Tarea

Sea A u conjunto no vacío con conjunto universal E. En 2^X se define la relación R como

$$XRY \Leftrightarrow X \cap A \subseteq Y \cap A$$

¿Qué propiedades verifica R? ¿Es relación de equivalencia? ¿Y si en la definición se cambia $\subseteq$ por $=$? En éste último caso calcular $[\varnothing]$ y $[E]$.

Tarea

1. *Considere el conjunto de enteros módulo 5 $\mathbb{Z}_5$ y la clase $[3]$. Encontrar una clase $[x]$ tal que $[3x] = [1]$.*
2. *¿Es posible repetir el ejercicio anterior con $\mathbb{Z}_6$?*

Tarea

Describir $[4] \in \mathbb{Z}_n$ *si*

1. $n = 2$
2. $n = 3$
3. $n = 6$
4. $n = 8$.

Tarea

Sea R *la relación de equivalencia en* $\mathbb{Z} \times \mathbb{Z}$ *definida por*

$$(a, b)R(c, d) \Leftrightarrow ad = bc.$$

Describir $[(1, 2)]$.

Tarea

¿Cuáles de estas colecciones de subconjuntos son particiones de $\{1, 2, 3, 4, 5, 6\}$*?*

1. $\{\{1, 2\}, \{2, 3, 4\}, \{4, 5, 6\}\}$
2. $\{\{1\}, \{2, 3, 6\}, \{4\}, \{5\}\}$
3. $\{\{2, 4, 6\}, \{1, 3, 5\}\}$
4. $\{\{1, 4, 5\}, \{2, 6\}\}$

Tarea

¿Cuáles de estas colecciones de subconjuntos son particiones del conjunto de cadenas de bits de longitud 8?

1. *El conjunto de cadenas de bits que empiezan por 1, el conjunto de cadenas de bits que empiezan por* 00 *y el conjunto de cadenas de bits que empiezan por 01.*
2. *El conjunto de cadenas de bits que contienen la cadena 00, el conjunto de cadenas de bits que contienen la cadena 10 y el conjunto de cadenas de bits que contienen a la cadena 11.*
3. *El conjunto de cadenas de bits que terminan en 00, el conjunto de cadenas de bits que que terminan en 01, el conjunto de cadenas de bits que terminan en 10 y el conjunto de cadenas de bits que terminan en 11.*
4. *El conjunto de cadenas de bits que terminan en 111, el conjunto de cadenas de bits que terminan en 011 y el conjunto de cadenas de bits que terminan en 00.*

Tarea

Enumerar los pares ordenados de las relaciones de equivalencia producidas por las siguientes particiones de $\{0, 1, 2, 3, 4, 5\}$*:*

1. $\{0\}, \{1, 2\}, \{3, 4, 5\}$
2. $\{0, 1\}, \{2, 3\}, \{4, 5\}$
3. $\{0, 1, 2\}, \{3, 4, 5\}$
4. $\{0\}, \{1\}, \{2\}, \{3\}, \{4\}, \{5\}$

Algunas aplicaciones de $\mathbb{Z}_n$: Protocolo Diffie-Hellman para intercambio de claves secretas

Sabemos que los enteros módulo n $\mathbb{Z}_n$ tienen una aritmética. Entonces, en particular se pueden calcular potencias de sus elementos: $[a]^0 = 1$ y si $n > 0$

$$[a]^n = \underbrace{[a] \dots [a]}_{n-\text{veces}}.$$

Por ejemplo, en $\mathbb{Z}_3$,

$$[2]^4 = [2]^2[2]^2 = [4][4] = [1][1] = [1].$$

Luego entonces se puede calcular logaritmos, pues los logaritmos no son mas que potencias:

$$\log_b(a) = x \Leftrightarrow b^x = a.$$

Por ejemplo, de nuevo en $\mathbb{Z}_3$: podemos poner $\log_{[2]}[1] = 4$ pues $[2]^4 = [1]$. Nótese que también $[2]^8 = [1]$ por lo que, para evitar conflictos ponemos

$$\log_{[b]}[a] = x \Leftrightarrow x = \min\{x \in \mathbb{N} \mid x > 0 \text{ y } [b]^x = [a]\}.$$

Esta clase de logaritmos, si se calcula en $\mathbb{Z}_n$, se llama *logaritmo discreto módulo n*.
Una de las ideas detrás del protocolo Diffie-Hellman es la creencia de que calcular logaritmos discretos es "difícil".

Necesitamos de la siguiente definición.

