Number Theory & Cryptography - Weekly meetings

Curso en Zacatecas [Q1 2015]

Luis J. Dominguez Perez

CIMAT-Zac, Enero 21 de 2015

Contenido, sección 1

Los seis fundamentales

Hay seis conceptos elementales que necesitan enfatizarse en las matemáticas de la criptografía. Sea S un conjunto de elementos, y $+$, $\times$, $\odot$ operadores binarios en S:

- Cerradura: S está cerrado sobre $\odot$ si para todo $a, b \in S$, $a \odot b \in S$
- Asociatividad

$$a \odot (b \odot c) = (a \odot b) \odot c.$$

los elementos en $\mathbb{R}$ son asociativos sobre $+$, y $\times$.

. . . los seis fundamentales

- Conmutabilidad: S es conmutativa sobre $\odot$ si para todo $a, b, c \in S$:

$$a \odot b = b \odot a$$

los elementos en $\mathbb{R}$ son conmutativos sobre $+$, y $\times$.

- Distributiva: S es distributivo sobre $+$ si para todo $a, b, c \in S$:

$$a \times (b + c) = (a \times b) + (a \times c)$$

los elementos en $\mathbb{R}$ son distributivos sobre la suma

. . . los seis fundamentales

- Identidad: El elemento $I \in S$ es una identidad sobre $+$ si para todo $a \in S$:

$$a + I = I + a = a$$

los elementos en $\mathbb{R}$ tienen el 0 como elemento identidad para la suma, y el 1 para la multiplicación

- Inverso: Sean $0, 1 \in S$ las identidades aditivas y multiplicativas, respectivamente, de S. Un elemento $a \in S$ es el inverso aditivo de $b \in S$ si $a + b = b + a = 0$. Es el inverso multiplicativo si $a \times b = b \times a = 1$. Por ejemplo, 2 es el inverso aditivo de -2 (y viceversa), mientras que 0.5 es su inverso multiplicativo.

Estructuras algebraicas

- Las estructuras algebraicas son el corazón de la mayoría de los criptosistemas y de los ataques criptoanalíticos.

- Sea G un conjunto de elementos, y $+, \times, \odot$ operadores binarios mapeando G a G, recordando las propiedades básicas discutidas en el inicio, tenemos que. . .

Objetos básicos

Los objetos matemáticos básicos son:

- Semigrupo: $\langle G, \odot \rangle$ es un semigrupo si G es cerrado y asociativo bajo $\odot$
- Monoide: $\langle G, \odot \rangle$ es un monoide si es un semigrupo, y existe un elemento identidad $e \in G$
- Grupo: $\langle G, \odot \rangle$ es un grupo si es un monoide, y existe un inverso para todo $a \in G$.
- Grupo abeliano: $\langle G, \odot \rangle$ es un grupo abeliano si es un grupo, y si $\odot$ es conmutativo
- Anillo: $\langle G, +, \times \rangle$ es un anillo si $\langle G, + \rangle$ es un grupo abeliano con identidad 0, $\langle G - \{0\}, \times \rangle$ es un monoide con identidad 1, y mantiene la propiedad distributiva bajo $+$
- Campo: $\langle G, +, \times \rangle$ es un campo si es un anillo, y $\langle G - \{0\}, \times \rangle$ es un grupo abeliano.

Ejemplos de estructuras algebraicas

Estructura	Monoide	Grupo	G. Abeliano	Anillo	A. Conmutativo	Campo
$\langle \mathbb{Q}^{n\times n}, \times \rangle$	✓	×	×	×	×	×
$\langle \mathbb{Q}^{n\times n}(inv), \times \rangle$	✓	✓	×	×	×	×
$\langle \mathbb{Z}, + \rangle$	✓	✓	✓	×	×	×
$\langle \mathbb{Q}^{n\times n}, +, \times \rangle$	–	–	–	✓	×	×
$\langle \mathbb{Z}/(15)\mathbb{Z}, +, \times \rangle$	–	–	–	✓	✓	×
$\langle \mathbb{Z}/(17)\mathbb{Z}, +, \times \rangle$	–	–	–	✓	✓	✓

- Las estructuras más utilizadas son los campos infinitos: $\mathbb{Q}, \mathbb{R}, \mathbb{C}$.
- En criptografía, las estructuras más utilizadas son las estructuras finitas, principalmente los grupos abelianos y los campos.

