Aritmetika Modularra, RSA Algoritmoa

Aurkibidea

Atalaren aurkibidea

Modulu finituko osoak I

Definizioa

Izan bedi, $n \in \mathbb{Z}$, $n > 1$. Esango dugu x eta y osoak **kongruenteak modulu n** direla, $x \equiv y \pmod{n}$ idatziz, baldin

$$n \mid x - y$$

Hau da, $\exists k \in \mathbb{Z}$ non $x - y = kn$ den.

Modulu finituko osoak I

Hurrengo espresioak baliokideak dira:

1. $x \equiv y(\mod n)$
2. $y \equiv x(\mod n)$
3. $x = y + kn$, k zenbaki oso bat izanez.
4. x eta y elementuek hondar berdina dutela n-z zatituta.

moduluko kongruentzia baliokidetasun erlazio bat da

- n moduluko kongruentzia baliokidetasun erlazio bat da. Partiketa bat sortzen du $\mathbb{Z}$ multzoan.
- Partiketaren klaseak hondarrak bezainbeste izango dira. Izan bedi $x \in \mathbb{Z}$, lehenik $[x]$ klasearen ordezkaria aukeratuko dugu, x zati n zatiketa euklidestarra kalkulatuz:

$$x = kn + r \ , 0 \leq r < n$$

Aurreko ekuaziotik ondorioztatzen da, $x \equiv r \pmod{n}$. Beraz, $[x]$ klasearen ordezkaritzat r aukeratuko dugu, r zatiketaren hondarra izanik .

$$[x] = [x]_n = \{r + kn \mid k \in \mathbb{Z}\} = [r]$$

$$[r] = \{\cdots, r - 2n, r - n, r, r + n, r + 2n, \cdots\}$$

n moduluko kongruentzia baliokidetasun erlazio bat da

- Baliokidetza klaseek multzo bat osatzen dute: $\mathbb{Z}_n = \{[0], [1], [2], \ldots, [n-1]\}$ **Zatidura multzoa**
- Adibidez, $n = 5$ izanik, klase berean egongo diren zenbakiak lerro berean daude:

$k < 0$			$[x]$	$k > 0$				
$\cdots$	-10	-5	0	5	10	15	20	$\cdots$
$\cdots$	-9	-4	1	6	11	16	21	$\cdots$
$\cdots$	-8	-3	2	7	12	17	22	$\cdots$
$\cdots$	-7	-2	3	8	13	18	23	$\cdots$
$\cdots$	-6	-1	4	9	14	19	24	$\cdots$

- $[x]$ **klasearen ordezkaria** r hondarra aukeratu dugu.
- Zatidura multzoa: $\mathbb{Z}_5 = \{[0], [1], [2], [3], [4]\}$

$+$ eta $\cdot$ eragiketak $\mathbb{Z}_n$ multzoan

$\mathbb{Z}_n$ multzoan definituko ditugu batuketa eta biderketa.

$$[x] + [y] = [x + y] \quad \text{eta} \quad [x] \cdot [y] = [x \cdot y]$$

edo berdina dena:

$$x(\bmod n) + y(\bmod n) = (x + y)(\bmod n)$$

eta

$$x(\bmod n) \cdot y(\bmod n) = (x \cdot y)(\bmod n)$$

$+$ eta $\cdot$ eragiketak $\mathbb{Z}_n$ multzoan

Hurrengo tauletan ikusten dira eragiketa hauek $\mathbb{Z}_5$ multzoan:

$+$	0	1	2	3	4
0	0	1	2	3	4
1	1	2	3	4	0
2	2	3	4	0	1
3	3	4	0	1	2
4	4	0	1	2	3

$\cdot$	0	1	2	3	4
0	0	0	0	0	0
1	0	1	2	3	4
2	0	2	4	1	3
3	0	3	1	4	2
4	0	4	3	2	1

$+$ eta $\cdot$ eragiketak $\mathbb{Z}_n$ multzoan

Hurrengo tauletan ikusten dira eragiketa hauek $\mathbb{Z}_4$ multzoan:

$+$	0	1	2	3
0	0	1	2	3
1	1	2	3	0
2	2	3	0	1
3	3	0	1	2

$\cdot$	0	1	2	3
0	0	0	0	0
1	0	1	2	3
2	0	2	0	2
3	0	3	2	1

$+$ eta $\cdot$ eragiketak $\mathbb{Z}_n$ multzoan

$\mathbb{Z}_4$ multzoko biderkatzeko taulan ikus daiteke:

- $2 = 2 \cdot 1 = 2 \cdot 3$ nahiz eta $1 \neq 3$. Hau da, multzo honetan badaude elementu erregularrak ez direnak edo sinplifikagarriak ez direnak.
- $0 = 2 \cdot 2$ nahiz eta $2 \neq 0$. Hau da, $\mathbb{Z}_4$ multzoan zeroren zatitzaileak daude.
- Eta nahiz eta $\mathbb{Z}_4$ multzoan elementu batzuk alderantzizko elementua ez izan, betetzen da $1 = 3 \cdot 3$

$+$ eta $\cdot$ eragiketak $\mathbb{Z}_n$ multzoan

- Kalkuluak errazteko garrantzitsua da jakitea $\mathbb{Z}_n$ multzoko elementuren batek alderantzizko elementua izango duen.
- Hori jakiteko hurrengo teorema erabiliko dugu:

Teorema

$r \in \mathbb{Z}_n$ multzoko elementuren batek alderantzizko elementua izango du baldin eta soilik baldin r eta n zenbaki lehen erlatiboak badira. ($z.k.h.(r, n) = 1 = rx + ny$). Edo baliokidea dena:

$$rx \equiv 1(\ \mathrm{mod}\ n)$$

- **r unitatea** :

Definizioa

$r \in \mathbb{Z}_n$ izanik, esango dugu r **unitatea** dela $\mathbb{Z}_n$ multzoan existitzen bada $s \in \mathbb{Z}_n$ elementu bat non $r \cdot s = s \cdot r = 1$ betetzen den.

- Ez da beharrezkoa $r \neq s$ izatea.

$+$ eta $\cdot$ eragiketak $\mathbb{Z}_n$ multzoan

$\mathbb{Z}_n$ multzoko unitateek osatzen duten multzoa $\mathbb{Z}_n^*$ deitzen da. Adibidez:

$$\mathbb{Z}_2^* = \{1\}$$

$$\mathbb{Z}_3^* = \{1, 2\}$$

$$\mathbb{Z}_4^* = \{1, 3\}$$

$$\mathbb{Z}_5^* = \{1, 2, 3, 4\}$$

$$\mathbb{Z}_6^* = \{1, 5\}$$

$+$ eta $\cdot$ eragiketak $\mathbb{Z}_n$ multzoan

Kalkula ezazue 17 zenbakiaren alderantzizkoa $\mathbb{Z}_{64}$ multzoan.

1. $z.k.h.(17, 64) = 1$ frogatu.
2. Bi zenbakien konbinazio lineal moduan jarri.
   $z.k.h.(17, 64) = 1 = (-15) \cdot 17 + 4 \cdot 64$
3. Aurreko teorema erabiliz, $(-15) \cdot 17 \equiv 1(\text{ mod } 64)$
4. Aztertu $\mathbb{Z}_{64}^*$ multzoan, zein klaseri dagokio -15?

$$-15 \equiv 49(\text{ mod } 64)$$

Euler-en Fi Funtzioa $\phi(n)$

- $\phi(n)$ funtzioa $\mathbb{Z}_n$ multzoaren unitate kopurua da:$\phi(n) = \|\mathbb{Z}_n^*\|$. Hau da, n baino txikiago izatea eta n-rekiko zenbaki lehen erlatibo izatea betetzen dituzten zenbaki positibo guztien kopurua. $\forall a \in \mathbb{Z}^+$
  - $1 \leq a \leq n$
  - $z.k.h.(a, n) = 1$
- Adibidez, $\mathbb{Z}_{15}$ multzoaren unitate kopurua: $\phi(15) = 8$.
- Nola aukeratuko dugu n zenbakia $\mathbb{Z}_n$ multzoan elementu ez-nulu guztiek alderantzizkoa izan dezaten? edo $\phi(n) = n - 1$ bete dezan?.

Euler-en Teorema

Teorema (Euler-en Teorema)

$a, n \in \mathbb{Z}^+$ bi zenbaki lehen erlatiboak izanik, $n \geq 2$:

$$a^{\phi(n)} \equiv 1 (\mod n)$$

Teorema (Fermat-en Teorema Txikia)

n zenbaki lehen bat bada , $n = p$, *Euler-en Teorema Fermat-en Teorema Txikia* bihurtzen da:

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

Euler-en Teorema

Korolarioa

p zenbaki lehena bada, $a \in \mathbb{Z}$ edozein zenbakitarako hau beteko da:

$$a^p \equiv a(\text{ mod } p)$$

Berreketak $\mathbb{Z}_n$ multzoan

Korolarioa

$z.k.h.(a, n) = 1$ betetzen bada,

$$x \equiv y(\bmod \phi(n)) \Rightarrow a^x \equiv a^y (\bmod n)$$

Eta berreketak kalkula daitezke hurrengo formularekin:

$$a^x \equiv a^{x(\bmod \phi(n))} (\bmod n)$$

Adibidez, kalkula ezazue $3^{9734888} (\bmod 100)$. Betetzen da $z.k.h.(3, 100) = 1$ eta

$$3^{9734888} (\bmod 100) = 3^{9734888(\bmod \phi(100))} (\bmod 100) =$$

$$= 3^{9734888(\bmod 40)} (\bmod 100) = 3^8 (\bmod 100) = 6561 (\bmod 100) =$$

$$= 61$$

Euler-en Teorema. Adibidea I

Aurreko teoremak eta korolarioa nola erabili erakusteko, kalkulatuko dugu r hondar positibo txikiena hurrengo ekuazioan, $r = 2^{68}(\text{ mod } 19)$.

- $p = 19$ zenbaki lehena da eta Fermat-en teoremaren arabera: $2^{19-1} \equiv 1 \text{ mod } 19$.
- Berretzailea honela deskonposa daiteke: $68 = 18 \cdot 3 + 14$
- Eta
  $2^{68}(\text{ mod } 19) = (2^{18})^3 \cdot (2^{14})(\text{ mod } 19) = (1^3 \cdot 2^{14})(\text{ mod } 19)$
- Oraindik $2^{14}(\text{ mod } 19)$ kalkulatzea geratzen zaigu.
- $2^4(\text{ mod } 19) = 16(\text{ mod } 19) = -3$. Kontutan izan $[-3] = [16]$ klase bera direla eta horrela kalkuluak errezagoak izango dira.

Euler-en Teorema. Adibidea II

- Aurrekoan kalkulatutakoaren arabera, $14 = 4 \cdot 3 + 2$ eta kalkulua horrela geratuko da

$$2^{14}(\text{ mod } 19) = (2^4)^3 \cdot 2^2(\text{ mod } 19) =$$

$$= (-3)^3 \cdot 2^2(\text{ mod } 19) = (-27) \cdot 4(\text{ mod } 19)$$

- $(-27)(\text{ mod } 19) = 11$ baina $[-8] = [11]$ klase berdinak dira eta horrela kalkuluak errezagoak izango dira.
- Beraz, bakarrik geratzen da $(-8)(4)(\text{ mod } 19) = (-32)(\text{ mod } 19) = 6 = r$, hondar positibo txikiena.

Atalaren aurkibidea

Diffie-Hellman Algoritmoa I

1. Gorkak eta Ainhoak funtzio bat erabiltzea adostuko dute: $f(x) = a^x (\bmod p)$ (p zenbaki lehen bat izanik).
2. Gorkak N_{G1} zenbaki bat aukeratuko du eta zenbakia ezkutuan gordeko du. Ainhoak N_{A1} beste zenbaki bat aukeratuko du eta zenbakia ezkutuan ere mantenduko du.
3. Zenbaki bana kodetuko dute aldez aurretik adostutako funtzioa erabiliz: $f(x) = a^x (\bmod p)$

$$N_{G2} = f(N_{G1}) = a^{N_{G1}} (\bmod p)$$

$$N_{A2} = f(N_{A1}) = a^{N_{A1}} (\bmod p)$$

4. Gorkak N_{G2} zenbakia bidaliko dio Ainhoari, eta Ainhoak N_{A2} zenbakia Gorkari.

Diffie-Hellman Algoritmoa II

5. Gorkak $C_G = {N_{A2}}^{N_{G1}} (\text{ mod } p)$ zenbakia kalkulatuko du, eta Ainhoak $C_A = {N_{G2}}^{N_{A1}} (\text{ mod } p)$. Bi zenbakiak berdinak izango dira: $C_G = C_A$
6. Eta zenbaki hori mezu bat kodetzeko gakoa izango da.

