udako euskal unibertsitatea

DIBISIBILITATEAREN TEORIA ETA KONGRUENTZIAK

IRUINEA 1979

udako euskal unibertsitatea

I

UDAKO EUSKAL UNIBERTSITATEA

IRUÑEA 1979

DIBISIBILITATEAREN TEORIA ETA KONGRUENTZIAK

EGILEAK:

Mª JESUS ALKAIN

Mª LUISA BERRIOTXOA

FERNANDO GARATEA

Mª KARMEN CASTILLO

EDURNE BIRITXINAGA

ARANTZA LABORDA

AURKIBIDEA

SARRERA

Bi hitz bakarrik gure lan hau aurkezteko.

Beste arlo batzutan bezala, Matematikan ere hainbat parte landu eta egin gabe daudela uste dugu. Hutsune horik, pixkanaka pixkanaka, denon artean bete behar ditugula pentsatzen dugunez, oraingo lan hau egiterakoan gure asmoa zenbakien teoria apur bat lantzea izan da.

Bereziki atal bi hauk aztertu ditugu: dibisibilitatea eta kongruentziak, zeren lehena bigarrenaren osagarri eta oinarri dela uste baitugu.

Bestalde, zenbakien teorian agertzen diren zenbait funtzio ohargarri aipatu nahi izan dugulako, hauetariko batzu aztertzeko gai bat eman dugu.

Kongruentziei dagokienez, inkognita bateko kongruentziak bakarrik aztertu ditugu, eta hauen artean lehen eta bigarren gradukoak. Kongruentzia moeta hauen soluzioak aurkitzeko, hasiera batetan bide orokorrak ematen dira, azkenean indizeen teoria baten bidez nola aska daitezkeen aipatzeko.

LEHEN GAIA

DIBISIBILITATEAREN TEORIA

OROKORRA

- Sarrera.
- Dibisibilitatea eraztun trukakor unitatedunetan.
- Eraztun faktorialak.
- Eraztun euklideatrak.
- Aplikazio edo bi klase partikularrak.
- Z multzoa.
- R x multzoa.

S A R R E R A

Lan honetan egin dena izan da Dibisibilitatearen teoria aurkeztu, era general batean, aplikaziorik eta kasu zehatzik ai payu gabe. Gero bukaeran zerbait esan dugu bi kasu garrantzitsuei buruz Z eta R [x] multzoei buruz. Agian beste batean aztertuko titugu sakonean kasu hauek. Hori da behintzat gure asmoa.

Lan honen eskema egin nahi izango bagenu, esan beharko genuke hasi garela Dibisibilatearen teoria honekin zer ikusirik duten zenbait definizio (oinarrizko definizioak) ematen, eta sortzen diren zenbait propietate aztertzen, esate baterako, elementu laburtezinei buruz edota elementu elkartuei buruz, e.a.

Bigarren pauso batean, eraztun Faktorialak definitu eta aztertzen ditugu. Eta honen ondorio bezala definitzen dira m.k.t. eta z.k.h.

Hirugarren zati bezala eraztun Euklidearrak ditugu. Definizioa propietateak eta faktorialekiko erlazioa.

Azterketa general hau amaitzen da eraztun printzipalak, faktorialak eta euklidearrak duten erlazioak aztertzen.

DIBISIBILITATEA ERAZTUN TRUKAKOR UNITATEDUNETAN

Biz A eraztun trukakor bat eta biz e bere elementu unitatea. Eman ditzagun a, b $\in$ A.

Definizioa: "b elementuak a zatitzen duela" diogu, edo "b a-ren zatitzaile bat dela", edo "a b-ren multiplo bat", baldin existitzen bada A-n q bat, q $\in$ A, non a=bq baita.
Kasu horretan b/a idatziko dugu edo a $\equiv$ 0 (b mod.), eta zera esango dugu: q dela "a elementua b elementuz zatitutako zatidura".

Beraz:

b/a (edo a$\equiv$0 (b mod.)) $\Leftrightarrow$ $\exists$ q$\in$A non a = bq baita.

Definizioa(bis): Baldin (a) a$\in$A elementuak sortutako ideala bada, "b elementuak a zatitzen duela" diogu ===== (a)$\subset$(b).

Bi definizio hauek baliokideak dira.

Frogapena:Baldin b a-ren zatitzaile bat bada lehenago definizioaren eran, $\exists$ q$\in$A non a=bq baita. Beraz $\forall$ y$\in$(a)-rentzat zera dugu: y= ar = bqr$\in$(b). Beraz,
(a)$\subset$(b).
Alderantziz, baldin b elementua a-ren zatitzaile bat bada bigarren definizioaren eran, (a)$\subset$(b). Beraz,
$\exists$ q$\in$A non a= bq baita. f.n.l.

1.Teorema: Dibisibilitate erlazioa,/halegia, erreflexio eta iragate propietateak betetzen ditu.

Frogapena: A) Erreflexioa: $\forall$ a A-rentzat a=ae. Beraz a/a.
B) Iragatea: baldin a/b eta b/c
$\exists$ p,q$\in$A non b=ap eta c=bq baitira.Beraz
c = a(pq) non pq$\in$A. Beraz
a/c.

2.Teorema: Bi dibisibilitate-erlazio biderka daitezke atalez atal, baina terminuen ordena aldatu gabe.

Frogapena: Izan ere,eman ditzagun a_1/b_1 eta a_2/b_2.
$\Leftrightarrow$ $a_1q_1 = b_1$ eta $a_2q_2 = b_2$. beraz
$a_1a_2q_1q_2 = b_1b_2 \Rightarrow a_1a_2\ b_1b_2$ f.n.l.

3. Teorema: Elementu baten zenbait multiploen edozein konbinazio lineala, elementu honen multiplo bat da, ere.

Frogapena: Eman ditzagun a/b_1 eta a/b_2

$\Longrightarrow a/(k_1b_1 + k_2b_2)$ non

$k_1, k_2 \in A$ baitira f.n.l.

A-ren unitateak

Definizioa: $u \in A$ elementua A eraztunaren "Unitate bat" dela diogu $\Longleftrightarrow u/e.$ *

Ondorioak: 1)Unitaten baten edozein zatitzailea, bera ere unitate bat da.

2) $\forall a \in A$, a edozein u unitateren multiploa da eta $q = u^{-1}a$ zatidura unibokikoki determinatua dago.

1.-Teorema: A-ren unitateak talde biderkakor bat osatzen dute. "Unitateen taldea" esango diogu eta U bidez adieraziko dugu.

Frogapena: a) U egonkorra da biderkaketarekiko, eta A-ren biderkaketak induzitutako legea U-n elakrkorra da.

b) U-k badu e elementua, $e \in U$. Eta baldin $u \in U$ bada, $\Longrightarrow u^{-1} \in U$.