Observaciones sobre las estructuras

- En el caso de la criptografía, los campos utilizados son los *Campos Finitos* (también conocidos como *Campos de Galois*).
- Los campos finitos son los enteros módulo un primo p, o una potencia $q = p^m$, denotados como $\mathbb{F}_q$, o $\mathbb{Z}/q\,\mathbb{Z}$. Con $m \in \mathbb{Z}$, pudiendo ser un número compuesto.
- En el caso de ser una potencia prima, se les conoce como *extensión de campo*

observaciones

- Utilizar la q es una generalización para describir el campo finito. Algunos autores prefieren utilizar p, o la potencia explícita según les convenga.
- Un caso interesante es cuando el primo es 2, o 3. Adicionalmente, la potencia m compuesta por $2^i 3^j$, con $i, j \in \mathbb{Z}$, sin ser ambos cero, es popular.

- *Recientemente* se incluyen como estructuras algebraicas comunes a los grupos abelianos de puntos en curvas elípticas sobre un campo finito (o su extensión): $E(\mathbb{F}_p)$, $E_1(\mathbb{F}_{2^{1971}})$, $E'(\mathbb{F}_{p^d})$, ...

Subestructuras

Un subgrupo/campo es un subconjunto del conjunto original, el cual es cerrado bajo ciertas operaciones, y tiene las mismas propiedades que el original.

- Por ejemplo, $\mathbb{Z}/(15)\mathbb{Z}$ es un anillo, el subconjunto $\{0, 3, 6, 9, 12\}$ es cerrado, asociativo, y conmutativo bajo la adición, además, ya que tiene un elemento identidad, también es un subgrupo abeliano de $\mathbb{Z}/(15)\mathbb{Z}$ bajo la adición.

Orden

- Sea $\langle G, \odot \rangle$ un grupo con un elemento identidad e. El orden de G, escrito como ord(G), u $|G|$ es el número de elementos en G. Si G es infinito, también lo es su orden.
- Otro tipo de orden existe para elementos en G. Si $a \in G$, entonces el orden de a es el entero positivo más chico $n > 0$, tal que:

$$\overbrace{a \odot a \odot \ldots \odot a}^{n \text{ times}} = 1$$

Si no existe n, entonces ord$(a) = \infty$.

Ejemplos

G	$\mathsf{ord}(G)$	a	$\mathsf{ord}(a)$
$\langle \mathbb{F}_{19}, \times \rangle$	18	7	3
$\langle \mathbb{F}_{19}, + \rangle$	19	7	19
$\langle \mathbb{F}_{17}, \times \rangle$	16	2	8
$\langle \{1, 3, 5, 9, 13\} \subset \mathbb{Z}/(14)\mathbb{Z}, \times \rangle$	6	11	3
$\langle \mathbb{Q}, \times \rangle$	∞	-1	2

Contenido de la sección 2

Divisibilidad

- Un concepto central en la teoría de números es la *divisibilidad*.
- Sean $a, b \in \mathbb{Z}$, se dice que a **divide** b (denotado como: $a|b$) si $az = b$ para algún $z \in \mathbb{Z}$. Se dice que a es un **divisor** de b, que b es un **múltiplo** de a, o que b es **divisible por** a. Si a no divide b, entonces se escribe como: $a \nmid b$

Sobre la divisibilidad

Para todo $a, b, c \in \mathbb{Z}$, tenemos que:

- $a|a$, $1|b$, y $a|0$
- $0|b$ sí y solo si $b = 0$
- $a|b$ sí y solo si $-a|b$, sí y solo sí $a| - b$
- $a|b$ y $a|c$, implica que $a|(b + c)$
- $a|b$ y $b|c$, implica que $a|c$.