Definición

Sea n entero positivo. Una raíz primitiva módulo n es una clase $[\alpha]$ *en* $\mathbb{Z}_n$ *tal que*

$$\{[\alpha]^0, [\alpha]^1, \ldots, [\alpha]^{p-2}\} = \{[1], [2], \ldots, [p-1]\} = \mathbb{Z}_n \backslash \{[0]\}.$$

Ejemplo

La clase $[2]$ es raíz primitiva módulo 13 porque en $\mathbb{Z}_{13}$:

$$[2]^0 = [1], [2]^1 = [2], [2]^2 = [4], [2]^3 = [8], [2]^4 = [3], [2]^5 = [6], [2]^6 = [12]$$

$$[2]^7 = [11], [2]^8 = [9], [2]^9 = [5], [2]^{10} = [10], [2]^{11} = [7], [2]^{12} = [1], [2]^{13} =$$

Pero la clase $[3]$ no es raíz primitiva módulo 13 porque

$$\{[3]^0, \ldots, [3]^{p-1}\} = \{[1], [3], [9]\}.$$

Supóngase que se tienen dos partes A y B. Usualmente a éstas se les llama Alicia y Beto (Alice, Bob).

Problema: Entre A y B quieren intercambiar claves secretas por un canal inseguro.

El canal inseguro podría ser una línea telefónica o bien Internet.

Solución: El protocolo Diffie-Hellman que consiste de los siguientes pasos:

1. Entre A y B eligen un número primo p y $[\alpha]$ una raíz primitiva módulo p. Tal información la intercambian por el canal inseguro.
2. A elige un número entero x al azar tal que $1 < x < p - 1$. Tal número A lo mantiene en secreto.
3. B eleige un número entero y al azar tal que $1 < y < p - 1$. Tal número B lo mantiene en secreto.
4. A calcula $[\alpha]^x$ y hace reducciones módulo p (i.e., en $\mathbb{Z}_p$) para obtener a tal que

$$[\alpha]^x = [a]$$

con $1 \leq a \leq p - 1$. El número a que A obtiene se lo envia a B por el canal inseguro.

5. B calcula $[\alpha]^y$ y hace reducciones módulo p (i.e., en $\mathbb{Z}_p$) para obtener b tal que

$$[\alpha]^y = [b]$$

con $1 \leq b \leq p-1$. El número b que B obtiene se lo envia a A por el canal inseguro.
6. Con el número b que A recibió, la misma A calcula $[b]^x$ y hace reducciones en $\mathbb{Z}_p$ para calcular r_A entero tal que

$$[b]^x = [r_A]$$

y $1 \leq r_A \leq p-1$.
7. Con el número a que B recibió, el mismo B calcula $[a]^y$ y hace reducciones en $\mathbb{Z}_p$ para calcular r_B entero tal que

$$[a]^y = [r_B]$$

y $1 \leq r_B \leq p-1$.
8. Fin: la clave secreta intercambiada es r_A para Alicia y r_B para Beto, pues resulta que $r_A = r_B$.

Que al final del protocolo $r_A = r_B$ es gracias al siguiente teorema

Teorema

$$r_A = r_B$$

Dem. Tenemos, por definición que

$$\begin{aligned}[r_A] &= [b]^x \\ &= ([\alpha]^y)^x \\ &= [\alpha]^{yx}.\end{aligned}$$

Similarmente

$$\begin{aligned}[r_B] &= [a]^y \\ &= ([\alpha]^x)^y \\ &= [\alpha]^{xy}.\end{aligned}$$

Luego, como $xy = yx$, se sigue que $[r_A] = [r_B]$. Luego r_A y r_B están relacionados, esto es, $r_A \equiv r_B \pmod{p}$, lo que implica que $p|(r_A - r_B)$. Es decir $r_A - r_B$ es múltiplo de p, entonces también $|r_A - r_B|$ es múltiplo de p. Pero como $0 \leq |r_A - r_B| \leq p - 1$ entonces se sigue que $|r_A - r_B| = 0$, es decir $r_A = r_B$.

Ejemplo

Alicia y Beto desean intercambiar una clave secreta por e-mail.

1. Para esto eligen al primo 47 y raíz primitiva $[5]$ módulo 47. Intercambian esta información por e-mail, el cual es un canal inseguro. Así que una tercera parte E (Eva) conoce esta información.
2. Alicia elige un número x al azar con $1 < x < 47$, digamos $x = 30$ y lo mantiene en secreto.
3. Beto elige un número y al azar con $1 < y < 47$, digamos $y = 4$, y lo mantiene en secreto.
4. Alicia calcula $[5]^x = [5]^{30}$ en $\mathbb{Z}_{13}$: $[5]^{30} = [36]$. Alicia envia el número 36 a Beto por e-mail. Nótese que E se entera de este número.
5. Beto calcula $[5]^y = [5]^4$ en $\mathbb{Z}_{13}$: $[5]^4 = [14]$ y envia 14 por e-mail a Alicia. De nuevo E se entera de éste número.
6. Con el número 14 que Alicia recibió de Beto ella calcula $[14]^x = [14]^{30}$ en $\mathbb{Z}_{13}$: $[14]^{30} = [24]$.