2.-Teorema: Eraztun integro unitario batean:

$$(a) = (b) \Longleftrightarrow a = bu \ , \ u \in U.$$

Frogapena: $A = bu$, u U $(\Longrightarrow b = au^{-1})$

$\Longleftrightarrow b/a$ eta a/b , eraztun integroa baita,

$\Longleftrightarrow (a) = (b)$ f.n.l.

* **Baliokideki u A-ren unitate bat da $\Longleftrightarrow$ alderanzkarria bada A-n.**

Elkartze erlazioa

Definizioa: a,b∈A elementuak "elkartuak" direla diogu, baldin

a = bu bada non u∈U baita.

Ondorioak: 1) a eta b elkartuak ========⇒ a/b eta b/a⇐======⇒ (a) = (b).

2) m/a eta n, m elkartuak ======⇒n/a.

1.- Teorema: Elkartze erlazioa, baliokidetasun erlazio bat da A-n, bateragarria biderkaketarekiko.

Frogapena: Idatz dezagun R elkartze erlazioa.

a) R Baliokidetazunezkoa dela erraz froga daiteke.

b) Bateragarritasuna: xRy eta x' Ry' =====⇒ xx' R yy'

izan ere, x = yu eta X' = y'u' ======⇒ xx' = yy'uu'

=======⇒ xy R xý´ f.n.l.

2.-Teorema: A multzoko / dibisibilitate erlazioak, A/R multzoan dibisibilitate erlazio antisimetriko bat induzitzen du.

Zatitzaile propio eta inpropioak

Definizioa: Eman dezagun a∈A elementua. a elementu honi elkartutako elementuak eta eraztunaren unitateak, a elementuaren zatitzailea "inpropioak" esaten dira. Beste gainontzeko zatitzaileak, existitzen badira,zatitzaile "propioak" esaten dira. Zatitzaile propiorik ez duen elementu bati, unitate bat ez bada, "irreduziblea" esaten zaio.

ERAZTUN FAKTORIALAK

Definizioa: Eraztun faktoriala (edo faktorizazio bakarreko eraztuna, edo eraztun gaussiarra (= Gauss-ena) ondoko bi baldintza hauek betetzen dituen integritate dominio bati esaten zaio:

1)Unitate ez den edozein a elementu bat, elementu irreduzibleen (berdinak ala ez) biderkadura finitua da:

$$a = p_1 p_2 \cdot\cdot\cdot\cdot p_r = \prod_{i=1}^{r} p_i$$

a irreduzibleretzat, ontzat ematen da honelako adierazpen bat, non r = 1 bai litzateke.

2)Deskonposaketa hau bakarra da, ordena eta unitate diren faktoreak ezik.

Ondorioak: Biz A faktoriala.

a) $a \in A$ elementuak ondoko bi deskonposaketa hauek baditu, $a = p_1 p_2 \cdot\cdot\cdot\cdot p_r = q_1 q_2 \cdot\cdot\cdot\cdot\cdot q_s$ non p_i, q_j irreduzibleak baitira, orduan zera dugu $r = s$ eta q_j guztiak ongi ordenatuz gero, p_i eta q_i elkartuak dira ($i = 1,2,\ldots.r$).

b) A/R zatidur erditaldea faktoriala da ere.

1.Teorema: Eman dezagun A integritate dominio bat eta jo dezagun goiko definizioaren lehenengo baldintza betetzen duela. Orduan, A faktoriala da baldin eta bakarrik baldin ondoko baldintza hau betetzen badu:

2') Edozein p elementu irreduzibleak, ab biderkadura bat zatitzen badu, horietako biderkagairen bat gutxienez zatitu behar du (Gauss-en baldintza).

Frogapena:

$\Longrightarrow$ Bira A eraztun faktoriala eta p elementu irreduzible bat non, ab zatitzen baitu:

$$ab = pc$$

- a eta b ez dira biak unitateak.
- Baldin bat unitate bada, a adibidez, $\Longrightarrow p/b$
- Eman ditzagun beraz, a, b eta c-ren deskonposaketa faktore

irreduzibletan

$$a = \prod_{i=1}^{r} p'_i \ , \quad b = \prod_{j=1}^{s} p''_j \ , \quad c = \prod_{l=1}^{t} q_l$$

Zera dugu: $\prod_{i=1}^{r} p'_i \cdot \prod_{j=1}^{s} p''_j = p \cdot \prod_{k=1}^{t} q_k$

Baina 2) baldintzaren ondorioz, p elementua p'_i , p''_j elementuaren baten elkartua da; beraz p elementuak zatitzen du a eta b elementuetatik bat, gutxienez.

<=====| Ikus dezagun orain alderantzizkoa: 2')-K 2)-ra darama halabeharrez. Frogapena egiteko errekurrentzia erabiliko dugu a-ren lehenengo deskonposaketan agertzen diren biderkagai irreduzibleen kopururen gain, r-ren gain halegia.
Bistan da proposapena egia dela r = 1-entzat, elementu irreduziblearen definizioarengatik. Jo dezagun orain, teorema egia dela lehenengo deskonposaketak r biderkagai baino gutxiago dituenean (r>1) eta izan bedi

$$a = \prod_{i=1}^{r} p_i = \prod_{j=1}^{s} q_j$$

P_1 elementu irreduzibleak

$q_1 \cdot \prod_{j=1}^{s} q_j$ zatitzen du,beraz, q_1 zatitzen du,

edo $\prod_{j=1}^{s} q_j$ zatitzen du;

Berriro gauza bera errepikatuaz behin eta berriz, ikusten da nola p_1 elementuak, zatitzen du q_j elementuetatik gutxienez bat. Ordena ditzagun q elementuak $p_1 \overset{K}{-} q_1$ zatitu dezan: q_1 irreduziblea denez gero eta p_1 unitate bat ez denez gero, p_1 eta q_1 elkartuak dira:

$q_1 = \epsilon_1 p_1$ non ϵ_1 unitate bat baita. Beraz

$a = p_1 p_2 \cdots\cdots p_r = \epsilon_1 p_1 q_2 \cdots\cdots q_s$

Baina A integritate dominioan $p_1 \neq 0$ elementua sinplifikagarria da, beraz,

$p_2 \cdots\cdots p_r = \epsilon_1 q_2 \cdots q_s = q'_2 \cdots q_s$

non $q'_2 = \epsilon_1 q_2$ irreduziblea baita;

Eta errekurrentzia-ko hipotesiari jarraituz [illegible]

tuta dago.

Eman dezagun A eraztun faktoriala eta azter dezagun unitateak ez diren elementuen zenbait propietate. Izan bedi a hauetako elementu bat.