Observación: si $a|b$ y $b \nmid 0$, entonces $q \leq |a| \leq |b|$. De hecho, si $az = b \nmid 0$ para algún entero z, entonces $a \nmid 0$ y $z \nmid 0$; por lo que $|a| \geq 1$, $z \geq 1$, y $|a| \leq |a||z| = |b|$.

Sobre la divisibilidad

Teorema

Para todo $a, b \in \mathbb{Z}$, se tiene que $a|b$ y $b|a$ sí y sólo si $a = \pm b$. En particular, para todo $a \in \mathbb{Z}$, tenemos que $a|1$ sí y sólo si $a = \pm 1$

Sobre la divisibilidad

Proof.

Si $a = \pm b$, entonces $a|b$ y $b|a$. Asumamos que $a|b$ y que $b|a$ para probar que $a + \pm b$. Si a o b son cero, entonces el otro debe ser cero también. Asumamos que ninguno es cero. $a|b$ implica que $|a| \leq |b|$, y $b|a$ implica que $|b| \leq |a|$; por lo que $|a| = |b|$, entonces $a = \pm b$. Esto prueba la primera parte. La segunda parte viene de poner a $b = 1$, entonces $1|a$ En el pizarrón □

Números Primos

Sea n un número positivo y entero. Sabemos que 1 y n dividen n. Si $n > 1$ y ningún otro número además de 1 y n lo dividen, decimos que n es **primo**. Si $n > 1$ pero n no es primo, entonces decimos que n es **compuesto**. Nota: el número 1 no se considera ni primo, ni compuesto.

n es compuesto si y sólo si $n = ab$ para algún entero a, b con $1 < a < n$, y $1 < b < n$.

Normalmente, al hablar de un número primo o compuesto, nos referimos a un número entero positivo.

Teorema fundamental de la aritmética

Teorema

Todo entero n distinto de cero puede expresarse como:

$$n = \pm p_1^{e_1} \cdots p_r^{e_r}$$

donde $p_1, \ldots, p_r$ son primos distintos, y $e_1, \ldots, e_r$ son enteros positivos.

teorema fundamental de la aritmética (proof)

Proof

Por unicidad, la expresión que describe un número entero es única después de reordenar los primos:

- Asuma que $s > 1$ es el producto de números primos escrita de dos maneras diferentes:

$$\begin{aligned} s &= p_1 \cdot p_2 \cdots p_m \\ &= q_1 \cdot q_2 \cdots q_n. \end{aligned}$$

- Debemos demostrar que $m = n$ and that the q_j are a rearrangement of the p_i.

teorema fundamental de la aritmética (proof)

- Por el lema de Euclides (divisibilidad), p_1 debe dividir a uno de los q_j; reetiquetando los q_j de ser necesario, digamos que p_1 divide q_1. Dado que q_1 es primo, sus únicos divisores son el 1 y sí mismo, por lo que $p_1 = q_1$, entonces

$$\begin{aligned}\frac{s}{p_1} &= p_2 \cdots p_m \\ &= q_2 \cdots q_n.\end{aligned}$$

- Siguiendo el mismo razonamiento, p_2 debe de ser igual a alguno de los q_j restantes. Reetiquetamos otra vez de ser necesario, por ejemplo $p_2 = q_2$. Entonces,

$$\begin{aligned}\frac{s}{p_1 \cdot p_2} &= p_3 \cdots p_m \\ &= q_3 \cdots q_n.\end{aligned}$$

teorema fundamental de la aritmética (proof)

- Esto puede hacerse para todo m de p_i, demostrando que $m \leq n$. Si hubiera otra q_j tendríamos que

$$\frac{s}{p_1 \cdot p_2 \cdots p_m} = 1$$
$$= q_k \cdots q_n,$$

lo cual es imposible, dado que el producto de números mayores a 1 no puede ser igual a 1, por lo que $m = n$, y cada q_j es un p_i.

□

teorema fundamental de la aritmética (proof)

Proof.