Diffie-Hellman Algoritmoa. Adibidea. I

1. Gorkak eta Ainhoak funtzio bat adostuko dute: $f(x) = 7^x (\text{ mod } 11)$
2. Gorkak zenbaki bat aukeratuko du eta zenbakia ezkutuan gordeko du: $N_{G1} = 3$. Ainhoak beste zenbaki bat aukeratuko du eta ezkutuan gordeko du: $N_{A1} = 6$.
3. Biek erabiliko dute aldez aurretik adostutako funtzioa zenbaki berriak kalkulatzeko.

$$N_{G2} = f(3) = 7^3 (\text{ mod } 11) = 2$$

$$N_{A2} = f(6) = 7^6 (\text{ mod } 11) = 4$$

4. Gorkak 2 zenbakia bidaliko dio Ainhoari, eta Ainhoak 4 zenbakia Gorkari.

Diffie-Hellman Algoritmoa. Adibidea. II

5. Gorkak $C_G = 4^3 (\text{ mod } 11) = 9$ zenbakia kalkulatuko du. Eta Ainhoak $C_A = 2^6 (\text{ mod } 11) = 9$. Bi zenbakiak berdinak dira: $C_G = C_A = 9$.
6. Eta zenbaki hori mezu bat kodetzeko gakoa izango da.

Atalaren aurkibidea

RSA Algoritmoaren oinarriak

- RSA algoritmoa kodetzeko eskema bat da. Ronald Rivest, Adi Shamir eta Leonard Adleman-ek 1977. urtean diseinatuta.
- Algoritmoak mezu bat kodetzen du gako batekin (**kodetzeko gakoa**) eta beste gako batekin (**deskodetzeko gakoa**) deskodetzen du.
- Kodetzeko gakoa publikoa da (edonori eman dakioke) eta deskodetzeko gakoa pribatua da (mezu jasotzaileak bakarrik ezagutuko du)

RSA Algoritmoaren oinarriak

RSA algoritmoa hurrengo teorian oinarritzen da:

- p eta q bi zenbaki lehen emanik, eta m beste zenbaki positibo bat p eta q-rekiko zenbaki lehen erlatiboa izanik. Euler-en Teoremaren arabera:

$$m^{\phi(pq)} = m^{(p-1)(q-1)} = 1(\bmod pq)$$

- Orain pentsatuko dugu e eta d bi zenbaki lehen ditugula eta $e \cdot d = 1(\bmod \phi(pq))$ betetzen dutela. Orduan:

$$(m^e)^d = m^{(e \cdot d)} = m(\bmod pq)$$

- Beraz, m^e emanda, posiblea da $m(\bmod pq)$ aurkitzea $(m^e)^d$ berreketa eginez.

RSA Algoritmoa

1. Aurkitu p eta q bi zenbaki lehen handiak. Kalkulatu bere biderkadura: $n = pq$.
2. Aurkitu e eta d zenbakiak ($2 \leq e, d \leq \phi(pq)$), non $e \cdot d = 1(\mod \phi(pq))$, baita.
3. *Kodetzeko gako publikoa* (n, e) bikotea izango da. *Deskodetzeko gako pribatua* (n, d) bikotea izango da.
4. Mezua zati txikietan banatuta izango da eta zati bakoitza kodetuko da $m \leq n$ zenbaki oso positiboa bezala
5. $m' = m^e (\mod n)$ kalkulatuko da zati bakoitzerako.
6. Mezu jasotzaileak mezua deskodetuko du $m'' = m'^d (\mod n)$ kalkulatuz, non $0 \leq m'' < n$ den.

RSA Algoritmoa. Adibidea.

Eman dezagun Ionek Mireni mezu bat bidali nahi diola. Horretarako Mirenen gako publikoa bilatuko du, (n=85,e=3) adibidez. Eta 'KAIXO' mezua honela kodetuko du 'KAIXO'= $11, 1, 9, 24, 15$

$$m^e(\quad (\text{mód } n) = m')$$

$$11^3(\ \text{mod } 85) = 56$$

$$1^3(\ \text{mod } 85) = 1$$

$$9^3(\ \text{mod } 85) = 49$$

$$24^3(\ \text{mod } 85) = 54$$

$$15^3(\ \text{mod } 85) = 60$$

RSA Algoritmoa. Adibidea.

Mirenek m' mezua jasotzean deskodetuko du bere gako pribatuarekin, (n=85,d=11).

$$m'^{d}(\text{ mod } n) = m''$$

$$56^{11}(\text{ mod } 85) = 11$$

$$1^{11}(\text{ mod } 85) = 1$$

$$49^{11}(\text{ mod } 85) = 9$$

$$54^{11}(\text{ mod } 85) = 24$$

$$60^{11}(\text{ mod } 85) = 15$$

$11, 1, 9, 24, 15$ mezua deskodetuta 'KAIXO' da.

RSA Algoritmoa. Adibidea.

Aldez aurretik Mirenek $p = 5$ eta $q = 17$ zenbaki lehenak aukeratu ditu. Eta $d = 11$ zenbakia honela aukeratu du: $z.k.h.(m.k.t.(4, 16), d) = 1$.