1. Nola lortu a-ren zatitzaile guztiak:

Biz $a = P_1^{\alpha_1} p_2^{\alpha_2} \ldots\ldots p_e^{\alpha_e}$ $(p_i \neq P_j \; \alpha_i \geq 1)$

Baldin beste elementu a' batek a zatitzen badu, a'-ren faktore bakoitzak a zatitzen du ere, beraz faktore hori P_i baten elkartua da eta dagokion exponentea α_i' ez da α_i baino handiagoa. Beraz a-ren zatitzaile guztiak (unitate-faktore salbuespen) hauek dira:

P_i faktore irreduzibleekin eratutako biderkadurak, p_i bakoitzari ipintzen zaion exponentea α_i' honela mugatzen delarik

$$0 \leq \alpha_i' \leq \alpha_i$$

Beraz elementu batek a zatitzen badu, hauetako bat da (unitateak salbuespen) eta alderantziz, bistan den bezala hauetako bakoitzak a zatitzen du.

2. Bi elementuen zatitzaile komunak. Bi elementuen multiplo komunak.

a) Eman ditzagun $a, b \in A$ non a,b ez baitira unitateak $(a, b \notin U)$

$a \equiv \rho_1^{\alpha_1} \rho_2^{\alpha_2} \ldots \rho_e^{\alpha_e}$ (R) $\qquad b \equiv \rho_1^{\beta_1} \ldots \rho_e^{\beta_e}$ (R) $\quad (\alpha_i, \beta_i \geq 0)$

non p_i elementu batean gutxienez agertzen den faktore irreduzible bat baita.

a eta b-ren edozein zatitzaile komun h-rentzat, zera dugu:

$h \equiv \rho_1^{\lambda_1} \ldots \rho_e^{\lambda_e}$ (R) $\qquad$ non $0 \leq \lambda_i \leq \delta_i$ baita

eta $\delta_i = \min(\alpha_i, \beta_i)$

b) Era berean, a eta b-ren multiplo komun k batentzat, zera dugu: $k \equiv \rho_1^{k_1} \ldots \rho_e^{k_e}$ (R) non $\mu_i \leq K_i$ baita

eta $\mu_i = \max(\alpha_i, \beta_i)$

3. (a,b) z.k.h.

Goian idatzitako zatitzaile komun guztiek, haietako bat zatitzen dute: $z = \rho_1^{\delta_1} \ldots \rho_e^{\delta_e}$

Honi " a eta b-ren zatitzaile komunetatik handiena" esaten

zaio eta z = (a,b) z.k.h.

idatziko dugu.

Aski garbi dago z hau bakarra dela, A-ren unitate izan daitezkeen zenbait faktore salbuespen.

4. (a,b) m.k.t.

Goian idatzitako multiplo komun guztiak, haietako baten multiploak dira:

$$m = p_1^{\mu_1} \cdots p_e^{\mu_e}$$

Honi " a eta b-ren multiplo komunetatik txikiena" esaten zaio eta

m = (a,b) m.k.t.

idatziko dugu.

Lehen bezala, m bakarra da, A-ren unitate izan daitezkeen zenbait faktore salbuespen.

Bistan da : $\min(\alpha,\beta) + \max(\alpha,\beta) = \alpha + \beta$

beraz $\boxed{dm = ab}$

Era berean defini daitezke A-ren K elementuen m.k.t. eta z.k.h. Hauek ere bakarrak izango dira, unitate-faktoreak salbuespen.

Amaitu baino lehen, hitz bi "elementu elkarrekin primu" esaten zaienei buruz. Eman dezagun D integritate dominio bat eta biz e bere elementu unitatea.

D. Definizioa : Bi elementu $a,b \in D^* = D - \{0\}$ "zatitzaile komunik ez dutela" diogu, baldin a eta b zatitzen dituzten D ko elementu guztiak, unitateak badira.

Eraztuna FAKTORIALA bada, propietate hau beste honen kidekoa da: (a,b) z.k.h. = 1

2. Definizioa: Eman ditzagun $a,b \in D^* = D - \{0\}$. "a elementua b-kin primua dela "diogu, baldin D-ko elementu guztientzat hau betetzen bada: $b/ax \Longrightarrow b/x$

Ondorioa: a b-kin primua ========> b **a-kin primua.**

Frogapena: Jo dezagun a-k by zatitzen duela,

$$by = ax$$

Orduan hipotesisak dioenez, b/x

$$x = bq$$

Beraz $y = aq$. Beraz a/y. f.n.l.

a eta ***b*** elementuak "elkarrekin primuak direla" diogu.

Teorema:2.- Definizioak =======>1.- Definizioa.

Frogapena: Biz h, a eta b-ren zatitzaile komun bat.

$$a = a'h \qquad b = b'h$$

Beraz $ab' = ba'$

=======> b/b'. Beraz b eta b'elkartuak dira.

=======> h unitate bat da.

f.n.l.

Teorema: Eraztuna FAKTORIALA bada 1.- Definizioak ======> 2.- Definizioa.

Frogapena: Jo dezagun b/ax eta a eta b ez dutela zatitzaile komunik.

Zatitzaile komunik ez badute, ez dute izango faktore irreduzible berdinik. Beraz b-en agertzen den faktore irreduzible bakoitza x-en agertuko da ere, eta bere exponentea b-en ez da x-en duena baino handiagoa izango.

Beraz, b/x . f.n.l.

3.- Definizioa: Eman ditzagun a,b D. "a eta b elementuak Bezout-en erlazio bat betetzen duela" diogu, baldin existitzen badira D-en bi elementu x,y, non

$$xa + yb = e$$ baita.

Ondorioa: 3.- Definizioak ========>1.- Definizioa.

Baina jeneralean alderantzizkoa ez da egia izaten, nahiz eta eraztuna FAKTORIALA izan.

ERAZTUN EUKLIDEARRAK

Eman dezagun E eraztun trukakor bat, 0-ren zatitzailerik gabekoa.

Definizioa: E eraztun euklidearra dela diogu, baldin defini badaiteke aplikazio bat E^* eta zenbaki oso positiboen artean (≥ 0)

$$\varphi: \begin{array}{ccc} E^* & \longrightarrow & Z^+ \\ a & \longmapsto & a \end{array}$$

bi baldintza hauek betetzen dituelarik:

1.- Baldin b-k a zatitzen badu: $\varphi(b) \leq \varphi(a)$

2.- Baldin a eta b E-ko edozein bi elementu, $b \neq 0$, badira, exiztitzen dira E eraztunean q,r elementuak, non

$a = bq + r$ baita, eta baldin $r \neq 0$ bada, orduan $\varphi(r) < \varphi$ (baldin $r = 0$ bada, b / a, beraz 1.-).

Ondorioak:

1.- Eraztun euklidear batek badu lementu unitatea.

