Aritmetika Modularra

Irakasgaia: Matematika Diskretua
Titulazioa: Informatikaren Ingeniaritzako Gradua
Informatika fakultatea
Donostia

n moduluko kongruentzia

Definizioa (n moduluko kongruentzia)

$n \in \mathbb{Z}$, $n > 1$ izanik, $a, b \in \mathbb{Z}$ kongruenteak modulu n dira, $a \equiv b \bmod n$, 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 Euklidestarra)

$a, b \in \mathbb{Z}$ 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: $0, 1, \ldots, b - 1$.

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

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

$$\begin{array}{r|l} a & n \\ r & q \end{array} \qquad a = r + qn, \quad 0 \leq r < n \quad \rightarrow \quad \boxed{a \equiv r \bmod n}$$

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

Batuketa eta Biderketa modularrak

Batuketa eta biderketa

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

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

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

Zatiketa

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

Alderantzizko modularra

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

Teorema (Alderantzizko modularraren existentzia)

$a^{-1} \bmod n$ existitzen da baldin eta soilik baldin $\text{zkh}(a, n) = 1$.

$\mathbb{Z}_n$ multzoan alderantzikagarri 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, $a^{-1} \bmod n$ kalkulatzeko Euklidesen algoritmoa erabiliko dugu.

Alderantzizko modularraren 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:

$$ax + ny = 1 \Rightarrow ax = 1 + (-y)n \Rightarrow ax \equiv 1 \bmod n$$

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

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

Euler-Fermat teoremak

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, $p_1, \ldots, p_r$ lehen desberdinak izanik. $\phi(n) = \frac{n}{p_1 \ldots p_r}(p_1 - 1) \ldots (p_r - 1)$.

Teorema (Euler-en teorema)

Izan bitez $a, n \in \mathbb{Z}^+$ zenbaki lehen erlatiboak, $\text{zkh}(a, n) = 1$. Zera betetzen da: $\boxed{a^{\phi(n)} \equiv 1 \bmod n}$

Euler-Fermat teoremak

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, $\boxed{a^{n-1} \equiv 1 \bmod n}$

Oharrak:

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

Berreketa modularra

$a, x \in \mathbb{Z}$, $x \geq 0$ izanik, a^x berreketa biderketen bidez kalkulatzean, 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, $a^x \bmod n$ kalkulatzean:

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

$$((a \bmod n) \cdot (b \bmod n)) \bmod n = (a \cdot b) \bmod n$$

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

Berreketa modularra

Berreketa bitarraren metodoa

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

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

Berreketaren honako hiru propietateetan oinarritzen da:

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

Bibliografia

- Aritmética modular
  http://es.wikipedia.org/wiki/Aritmética_modular
- Modular Multiplicative Inverse edo alderantzizko modularra
  http://en.wikipedia.org/wiki/Modular_multiplicative_inverse
- 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 algorithm. Proofs of correctness
  http://en.wikipedia.org/wiki/RSA_(algorithm)
- 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