En el pizarrón □

Conceptos

Teorema - Propiedad de la división con residuo

Sea $a, b \in \mathbb{Z}$ con $b > 0$. Existen $q, r \in \mathbb{Z}$ únicos tales que $a = bq + r$, con $0 \leq r \leq b$.

Número liso

Si un número entero positivo es divisible solamente por números primos "pequeños", se dice que es un número *liso* (smooth).

Los números lisos son muy utilizados en el criptoanálisis para verificar un sistema (romperlo). Por otro lado, los números que solamente se pueden factorizar por dos números primos muy grandes son esenciales para la criptografía de clave pública.

Divisor

Máximo común divisor

Dados dos números $a, b \in \mathbb{Z}$, distintos a cero, el Máximo común divisor (MCD), denotado como MCD(a, b), o en ocasiones símplemente como (a, b), es un número entero d que es el más grande que divide tanto a a como a b.

Mínimo común múltiplo

Dados dos números $a, b \in \mathbb{Z}$, distintos a cero, el mínimo común múltiplo (mcm), denotado como mcm(a, b) es el número entero positivo más pequeño al cual a y b dividen.

Algoritmo de Euclides

El algoritmo de Euclides es una manera rápida de encontrar el MCD(a, b) aún cuando se desconozcan los factores primos de a y b.

El algoritmo funciona así:

- Reordene para que $a > b$
- Divida a sobre b, y guarde el cociente q_1, y el residuo $r_1 : a = q_1 b + r_1$
- Reordene para que $a > b$: b es el nuevo a, y r_1 es el nuevo b
- Divida b sobre r_1 y guarde q_2 y $r_2 : b = q_2 r_1 + r_2$
- Reordene para que $a > b \ldots$
- Se detiene el algorimto cuando el último residuo divide al anterior: $r_n | r_{n-1}$

Ejemplo:

Encontrar el MCD(1547, 560):

$$\begin{aligned} 1547 &= 2 \cdot 560 + 427 \\ 560 &= 1 \cdot 427 + 133 \\ 427 &= 3 \cdot 133 + 28 \\ 133 &= 4 \cdot 28 + 21 \\ 28 &= 1 \cdot 21 + 7 \end{aligned}$$

Dado que $7|21$ hemos terminado: MCD$(1547, 560) = 7$.

Ejercicio

- Genere un programa en Maple para calcular el MCD.

Propiedades

- Por definición $\text{MCD}(0,0) = 0$
- $\text{MCD}(a,b) = \text{MCD}(b,a)$
- $\text{MCD}(a,b) = \text{MCD}(-a,b)$
- $\text{MCD}(-a,0) = |a|$
- $\text{MCD}(a,b) \cdot c = \text{MCD}(ac,bc)$, si $c \geq 0$
- $\text{mcm}(a,b) \cdot c = \text{mcm}(ac,bc)$, si $c \geq 0$
- $ab = \text{MCD}(a,b)\text{mcm}(a,b)$, si $a,b \geq 0$
- $\text{MCD}(\text{mcm}(a,b),\text{mcm}(a,c)) = \text{mcm}(a,\text{MCD}(b,c))$
- $\text{mcm}(\text{MCD}(a,b),\text{MCD}(a,c)) = \text{MCD}(a,\text{mcm}(b,c))$

Propiedades binarias

- Si a, b son pares, entonces:
  - $\text{MCD}(a, b) = 2 \cdot \text{MCD}(a/2, b/2)$
- Si a es par, y b es impar, entonces:
  - $\text{MCD}(a, b) = \text{MCM}(a/2, b)$
  - $\text{MCD}(a, b) = \text{MCM}(a - b, b)$
- Si a, b son impares, entonces:
  - $a - b$ es par
  - $|a - b| < \max(a, b)$

Ejercicio

- Genere un programa en Maple para calcular los números primos menores a 10000.

- Si contamos a 2 como el primer número primo, 3 el segundo, ¿cuál es el 100mo. primo?