Esan dugun bezala $\varphi(E^*)$ Z^+-en azpimultzo ez-huts bat da. Ordenazio onaren printzipioz, $\varphi(E^*)$-k badu elementu minimo bat m. Balio minimo hau hartzen duten eraztunen elementuetatik aukera dezagun bat; biz a elementu hau. Beraz $\varphi(a) = m$ Definizioaren bigarren baldintza (a,a) bikoteari aplikatuaz, zera dugu: existitzen dira E eraztunean q,r, elementuak, non

$$a = aq + r \quad \text{baita.}$$

Baldin $r \neq 0$ bada, $\Longrightarrow \varphi(r) < \varphi(a)$. Baina hau ezina da, $\varphi(a)$ minimoa baita. Beraz $r = 0$ eta existitzen da q bat non

$$a = qa \quad \text{baita.}$$

Eman dezagun orain eraztunaren edozein x elementu bat:

$$xa = xqa$$

halabeharrez $(x - qx)a = 0$. Baina alde batetik $a \neq 0$ $\varphi(a)$ existitzen baita, eta bestetik E-n ez dago 0-ren zatitzailerik, beraz

$$x - qx = 0$$

$\forall x \in E$: $x = qx$ $\Longrightarrow$ q da eraztunaren elementu unitatea 1 bidez adieraziko dugu.

Bestalde $\forall a \in E$, $a = 1a$. Halabeharrez $\varphi(1) \leq \varphi(a)$ $\forall a \in E - \{0\}$

2.- (u) = (1) propietateak, eraztunaren u unitateak bereizten ditu:

Beste hitzetan adierazia:

u unitate bat da bba $\varphi(u) = \varphi(1)$ bada.

$\Longrightarrow$ Baldin u unitate bat bada, u/1. Beraz $\varphi(u) \leq \varphi(1)$. Baina lehen ikusi dugun bezala $\varphi(1) \leq \varphi(a)$ a guztientzat, beraz

$$\varphi(u) = \varphi(1)$$

$\Longleftarrow$ Baldin $\varphi(u) = \varphi(1)$ bada, kontutan izanik 1-ek elementu guztiak zatitzen dituela, eta hurrengo propietatea aplikatuaz u eta 1 elkartuak direla ondorioztatzen da. Beraz u unitate bat da.

3.- Eraztun euklidear batean baldin b-k a zatitzen badu eta $\varphi(a) = \varphi(b)$ bada, orduan a eta b elkartuak dira.

$b / a \Longrightarrow a = bq'$

Bestalde definizioaren bigarren baldintza aplikatuaz

$$b = aq + r.$$

Baldin $r \neq 0$ bada, $\varphi(r) < \varphi(a) = \varphi(b)$. Baina

$r = b - aq = b(1 - qq')$. Beraz, definizioaren lehengo baldintzak dioenez $\varphi(b) \leq \varphi(r)$.

Beraz $r = 0$ izan behar du.

Baina baldin $r = 0$ bada, $b = aq$ eta bestalde

$a = bq'$ Beraz a eta b elkartuak dira.

1.- Teorema: Eraztun euklidear E batean, zatitzaile komunik ez duten $E - \{0\}$ -ko bi elementuk a eta b Bezout-en identitate bat betetzen dute.

Frogapena:

Biz $I, E - \{0\}$ -ko α a + β b elementuen multzoa, non $\alpha \in E - \{0\}$ eta $\beta \in E - \{0\}$ baitira. Kontsidera dezagun $\varphi(\alpha a + \beta b)$ osoen multzoa.

Beraz eraztun euklidear batean, elementu primuei buruzko I eta 2 Definizioak, 7. eta 8. orrialdean, identikoak dira.

2.- Teorema: E Eraztun euklidear bat faktoriala da.

Frogapena: Frogatuko duguna hau da:

1) Unitate ez den edozein a elementu bat, elementu irreduzibleen biderkadura finitua da.

2) Edozein p elementu irreduzible batek, ab zatitzen badu, gutxienez horietako biderkagairen bat zatitu behar du.

1) Frogapena hau eratorpenez egingo dugu $\varphi(a)$ balioren gain.

a = 1 bada, propietatea egiazkoa da, $\varphi(a) = \varphi(1)$ berdintzak a unitate bat izatea bait dakar, halabeharrez. Jo dezagun teorema egiazko dela edozein a'-rentzat non $\varphi(a') < \varphi(a)$ eta froga dezagun teorema a-rentzat.

Baldin a laburtezina balitz, propietatea frogatuta legoke.

Baldin a laburtezina ez bada, a = bc izanen da, non ez b eta ez c ez dira a-ren elkartuak, eta $\varphi(b) < \varphi(a)$; $\varphi(c) < \varphi(a)$ zeren eta eraztun euklidear batean b-k a zatitzen badu eta $\varphi(b) = \varphi(a)$ badira, orduan a eta b elkartuak dira. Beraz, eratorpen-hipotesiari jarraituaz, b eta c biak, elementu laburtezinen biderkadura dira. Gauza bera gertatzen da ba beraz, a-rekin.

2') Froga dezagun orain bigarren propietate hau. Eman dezagun p laburtezina, $p \in E$ eta jo dezagun p-k ab zatitzen duela eta ez duela a zatitzen. Orduan p eta a ez dute zatitzaile komunik eta existitzen dira $\alpha \in E$ eta $\beta \in E$ non,

$$1 = x\, a + \beta\, p \qquad \text{baita.}$$

Beraz $$b = x\, ab + \beta\, bp$$

Eta p-k ab zatitzen duenez gero, p-k b zatitzen du.

3.- Teorema: E eraztun euklidear bat, eraztun printzipala da.

Frogapena:

Frogapena egin baino lehen, gogora dezagun zer den eraztun printzipal bat: eraztun trukakor bat, elementu unitateduna, eta non ideal guztiak printzipalak baitira. Egin dezagun orain frogapena: lehenego ta behin, E eraztun trukakorra eta elementu unitateduna da. Bestalde har dezagun E-ko $\mathfrak{A}$ ideal bat. Baldin $\mathfrak{A} = (0)$ bada, printzipala da. Pentsa dezagun beraz, $\mathfrak{A} \neq (0)$ dela. Kontsidera dezagun eraztun euklidearraren definizioan idatzi dugun funtzioa eta izan bedi a $\varphi(a)$ minimoa duten $\mathfrak{A}$ -ko elementuetatik bat. Biz x $\mathfrak{A}$-ko elementu bat.

E euklideoa denez gero, badira $q \in E$, $r \in E$ non

$x = aq + r$ baita; $r = 0$ delarik edo baldin $r \neq 0$ bada, $\varphi(r) < \varphi(a)$.

Baina azkeneko hau ezin gerta daiteke, a aukeratu dueun bezala izateagatik, hots, $\varphi(a)$ minimoa, beraz, $r = 0$ behar du izan. Beraz $x = aq$ eta $\mathfrak{A}$ ideal printzipala da, $\mathfrak{A} = (a)$.

4.- Teorema.- 0-ren zatitzailerik ez duen eraztun printzipal bat, eraztun faktoriala da.

Frogapena: Eraztun printzipal batean, edozein elementu bat, elementu laburtezin-kopuru finitu baten biderkadura da. Beraz faktoriala dela frogatzeko gelditzen zaigun gauza bakarra, deskonposaketa hau bakarra dela frogatzea da. Baina honetarako nahiko da Gaussen baldintza betetzen dela frogatzea (ikus 4. orrialdean 1.- Teorema).

