{Z}_n$

Test de primalidad de Miller-Rabin

WITNESS(a, n):

sean k y q, tal que $n-1 = 2^k q$
$x_0 \leftarrow a^q \bmod n$
for $i \leftarrow 0$ hasta k **do**
  $x_i \leftarrow (x_{i-1})^2 \bmod n$
  if $x_i = 1$ y $x_{i-1} \neq \pm 1$ **then**
    return *true*
  end if
end for
if $x_k \neq 1$ **then**
  return *true*
end if
return *false*

Miller-Rabin(n, s):

for $i \leftarrow 1$ hasta s **do**
  $a \leftarrow RANDOM(2, n-1)$
  if $WITNESS(a, n)$ **then**
    return *compuesto*
  end if
end for
return *primo*

Test de primalidad de Miller-Rabin

Teorema

Los numeros de Carmichael fallan facilmente el test de primalidad de Miller-Rabin

Nota

A diferencia del test de Fermat, no hay malos n para el test de Miller-Rabin, la probabilidad de fallo dependerá solo de la *suerte* seleccionando a y la cantidad de intentos s

Teorema

Dado $n \in \mathbb{Z}$ impar, $n > 2$ y $s \in \mathbb{Z}^+$, la probabilidad de error de Miller-Rabin(n, s) es a lo sumo 2^{-s}

Generación de primos

- Para varios algoritmos de criptografía necesitaremos números primos muy grandes
- Teniendo un generador de números aleatorios debemos lograr un número primo sin muchos intentos

Consideremos $n \in \mathbb{Z}^+$ un número con β bits y los eventos A: n es primo y B: $\mathit{Miller\text{-}Rabin}(n, s) = \mathit{primo}$

Lema

$$P(A) \approx \frac{1}{\ln n} \approx \frac{1{,}443}{\beta}$$

Nota

El valor de intentos esperados para obtener un primo es $\approx \frac{\beta}{1{,}443}$

Generación de primos

- $P(\overline{B} \mid A) = 0$
- $P(B \mid A) = 1$
- $P(B \mid \overline{A}) \leq 2^{-s}$
- $P(\overline{B} \mid \overline{A}) > 1 - 2^{-s}$

Lema

$P(A \mid B) \geq \frac{1}{1+2^{-s}(\ln n - 1)}$

Demostración.

$P(A \mid B) = \frac{P(A)P(B \mid A)}{P(A)P(B \mid A) + P(\overline{A})P(B \mid \overline{A})}$ □

Nota

Para cualquier aplicación imaginable basta con $s = 50$ y de hecho en la práctica podemos usar valores pequeños con buenos resultados