Contenido de la sección 3

MCD revisitado

Hemos visto anteriorme cómo calcular el máximo común divisor de un número. Si $a, b \in \mathbb{Z}$, con $0 < b \leq a$, entonces:

- del algoritmo tradicional de la división sabemos que existen $q, r \in \mathbb{Z}$, con $r < b$, y $a = bq + r$.
- si $g \in \mathbb{Z}$, y $g|a$ y $g|b$, entonces:

$$g|(a - bq) \Rightarrow g|r$$

MCD revisitado

Ahora bien:

- Si MCD$(a, b) = g$, entonces implica que $g|r$, donde r es el residuo que resulta de dividir a por b
- Si $r = 0$, entonces $b|a$, y el máximo común divisor de a, b es b.
- Si $r \neq 0$, entonces MCD$(a, b) =$ MCD(b, r), la cual es una operación más económica. Repitiendo este proceso hasa que $r = 0$ nos da el algoritmo MCD.

Algoritmo MCD

Algoritmo simple de MCD:

Require: Integers $0 < b \leq a$
Ensure: MCD(a, b)
  $n = a$; $d = b$
  $r = n - (d \times \lfloor \frac{n}{d} \rfloor)$
  while $r \neq 0$ **do**
    $n = d$
    $d = r$
    $r = n - (d \times \lfloor \frac{n}{d} \rfloor)$
  end while
  return MCD$(a, b) = d$

MCD extendido

El algoritmo MCD extendido es idéntico al algoritmo estándar, pero además carga con información adicional. Si MCD$(a, b) = g$, entonces sabemos que existen $x, y \in \mathbb{Z}$ tal que:

$$ax + by = g$$

y es la mínima combinación lineal positiva para a y b.

MCD extendido

- Note que si el MCD es 1, entonces esta ecuación nos da los inversos para $a \bmod b$, y $b \bmod a$: $x \equiv a^{-1} \bmod b$, y $y \equiv b^{-1} \bmod a$.
- Si el MCD no es 1, entonces, y dado que es la combinación linear más pequeña, se dice que no existen inversos para $a \bmod b$ o $b \bmod a$.
- Extendiendo el algoritmo de MCD para calcular este dato extra, nos da un algoritmo eficiente para calcular los inversos multiplicativos.

Cómo extender el algoritmo MCD

Para extender el algoritmo MCD, la parte de la ecuación debe de agregarse a las iteraciones. Los valores iniciales de la ecuación son:

$$a(1) + b(0) = a$$
$$a(0) + b(1) = b$$

Algoritmo extendido de MCD

Require: Integers $0 < b \leq a$

Ensure: $x, y, \text{MCD}(a, b)$ tal que $ax + by = \text{MCD}(a, b)$

$v_0 = a$; $v_1 = b$

$x_0 = 1$; $y_0 = 0$

$x_1 = 0$; $y_1 = 1$

$i = 1$ {puntero al valor v más pequeño}

while $v_i \neq 0$ **do**

$i = i + 1 \bmod 2$

$q = \left\lfloor \frac{v_i}{v_{i+1 \bmod 2}} \right\rfloor$

$v_i = v_i - (q \times v_{i+1 \bmod 2})$

$x_i = x_i - (q \times x_{i+1 \bmod 2})$

$y_i = y_i - (q \times y_{i+1 \bmod 2})$

end while

$i = i + 1 \bmod 2$

return $x_i, y_i, \text{MCD}(a, b) = v_i$

Ejercicio

- Implemente el algoritmo extendido de Euclides (MCD)

- Calcule el inverso multiplicativo de $101 \bmod 1999$, y el inverso de $1999 \bmod 101$ utilizando el algoritmo.

Contenido de la sección 4

Congruencias

Propiedades básicas

Dados tres enteros a, b, y m, decimos que a es *congruente a* b *módulo* m, denotado: $a \equiv b \bmod m$, si la diferencia $a - b$ es divisible por m.

A m se le conoce como el *módulo* de la congruencia.