Jo dezagun p elementu batek ab zatitzen duela. Eraztuna printzipala delarik, (a) + (b) ideala, printzipala da. Beraz badago eraztunean d elementu bat, non

$(a) + (b) = (d)$ baita

Badira beraz, u eta v elementuak eraztunean, non

$d = au + bv$ baita.

Bestalde (a) $\subseteq$ (d) eta (B) $\subseteq$ (d) direnez gero, badira eraztunean a'eta b'elementuak, non

$$a = a'd \qquad b = b'd \qquad \text{baita.}$$

Eraztun printzipal eta zeroen zatitzailerik gabeko batean, a eta b elementuak badute beraz, zatitzaile komunetik handien bat d, ondoko expresioak definituta

$$d = au + bv$$

Eta partikularrean, eraztun printzipal bateko a eta p bi lementu zatitzaile komunik ez badute, Bezout-en identitate batez lotuta daude:

$$1 = xa + yp.$$

Beraz, b bidez biderkatzen badugu

$$b = bxa + byp.$$

Baldin p-k ab zatitzen badu, orduan b ere zatitzen du.

Ondorioa: Eraztun printzipal batean, beraz euklidearretan ere, elementu primuei buruzko 1, 2, eta 3 Definizioak (7.8. orr.) baliokideak dira.

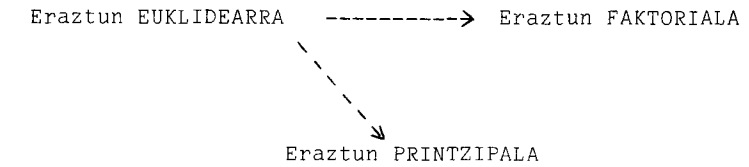
Ondorioa: Gaussen baldintza betetzen duen edozein integritate dominio batean, (partikularrean eraztun printzipal eta zeroren zatitzailerik gabeko batean), (a) ideala primua da, baldin eta solik baldin a laburtezina bada.

Frogapena: $xy \in (a) \Longrightarrow xy = \rho a \Longrightarrow$ baldin a laburtezina bada, a-k faktoreetatik bat zatitzen du, bis hau x, $\Longrightarrow x = ra$, hots, $x \in (a)$ eta (a) ideala ez litzateke primua izango.

Alderantziz, edozein eraztunean, baldin a laburtezina ez bada, (a) ez da primua zeren alde batetik a = pq non p edo q ez dira ez unitateak, ez a-rekiko elkartuak, eta bestetik $p = \rho a$ edo $q = \rho' a$ bateraezinak badira. Zera dugu bada,

$$pq \in (a)\ ,\ p \notin (a)\ ,\ q \notin (a) \text{ eta (a) ez da primua.}$$

Laburki:



Eraztun PRINTZIPALA eta 0-ren zatitzailerik gabekoa -----> Eraztun FAKTORIALA

APLIKAZIOAK EDO BI KASU PARTIKULARRAK. Z eta R(x) integritate dominioak.

Jakina da Dibisibilitatearen Teoria Z multzoan, duen zabalpena gure gizartean,txikitandik ikasten baitira adibidez, zenbaki primuak, zenbaki multzo baten m.k.t. , z.k.h. eta beste zenbait bitxitasun.
Era berean, (nahiz eta beste maila batean) R multzoa n koefizienteak dituzten polinomioen multzoa ikasterakoan, beste hainbeste explikatzen zaigu.
Azpimarratu nahi dugu behin eta berriz, Aritmetika elementalean (Z-ren kasuan) edo Algebran (R(x)-en kasuan) ikasten diren zenbait eta zenbait propietate Dibisibilitatearen teoriaren arloan, ez direla Z-ren edo R(x)-ren berezitasun batzuk, edozein integritate-eremu batenak baino, kontutan hartuaz noski, multzo hauetan behar bada, laburpen batzuk sortzen zaizkigula, kasu partikularrak baitira. Hala nola, unitateen multzoa Z-ren kasuan adibidez, $\{1,-1\}$ besterik ez da, eta R(x)-en kasuan ez-zero konstanteen multzoa.

Z eta R (x)-en azterketa sakona orain egingo ez badugu ere, aipa ditzagun hemen aurrean ipinitako teoria generalaren zenbait aplikazio:

Z MULTZOA

Z multzoa, zenbaki osoen multzoa halegia, batuketa eta biderkaketarekin integritate eremu bat da, hots, eraztun trukakorra, unitateduna eta zeroen zatitzailerik gabekoa.
Bestalde, Z multzoa aipatutako eragiketekin eraztun auklidear bat da, existitzen baita $\varphi : Z^+ \dashrightarrow Z^+$ aplikazioa, definizioak eskatzen dituen baldintzak betetzen dituelarik, beraz, printzipala eta faktoriala. Eraztun honen elementu laburtezinak edo irreduzibleak, normalean primuak deitzen direnak dira.
Eraztun honetan unitateak 1 eta -1 dira eta horiek bakarrik.
Horregatik a zenbaki baten elementu elkartuak -a eta a bera dira bakarrik.

Elkartze erlazioak, baliokidetasun erlazio bat denez gero, zatidura-multzo bat sortzen du $Z/R = \{(x,-x) / x \in Z\}$. Erdi talde trukakorra da $N \vee \{o\}$-rekiko isomorfoa.

R elkartze erlazio hau eta $f: Z \longrightarrow Z^{+} \vee \{0\}$ aplikazioak definitzen duen baliokidetasun eralzioa, berdinak dira.

$x \longmapsto |x| = \sup(x,-x)$

R[x] multzoa

R gorputza denez gero, R (x) integritate eremu bat da, hots eraztun trukakorra unitateduna eta zeroren zatitzailerik gabekoa, batuketa eta biderkaketa barne- eragiketak bezala.

Bestalde, R (x) multzoa aipatutako eragiketekin eraztun euklidear bat da, existitzen baita $\varphi: R(x) - \{o\} \longrightarrow Z^{+} \vee \{0\}$

$F \longmapsto gr.f = f.$ maila

aplokazioa, definizioak eskatzen dituen baldintzak betetzen dituelarik. Izan ere:

1) $f/g \Longrightarrow gr\ f < gr\ g \Longleftrightarrow \varphi(f) < \varphi(g)$

2) $\forall f,g \in R(x) \wedge g \neq o, \exists g,r \in R(x) \ni f = gg + r$ non $r = o$ ala $\varphi(r) < \varphi(g)$. baita.

Beraz R(x) eraztun euklidearra da eta horregatik printzipala eta faktoriala ere. Eraztun honen elementu laburtezinak edo irreduzibleak, lehenengo graduko polinomiak eta R-en zerorik ez duten bigarren graduko polinomioak dira. Eraztun honetan unitateak ez-zero diren konstanteak dira eta horiek bakarrik. Beraz R^{*} multzoko elementuak.

