

Aritmetika Modularra

Irakasgaia: Matematika Diskretua
Informatika fakultatea
Donostia

1

n moduluko kongruentzia

Definizioa (n moduluko kongruentzia)

$n \in \mathbb{Z}$, $n > 1$ izanik, $a, b \in \mathbb{Z}$ kongruenteak modulu n dira, $a \equiv b \pmod{n}$, baldin $n \mid a - b$ hau da, $\exists k \in \mathbb{Z} \ / \ a = b + kn$; $a - b$ zenbakia n ren multiploa da; a eta b zenbakiek hondar bera uzten dute n zenbakiaz zatitzean.

Teorema (Zatiketa Euklidentarra)

$a, b \in \mathbb{Z}$ emanik, $b > 0$, $\exists \mid q \in \mathbb{Z} \ \exists \mid r \in \mathbb{Z}$ non $a = qb + r$ den. r hondarra da, $0 \leq r < b$ izanik. Hondar posibleak: $0, 1, \dots, b - 1$.

$$\begin{array}{l} a \\ r \end{array} \mid \begin{array}{l} b \\ q \end{array} \quad a = r + qb, \quad 0 \leq r < b.$$

n moduluko kongruentzian, hondar posibleak: $0, 1, \dots, n - 1$.

$$\begin{array}{l} a \\ r \end{array} \mid \begin{array}{l} n \\ q \end{array} \quad a = r + qn, \quad 0 \leq r < n \quad \rightarrow \quad \boxed{a \equiv r \pmod{n}}$$

$$\boxed{n \text{ moduluko hondarren multzoa: } \mathbb{Z}_n = \{0, 1, \dots, n - 1\}}$$

2

Batuketa eta Biderketa modularrak

Batuketa eta biderketa

\mathbb{Z}_n multzoan batuketa eta biderketa modularra horrela egiten dira:

$$\boxed{((a \pmod{n}) + (b \pmod{n})) \pmod{n} = (a + b) \pmod{n}}$$

$$\boxed{((a \pmod{n}) \cdot (b \pmod{n})) \pmod{n} = (a \cdot b) \pmod{n}}$$

Zatiketa

Zatiketa ez dago elementu guztietarako definituta, eta badagoenean alderantzizko modularraz biderkatuz kalkulatu ohi da.

3

Alderantzizko modularra

- \mathbb{Z} multzoko elementu guztiek ez dute alderantzizkorik, ezta \mathbb{Z}_n multzoko guztiek alderantzizko modularrik ere.
- a elementua alderantzizkagarria izateko $a \cdot a^{-1} = 1$ beteko duen a^{-1} existitu behar da multzoan.

Teorema (Alderantzizko modularren existentzia)

$a^{-1} \pmod{n}$ existitzen da baldin eta soilik baldin $\text{zkh}(a, n) = 1$. \mathbb{Z}_n multzoan alderantzizkagarri diren elementuen multzoa \mathbb{Z}_n^* da. n moduluko hondarren multzo murriztua:

$$\boxed{\mathbb{Z}_n^* = \{a \in \mathbb{Z}_n : \text{zkh}(a, n) = 1\}}$$

Alderantzizko modularra existitzen denean, $a^{-1} \pmod{n}$ kalkulatzeko Euklidesen algoritmoa erabiliko dugu.

4

Alderantzizko modularren kalkulua

Euklidesen algoritmoa erabiliz

Izan bitez $a, n \in \mathbb{Z}$ lehen erlatiboak, $\text{zkh}(a, n) = 1$.

Dakigunez, $\exists x, y \in \mathbb{Z}$ non $xa + yn = \text{zkh}(a, n)$.

Hortaz,

$$\text{zkh}(a, n) = 1 \Leftrightarrow \exists x, y \in \mathbb{Z} \text{ non } ax + ny = 1.$$

a -ren alderantzizko modularra x dela ondoriozta daiteke horrela:

$$ax + ny = 1 \Rightarrow ax = 1 + (-y)n \Rightarrow ax \equiv 1 \pmod{n}$$

$$\Rightarrow \boxed{a^{-1} \equiv x \pmod{n}}.$$

Euklidesen algoritmoa erabiliz x kalkulatu dugu, hau da, a^{-1} .

5

Euler-Fermat teorema

Definizioa (Euler-en funtzioa, $\phi(n)$)

Eulerren funtzioa, $\phi(n)$, n moduluko hondarren multzo murriztuak duen elementu kopurua da, hau da, \mathbb{Z}_n^* multzoaren kardinala.