Propiedades

Propiedades de la congruencia:

1. ◦ $a \equiv a \bmod m$
   ◦ $a \equiv b \bmod m$ **sí y solo sí** $b \equiv a \bmod m$
   ◦ **Si** $a \equiv b \bmod m$**, y** $b \equiv c \bmod m$**, entonces** $a \equiv c \bmod m$

   Para una m fija, esto significa que la congruencia módulo m es una *relación de equivalencia*.

Propiedades. . .

2. ◦ Para una m fija, cada *clase de equivalencia* con respecto a un módulo m tiene 1 y sólo 1 representante entre 0 y $m-1$.
   ◦ El conjunto de clases de equivalencia (*clases residuales*) se denota como $\mathbb{Z}/m\mathbb{Z}$
   ◦ Cualquier conjunto de representantes para las clases residuales es llamado *conjunto completo de residuos módulo* m.

Propiedades. . .

3. **Si** $a \equiv b \bmod m$ **and** $c \equiv d \bmod m$**, then** $a \pm c \equiv b \pm d \bmod m$ **and** $ac \equiv bd \bmod m$**.**

En otras palabras, las congruencias (con el mismo módulo) se pueden sumar, restar, o multiplicar.

- El conjunto de clases de equivalencia $\mathbb{Z}/m\mathbb{Z}$ es un anillo conmutativo (lo veremos en la siguiente unidad). Esencialmente, las clases residuales se pueden sumar, restar, o multiplicar, y los axiomas básicos aplican (asociatividad, conmutabilidad, inversos aditivos, etc.)

Propiedades. . .

4. Si $a \equiv b \bmod m$, entonces $a \equiv b \bmod d$ para cualquier $d|m$
5. Si $a \equiv b \bmod m$, $a \equiv \bmod n$, y m y n son primos relativos, entonces $a \equiv b \bmod mn$

Pequeño teorema de Fermat

Teorema

Sea p un primo. Cualquier entero a satisface $a^p \equiv a \bmod p$, y cualquier entero a no divisible por p satisface $a^{p-1} \equiv 1 \bmod p$

Pequeño teorema de Fermat (proof)

- Suponga que $p \nmid a$.
- Tenemos que los enteros $0a, 1a, 2a, \ldots, (p-1)a$ son el conjunto de residuos módulo p.
- Observe que 2 elementos, ia y ja tendrían que estar en la misma clase residual $ia \equiv ja \bmod p$; sin embargo, esto significaría que $p|(i-j)a$, como a no es divisible por p, tendríamos que $p|(i-j)$, pero como $i, j < p$ se requiere que $i = j$ para que esto sucediera
- Concluímos que los enteros $a, 2a, \ldots, (p-1)$ son un reacomodo de $a, 2, \ldots, p-1$ cuando se considera el módulo $p \ldots$.

Pequeño teorema de Fermat (proof)

- Ahora tenemos que los números de la primera secuencia son congruentes módulo p a los números de la segunda secuencia: $a^{(p-1)}(p-1)! \equiv (p-1)! \bmod p$. Entonces, $p|((p-1)!(a^{p-1}-1))$
- Dado que $(p-1)!$ no es divisible por p, nos quedamos con $p|(a^{p-1}-1)$.
- Finalmente, si multiplicamos ambos lados de la congruencia $a^{p-1} \equiv 1 \bmod p$, tenemos la primer congruencia del teorema cuando a no es divisible por p
- Si a es divisible por p, entonces ambos lados se hacen $\equiv 0 \bmod p$.

□

Pequeño teorema de Fermat (proof)

Proof.

En el pizarrón □

Corolario sobre el pequeño teorema de Fermat

Corolario

Si a no es divisible por p y si $n \equiv m \bmod (p-1)$, entonces $a^n \equiv a^m \bmod p$.

Corolario sobre el pequeño teorema de Fermat (proof)

Proof

- Suponga que $n > m$
- dado que $p - 1 | n - m$, tenemos que $n = m + c(p - 1)$, para un entero positivo c.
- multiplicando la congruencia $a^{p-1} \equiv 1 \bmod p$ por sí misma c veces
- y después por $a^m \equiv a^m \bmod p$, obtenemos $a^n \equiv a^m \bmod p$.