BIGARREN GAIA

ZENBAKIEN TEORIAREN

FUNTZIO GARRANTZITSUENAK

- $[x]$, $\{x\}$ funtzioak.
- Zenbaki baten zatitzaileen kopuruko batukaketak.
- Möbius-en funtzioa.
- Euler-en funtzioa.

BIGARREN GAIA

ZENBAKIEN TEORIAREN FUNTZIO GARRANTZITSUENAK

§ 1. $[x]$, $\{x\}$ FUNTZIOAK

a.-Zenbakien teorian, $[x]$ funtzioak paper garrantzitsua dauka; hau x-en balio erreal guztietarako definitzen da eta x baino ttikiagoa den zenbaki osoen arteko handiena adierazten du. Funtzio hau x-en parte osoa deitzen da.

Adibideak

$$[1] = 1 \quad ; \quad [2,6] = 2 \quad ; \quad [-4,75] = -5$$

Batzutan, $\{x\} = x - [x]$ funtzioa ere kontsideratzen da. Funtzio hau x-en parte frakzionari edo zatikiar deitzen da.

Adibideak

$$\{1\} = 0 \quad ; \quad \{2,6\} = 0,6 \quad ; \quad \{-4,75\} = 0,25$$

b.-Sartu ditugun funtzioek zertarako balio duten erakusteko, datorren teorema frogatuko dugu:

n! delakoaren biderkaduran, p zenbaki primuak duen berretzailea, zera da:

$$\left[\frac{n}{p}\right] + \left[\frac{n}{p^2}\right] + \left[\frac{n}{p^3}\right] + \cdots$$

Frogapena

n! biderkaduran, p zenbakiaren multiplo diren faktoreen kopurua $\left[\frac{n}{p}\right]$ da, haien artean, p^2 delakoaren multiploak, $\left[\frac{n}{p^2}\right]$ dira, hauen artean p^3-ren multiploak $\left[\frac{n}{p^3}\right]$ dira; eta abar.

Adierazitako zenbakien batuketak, bilatutako berretzailea ematen du, zeren n! biderkaduran p^m-ren multiplo, baina ez p^{m+1}-ren multiploa, den faktore bakoitza, m bider adierazi dugun moduz kontatzen da, p-ren, p^2-ren, p^3-ren... eta azkenez p^m-ren multiplo moduz.

Adibidea

40! biderkaduran, 3 zenbakiaren berretzailea ondokoa da:

$$\left[\frac{40}{3}\right] + \left[\frac{40}{9}\right] + \left[\frac{40}{27}\right] = 13 + 4 + 1 = 18$$

§ 2.ZENBAKI BATEN ZATITZAILEEI HADATURIKO BATUKETAK

a.-Zenbakien teorian funtzio multiplikatiboak oso paper garrantzitsua daukate. $\Theta(a)$ funtzio bat multiplikatibo deitzen da,datozen baldintzak kunplitzen badira:

1- $\Theta(a)$ funtzioa,a zenbaki oso positibo guztietarako definituta badago eta honelako a batentzat ere zero egiten ez bada.

2- Edozein a_1 eta a_2 zenbaki oso positiboentzat,beren artean primu izanik,

$$\Theta(a_1 \cdot a_2) = \Theta(a_1) \cdot \Theta(a_2)$$

Adibidea

Erraz ikusten da $\Theta(a) = a^s$ funtzioa multiplikatiboa dela,s delakoa edozein zenbaki erreal edo konplexu izanik.

b.- $\Theta(a)$ funtzioaren adierazitako propietateetik, $\Theta(1) = 1$ dela ateratzen da.

Suposa dezagun, $\Theta(a_2)$ zero ez dela.Orduan : $\Theta(a_2) = \Theta(1 \cdot a_2) = \Theta(1)\,\Theta(a_2)$;hau da: $\Theta(1) = 1$.

Gainera,hurrengo propietate garrantzitsua ateratzen dugu: $\Theta_1(a)$ eta $\Theta_2(a)$ funtzioak,multiplikatiboak badira,orduan $\Theta_3(a) = \Theta_1(a)\,\Theta_2(a)$ funtzioa ere multiplikatiboa da.

Frogapena

$\Theta_3(1) = \Theta_1(1)\,\Theta_2(1) = 1$ daukagu.

Gainera, $(a_1, a_2) = 1$ betetzen den kasuan,zera geratzen da:

$$\Theta_3(a_1 \cdot a_2) = \Theta_1(a_1 \cdot a_2)\,\Theta_2(a_1 \cdot a_2) = \Theta_1(a_1)\cdot\Theta_1(a_2)\cdot\Theta_2(a_1)\Theta_2(a_2) =$$

$$= \Theta_1(a_1)\Theta_2(a_1)\,\Theta_1(a_2)\Theta_2(a_2) = \Theta_3(a_1)\,\Theta_3(a_2)$$

c.-Bira $\Theta(a)$ funtzio multiplikatibo bat eta $a = p_1^{\alpha_1} \cdot p_2^{\alpha_2} \cdots p_k^{\alpha_k}$,a zenbakiaren deskonposaketa kanonikoa.

$\sum_{d|a}$ notazioaz,a zenbakiaren d zatitzaile guztiei hedaturiko batuketa adierazten badugu,zera daukagu:

$$\sum_{d|a} \theta(d) = \left(1 + \theta(p_1) + \theta(p_1^2) + \ldots + \theta(p_1^{\alpha_1})\right) \cdots \left(1 + \theta(p_k) + \theta(p_k^2) + \ldots + \theta(p_k^{\alpha_k})\right)$$

(a=1 kasuan,bigarren atala 1 dela suposatzen da)
Identitate hau frogatzeko,bigarren atalean parentesiek ireki ditzagun.Gaien batuketa bat ateratzen da,ondoko forma hau daukalarik:

$$\theta(p_1^{\beta_1}) \theta(p_2^{\beta_2}) \cdots \theta(p_k^{\beta_k}) = \theta(p_1^{\beta_1} p_2^{\beta_2} \cdots p_k^{\beta_k}) ;$$

$$0 \le \beta_1 \le \alpha_1 , \quad 0 \le \beta_2 \le \alpha_2 , \ldots , \quad 0 \le \beta_k \le \alpha_k$$

non termino hauen artean zenbaki primu guztiak dauden eta behin bakarrik;Hau da, $(e, \xi 6, cdp\ I)$ lehenengo atalean dagoena.

d.- $\theta(a) = a^s$ funtzioaren kasuan, c propietateak forma hau hartzen du:

$$\sum_{d|a} d^s = \left(1 + p_1^s + p_1^{2s} + \cdots + p_1^{\alpha_1 s}\right) \cdots \left(1 + p_k^s + p_k^{2s} + \cdots + p_k^{\alpha_k s}\right)$$