Teorema ($\phi(n)$ ren kalkulurako)

Izan bitez $p, q, n \in \mathbb{Z}$.

- n zenbakia lehena bada, orduan $\phi(n) = n - 1$.
- $n = pq$ bada, p eta q bi zenbaki lehen desberdinak izanik, orduan $\phi(n) = (p - 1)(q - 1)$.
- $n = p_1^{e_1} \cdots p_r^{e_r}$ moduan idatz daiteke, p_1, \dots, p_r lehen desberdinak izanik. $\phi(n) = \frac{n}{p_1 \cdots p_r} (p_1 - 1) \cdots (p_r - 1)$.

Teorema (Euler-en teorema)

Izan bitez $a, n \in \mathbb{Z}^+$ zenbaki lehen erlatiboak, $\text{zkh}(a, n) = 1$. Zera

betetzen da: $\boxed{a^{\phi(n)} \equiv 1 \pmod{n}}$

6

Euler-Fermat teorema

n zenbaki lehena izanik $\phi(n) = n - 1$ denez, Euler-en teorema honela geratzen da.

Teorema (Fermat-en teorema txikia)

Izan bedi $n \in \mathbb{Z}^+$ lehena. $a \in \mathbb{Z}^+$ izanik, $\boxed{a^{n-1} \equiv 1 \pmod{n}}$

Oharrak:

1. Euler-Fermat teorema erabiliz, berreketa modularra kalkulatzeko posible bada ere, gehienetan ez da praktikoa.
 - $\phi(n)$ kalkulatzeko ez da beti erraza gertatzen, n oso handia denean zenbaki lehenetan faktorizatzea ez da erraza...
 - Teoremei esker zenbait kasutan berreketa modularren kalkulua asko laburtzea lortzen da, baina ez beti...
2. **Kriptografian**, gako publikoko zifratze-algoritmoetan, oso garrantzitsuak gertatzen dira Euler-Fermat teorema

7

Berreketa modularra

$a, x \in \mathbb{Z}$, $x \geq 0$ izanik, a^x berreketa biderketen bidez kalkulatzeko, x berretzailea handia denean bi arazo mota sortzen dira:

- a^x handiegia da. Kalkulatu nahi izateak arazoak sor ditzake!
- a zenbakia bere buruarekin $x - 1$ aldiz biderkatu behar da. Biderketa kopuru handia!

Aritmetika modularrean, $a^x \pmod{n}$ kalkulatzeko:

- Zenbaki handiegien arazoa ekiditen da, ez dago a^x kalkulatu beharrik, horrela eragiten delako.

$$((a \pmod{n}) \cdot (b \pmod{n})) \pmod{n} = (a \cdot b) \pmod{n}$$

- Berreketa bitarraren metodoa. x berretzailearen adierazpen bitarra erabiliz biderketa kopuru minimoa kalkulatu da.

8

Berreketa modularra

Berreketa bitarraren metodoa

- Berreketa handiak modu eraginkorrean kalkulatzeko metodoa.
- x ren adierazpen bitarra erabiltzen da.
- a^x berreketa kalkulatzeko algoritmo errekursiboa:

$$a^x = \begin{cases} a & x = 1 \text{ bada} \\ (a^{\frac{x}{2}})^2 & x \text{ bikoitia bada} \\ aa^{x-1} & x \text{ bakoitia bada} \end{cases}$$

Berreketa honako hiru propietateetan oinarritzen da:

$$a^1 = a, \quad a^{x+y} = a^x a^y, \quad a^{xy} = (a^x)^y$$

Bibliografia

- **Aritmetika modular**
https://eu.wikipedia.org/wiki/Aritmetika_modular
- **Biderketarekiko alderantzizko modularra**
https://eu.wikipedia.org/wiki/Biderketarekiko_alderantzizko_modularra
- **Teorema de Euler, Pequeño teorema de Fermat**
http://es.wikipedia.org/wiki/Teorema_de_Euler
http://es.wikipedia.org/wiki/Pequeño_teorema_de_Fermat
- **RSA algoritmoa. RSA-ren froga**
<https://eu.wikipedia.org/wiki/RSA>
- **Anexo: Números primos**
10000 baino txikiagoak diren zenbaki lehenak.
http://es.wikipedia.org/wiki/Anexo:Números_primos
- **Exponenciación binaria**
http://es.wikipedia.org/wiki/Exponenciación_binaria