Corolario sobre el pequeño teorema de Fermat (proof)

Proof.

En el pizarrón □

Chinese Remainder Theorem (CRT)

Definición

Sea R un anillo, I es un *ideal* de R si es un subconjunto no vacío de R tal que:

- I es un subgrupo de R con respecto a la ley de $+$
- para todo $x \in \mathbb{Z}$ y todo $y \in R$, $xy \in I$ y $yx \in I$.

- El ideal $I \subsetneq R$ es *primo* si para todo $x, y\ in R$ con $xy \in I$ se obtiene $x \in I$ o $y \in I$.
- El ideal $I \subsetneq R$ es *máximal* si para todo ideal J de R la inclusión $I \subset J$ implica que $J = I$ o $J = R$.
- Dos ideales I y J de R son *coprimos* si $I + J = \{i = j | i \in I y j \in J\}$ es igual a R.

Chinese Remainder Theorem (CRT)

Definición

Un ideal I de un anillo R está *finitamente generado* si existen elementos $a_1, \ldots, a_n$ tal que para cada $x \in I$ se pueda escribir $x = x_1 a_1 + \cdots + x_n a_n$ con $x_1, \ldots, x_n \in R$.

El ideal I es *principal* si $I = aR$ y R es un *dominio de ideals principales (PID)*, si es un dominio integral, y si cada ideal de R es principal. Ejemplos:

- El anillo de los enteros $\mathbb{Z}$
- El anillo de polinomios $\mathcal{K}[X]$, en donde $\mathcal{K}$ es un campo.

Chinese Remainder Theorem (CRT)

Teorema

Sean $I_1, \ldots, I_k$ ideales coprimos en parejas de R, entonces:

$$R/\prod_{i=1}^{k} I_i \simeq \prod_{i=1}^{k} R/I_i$$

Corolario

Sea $n_1, \ldots, n_k$ enteros coprimos, e.g. $(n_i, n_j) = 1$ para $i \neq j$.
Entonces, existe una solución simultánea a x:

$$\begin{cases} x & \equiv x_1 \bmod n_1 \\ x & \equiv x_2 \bmod n_2 \\ & \vdots \\ x & \equiv x_k \bmod n_k \end{cases}$$

congruentes entre si módulo $N = \prod_{i=1}^{k} n_i$

Chinese Remainder Theorem (CRT) - proof

- Unicidad módulo N: Suponga que x' y x'' son dos soluciones. Si $x = x' - x''$, entonces x debe de ser congruente a 0 módulo n_i, y por lo mismo, a módulo N.
- Definimos $N_i = N/n_i$ como el producto de los módulos *excepto el i-nésimo*. El $(n_i, n_j) = 1$, y existe un entero M_i tal que $N_i M_i = 1 \bmod n_i$
- Si tenemos que $x = \sum_i a_i N_i M_i$, para cada i los términos en la suma son divisibles por n_i, ya que $n_i | N_i$ para valores de $i \neq j$, así que para cada i tenemos que $x \equiv a_i N_i M_i \equiv a_i \bmod n_i$. $\square$

Chinese Remainder Theorem (CRT) - proof

Proof.

En el pizarrón □

Chinese Remainder Theorem (CRT)

Sabiendo que $x = \sum_i a_i N_i M_i$, ¿cómo se soluciona el siguiente sistema de ecuaciones?

$$\begin{cases} x & \equiv 1 \bmod 3 \\ x & \equiv 2 \bmod 5 \\ x & \equiv 4 \bmod 7 \\ x & \equiv 5 \bmod 11 \\ x & \equiv 9 \bmod 13 \end{cases}$$

Algoritmo CRT

Require: Enteros coprimos $n_1, \ldots, n_k$ y enteros x_1 para $1 \leq i \leq k$.