Partikularki, s=1 kasuan,lehen atalak a zenbakiaren $S(a)$ zatitzaileen batuketa adierazten du.Bigarren atala sinplifikatzen badugu,zera daukagu:

$$S(a) = \frac{p_1^{\alpha_1+1} - 1}{p_1 - 1} \cdot \frac{p_2^{\alpha_2+1} - 1}{p_2 - 1} \cdots \frac{p_k^{\alpha_k+1} - 1}{p_k - 1}$$

Adibidea

$$S(720) = S(2^4 \cdot 3^2 \cdot 5) = \frac{2^5 - 1}{2 - 1} \cdot \frac{3^3 - 1}{3 - 1} \cdot \frac{5^2 - 1}{5 - 1} = 2418$$

$S=0$ kasuan,aurreko expresioaren lehen atalak a zenbakiaren $\tau(a)$ zatitzaileen zenbakia adierazten du,eta hauxe daukagu:

$$\tau(a) = (\alpha_1 + 1)(\alpha_2 + 1) \cdots (\alpha_k + 1)$$

Adibidea

$$\tau(720) = (4+1)(2+1)(1+1) = 30$$

§ 3.MÖBIUS-EN FUNTZIOA

a.- $\mu(a)$ Möbius-en funtzioa, a zenbaki oso positibo guztietarako definitzen da. Funtzio hau datozen berdintzekin definitzen da:

- $\mu(a) = 0$ a, delakoa unitatea ez den karratu batez zatigarri bada.
- $\mu(a) = (-1)^K$ a delakoa karratu batez zatigarri ez bada; hemen k berretzaileak a zenbakiaren zatitzaile primuen kopurua adierazten du.

Partikularki, $a = 1$ kasuan, $K = 0$ kontsideratzen da eta horregatik $\mu(1) = 1$ hartzen dugu.

Adibideak

$\mu(1) = 1$; $\mu(5) = -1$; $\mu(9) = 0$

$\mu(2) = -1$; $\mu(6) = 1$; $\mu(10) = 1$

$\mu(3) = -1$; $\mu(7) = -1$; $\mu(11) = -1$

$\mu(4) = 0$; $\mu(8) = 0$; $\mu(12) = 0$

b.-Bira $\theta(a)$ funtzio multiplikatibo bat eta $a = p_1^{\alpha_1} \cdot p_2^{\alpha_2} \cdots p_K^{\alpha_K}$ a zenbakiaren deskonposaketa kanonikonoa. Orduan:

$$\sum_{d \mid a} \mu(d)\theta(d) = (1 - \theta(p_1))(1 - \theta(p_2)) \cdots (1 - \theta(p_K))$$

(a=1 kasuan bigarren atala unitatea dela suposatzen da)

$\mu(a)$ funtzioa multiplikatiboa da. Horregatik, $\theta_1(a) = \mu(a)\cdot\theta(a)$ funtzioa ere multiplikatiboa da. $\theta_1(a)$ funtzioari c-identitatea aplikatuz eta

$$\left\{ \begin{array}{l} \theta_1(p) = -\theta(p) \\ \theta_1(p^s) = 0 \quad s > 1 \text{ bada} \end{array} \right\}$$

direla kontutan daukagula, teorema hau zuzena dela ikusten dugu.

c.-Partikularki, $\theta(a) = 1$ eginez gero, b puntutik zera ateratzen dugu:

$$\sum_{d/a} \mu(d) = \begin{cases} 0, & a>1 \quad \text{baldin bada} \\ 1, & a=1 \quad \text{bada} \end{cases}$$

$\theta(d) = \frac{1}{d}$ eginez gero:

$$\sum_{d/a} \frac{\mu(d)}{d} = \begin{cases} \left(1-\frac{1}{p_1}\right)\left(1-\frac{1}{p_2}\right)\cdots\left(1-\frac{1}{p_k}\right), & a>1 \quad \text{bada} \\ 1 & a=1 \quad \text{bada} \end{cases}$$

d.-Suposa dazagun orain $\delta = \delta_1, \delta_2, \ldots, \delta_n$ zenbaki oso positiboak, $f = f_1, f_2, \ldots, f_n$ balio erreal edo konplexuekin korrespondentzian daudela.

Orduan,1 balioarekin korrespondentzian dauden f balioen batuketa, S' denotatuz,eta d zenbakiaren multiplo diren δ balioekin korrespondentzian dauden f balioen batuketa, S_d denotatuz,ondokoa dugu:

$$S' = \Sigma \mu(d) \cdot S_d$$

(non d delakoak, δ balioetariko bat gutxienez zatitzen duten zenbaki oso positibo guztien balioak hartzen baititu)

Frogapena

c atala aplikatuz,ondokoa dugu berehala:

$$S' = f_1 \sum_{d/\delta_1} \mu(d) + f_2 \sum_{d/\delta_2} \mu(d) + \cdots + f_n \sum_{d/\delta_n} \mu(d)$$

d zenbakiaren balio berbera duten gai guztiak batuz eta $\mu(d)$ parentesiaren kanpora ateraz gero,parentesi artean geldituko zaiguna,zera da: d delakoaren multiplo diren δ zenbakiekin korrespondentzian dauden f zenbakien batuketa;eta hori,definizioz, S_d da.

Beraz, $S' = \Sigma \mu(d) S_d$ (f n q l).

§ 4.EULER-EN FUNTZIOA

a.- $\varphi(a)$ Euler-en funtzioa, a zenbaki oso positibo guztietarako definitzen da eta $0, 1, \cdots, a-1$ [1] segidan, a-rekin primu diren zenbakien kopurua adierazten du.

Adibideak

$$\varphi(1) = 1 \quad ; \quad \varphi(4) = 2$$
$$\varphi(2) = 1 \quad ; \quad \varphi(5) = 4$$
$$\varphi(3) = 2 \quad ; \quad \varphi(6) = 2$$

b.- Biz $a = p_1^{\alpha_1} p_2^{\alpha_2} \cdots p_\kappa^{\alpha_\kappa}$ [2]
a zenbakiaren deskonposaketa kanonikoa.Orduan:

$$\varphi(a) = a\left(1 - \frac{1}{p_1}\right)\left(1 - \frac{1}{p_2}\right) \cdots \left(1 - \frac{1}{p_\kappa}\right), \quad [3]$$

edo beste modu batetara:

$$\varphi(a) = \left(p_1^{\alpha_1} - p_1^{\alpha_1 - 1}\right)\left(p_2^{\alpha_2} - p_2^{\alpha_2 - 1}\right) \cdots \left(p_\kappa^{\alpha_\kappa} - p_\kappa^{\alpha_\kappa - 1}\right) \quad [4]$$

partikularki,

$$\varphi(p^\alpha) = p^\alpha - p^{\alpha-1}, \quad \varphi(p) = p - 1 \quad [5]$$