Ensure: Entero x tal que $x \equiv x_i \bmod n_i$, para todo $1 \leq i \leq k$

$N \leftarrow n_1$; $x = x_1$

for $i = 2$ **to** k **do**

Calcule u y v tal que $un_i + vN = 1$ [use el GCD extendido]

$x \leftarrow un_i x + vNx_i$

$N \leftarrow Nn_i$

$x \leftarrow x \bmod N$

end for

return x

Algoritmo CRT

i	n_i	x_i	N	u	v	x	$x \bmod n_i$
1	3	1	3	–	–	1	1
2	5	2	15	-1	2	7	2
3	7	4	105	-2	1	67	4
4	11	5	1155	-19	2	907	5
5	13	9	15015	-533	6	8992	9

Función Euler phi φ

Definición

La función φ de Euler, también llamada *totient*, es la función definida por la siguiente regla:

$$\varphi(m) = \#\mathbb{Z}/m\mathbb{Z} = \#\{0 \leq a < m : \mathsf{MCM}(a, m) = 1\}$$

Podemos calcular el valor con:

$$\varphi(n) = n \prod_{p|n} \left(1 - \frac{1}{p}\right)$$

Ejemplo

Calcular para 100:

- Factores: $2, 5$
- $\varphi(100) = 100 \times \left(1 - \frac{1}{2}\right) \times \left(1 - \frac{1}{5}\right) = 40$

- En el caso de números primos, $\varphi(p) = p - 1$.
- En el caso de potencias de primos, $\varphi(p^\alpha) = p^\alpha(1 - \frac{1}{p})$

Ejercicio

- Genere un programa en Maple para calcular la función φ de Euler.

Observaciones

Corolario

La función Euler phi-function is *multiplicativa*, esto es $\varphi(mn) = \varphi(m)\varphi(n)$, siempre y cuando $(m, n) = 1$.

Observaciones

Proof

- Se deberán de contar los enteros entre 0 y $mn-1$ que no tienen factor común con mn.
- Para todo elemento (j) en el rango, sea j_1 el residuo módulo m no-negativo más chico, y j_2 el de módulo n.
- Del Chinese Remainder Theorem tenemos que por cada j_1, j_2 hay solamente una $0 \leq j < mn-1$ que cumple con $j \equiv j_1 \bmod m$, $j \equiv j_2 \bmod n$.
- Note que j no tiene factor común con $m : (j_1, m) = 1$, ni con $n : (j_2, n) = 1$, por lo que las j's que vamos a contar tienen correspondencia $1-$to-1 con los pares j_1, j_2 correspondientes.
- El número posible de j_1's son $\varphi(m)$, y el número de j_2's es $\varphi(n)$, por lo que el número de parejas es $\varphi(m)\varphi(n)$.

Observaciones

Proof

En el pizarrón

Observaciones

Proposición

Si $(a, m) = 1$, entonces $a^{\varphi(m)} \equiv 1 \bmod m$

Observaciones - proof

Proof

m es una potencia prima ($m = p^\alpha$).

- Si $\alpha = 1$, es el teorema pequeño de Fermat
- Si $\alpha \geq 2$, y la fórmula aplica para la $(\alpha - 1)-$ava potencia de p, entonces $a^{p^{\alpha-1}-p^{\alpha-2}} = +p^{\alpha-1}b$, para un entero b.
- Elevando ambos lados de la ecuación a la p potencia (y tomando en cuenta que los coeficientes del binomio en $(1+x)^p$ son divisibles por p), tenemos que $a^{p^\alpha - p^{\alpha-1}}$ es igual a 1 más la suma de cada término divisible por P^α, esto es $a^{\varphi(p^\alpha)} - 1$ es divisible por p^α.
- Dada la multiplicabilidad de φ, $a^{\varphi(m)} \equiv 1 \bmod p^\alpha$, y ya que $p^\alpha | m$, y que estas potencias primas no tienen factores comunes, tenemos que $a^{\varphi(m) \equiv 1 \bmod m}$.

Observaciones - proof

Proof

En el pizarrón