Aplika dezagun § 3 ,d teorema.Kasu honetan, δ_κ zenbakiak eta f_κ zenbakiak honela definitzen ditugu:
Suposa dezagun,k azpiindizeak [1] segidaren zenbakiak kurritzen dituela.Egin dezagun, $\delta_\kappa = (\kappa, a)$ eta δ_κ balio bakoitza korrespondentzian jarriko dugu $f_\kappa = 1$ zenbakiarekin.
Orduan,S' delakoa, $\delta_\kappa = (\kappa, a)$ balioetarik 1 direnen kopurua,hau da, $\varphi(a)$ izango da;eta S_d delakoa, $\delta_\kappa = (\kappa, a)$ balioetarik d-ren multiplo direnen kopurua izango da.
Baina(k,a)d-ren multiploa izan daiteke,bakarrik d a-ren zatitzailea denean.Baldintza hau betetzen denean, S_d delakoa d-ren multiplo diren k balioen kopúrua izango da,hau da, $\frac{a}{d}$ izango da.
Hala,ba: $\varphi(a) = \sum_{d|a} \mu(d) \frac{a}{d}$ .daukagu,eta

hemendik, § 3 ,c kontuetan hartuz,(3) formula ateratzen da;eta honetatik,(2) erabiliz,(4) formula ateratzen da.

Adibideak

$$\varphi(60) = 60\left(1-\frac{1}{2}\right)\left(1-\frac{1}{3}\right)\left(1-\frac{1}{5}\right) = 16 \;;$$

$$\varphi(81) = 81-27 = 54$$

$$\varphi(5) = 5-1 = 4$$

c.- $\varphi(a)$ funtzioa multiplikatiboa da $(a_1, a_2)=1$ bada,b puntutik $\varphi(a_1 a_2) = \varphi(a_1)\varphi(a_2)$ ateratzen da.

Adibidea

$$\varphi(405) = \varphi(81)\varphi(5) = 54 \cdot 4 = 216 \;;$$

d.- $\sum_{d|a} \varphi(d) = a$

Formula honen baliõgarritasuna ikusteko § 2 ,c identitatea aplikatzen dugu $\theta(a) = \varphi(a)$ funtzioaren kasurako

$$\sum_{d|a} \varphi(d) = \left(1+\varphi(p_1)+\varphi(p_1^2)+\cdots+\varphi(p_1^{\alpha_1})\right)\cdots\left(1+\varphi(p_k)+\cdots+\varphi(p_k^{\alpha_k})\right)$$

(5) erabiliz,bigarren atala honela idatz daiteke:

$$\left(1+(p_1-1)+(p_1^2-p_1)+\cdots+(p_1^{\alpha_1}-p_1^{\alpha_1-1})\right)\cdots\left(1+(p_k-1)+(p_k^2-p_k)+\cdots+(p_k^{\alpha_k}-p_k^{\alpha_k-1})\right)$$

eta hau,gai berberak parentesi handi bakoitzean laburtu eta gero, $p_1^{\alpha_1} p_2^{\alpha_2}\cdots p_k^{\alpha_k} = a$ geratzen da.

Adibidea

a = 12 Egiten badugu,

$$\varphi(1)+\varphi(2)+\varphi(3)+\varphi(4)+\varphi(6)+\varphi(12) =$$

$$= 1+1+2+2+2+4 = 12$$

HIRUGARREN GAIA

KONGRUENTZIAK

- Definizioak.
- Kongruentzien oinharrizko propietateak.
- Moduluari dagozkion kongruentzien propietateak.
- Modulu batekiko hondar klaseen eraztuna.
- Z_m-n eragiketak.
- Hondarren sistema osoa.
- Hodarren sistema laburtua.
- Euler-en funtzioaren propietate multiplikatiboa.
- Euler-en teoreme.
- Moduluarekiko primuak diren hondarren talde multiplikatiboa.

KONGRUENTZIAK

DEFINIZIOAK

1. Bira a, b, m $\in$ Z eta m > 0 a - b zenbakia m zenbakiaz zatigarria bada, orduan a eta b zenbakiak m moduluarekiko kongruenteak direla esaten da. $a \equiv b \pmod{m}$ idazten da eta a kongruente b m modulu irakurtzen.

Emandako definizioa oinarrizkotzat hartuz ondoko definizio baliokide hauk ditugu:

2. a eta b zenbakiak m moduluarekiko kongruenteak dira baldin eta soilik baldin $a = b + mq$ $q \in Z$ berdintza betetzen bada.

3. Biz a, b $\in$ Z eta kontsidera dezagun hondarra duen zatiketa

$$a = m q + r_1 \qquad 0 \leq r_1 < m$$

$$b = m q + r_2 \qquad 0 \leq r_2 < m$$

orduan a eta b m- moduluarekiko kongruenteak dira baldin eta soilik baldin $r_1 = r_2$ bada.

Dakusagun definizio hauen baliokidetasuna:

- 1 eta 2 definioak baliokideak dira:

Suposa dezagun a eta b 1.definizioaren araura m moduluarekiko kongruenteak direla, orduan:

$$a \equiv b \pmod{m} \iff m / a - b \iff a - b = m q, \; q \in Z \iff$$

$$\iff a = b + m q, \; q \in Z$$

Beraz a eta b m moduluarekiko kongruenteak dira 2.definizioaren aranera.

- 1. eta 3.definizioak baliokideak dira:

Suposa dezagun a eta b 1.definizioaren araura m moduluarekiko kongruenteak direla eta kontsidera ditzagun hondarra dituen ondoko zatiketak:

$$a = m q_1 + r_1 \qquad 0 \leq r_1 < m$$

$$b = m q_2 + r_2 \qquad 0 \leq r_2 < m$$

Berdintza hauen kenketa eginik zera dugu:

$$a - b = m\,(q_1 - q_2) + (r_1 - r_2)\text{, baina nola } m \mid a - b$$

1.definizioaren arauera orduan $m \mid r_1 - r_2$.

Baina $0 \leq r_2 \leq r_1 < m \Rightarrow 0 \leq r_1 - r_2 < m$.

Orduan: $m \mid r_1 - r_2$ eta $0 \leq r_1 - r_2 < m \rightarrow r_1 - r_2 = 0 \rightarrow r_1 = r_2$

Alderantziz:

Suposa dezagun $r_1 = r_2 \rightarrow a - b = m\,(q_1 - q_2) \rightarrow m \mid a - b \rightarrow$

$\rightarrow a \equiv b \pmod m$ 1.definizioaren arauera.

Honela 1. 2. eta 3.definizioa baliokideak direla frogaturik dago.

KONGRUENTZIEN OINARRIZKO PROPIETATEAK

1.- Erreflexiboa

$a \equiv a \pmod m \qquad \forall\, a \in Z$

Hau argi dago, zeren $m \mid 0$ betetzen baita.

2.- Simetrikoa

$a \equiv b \pmod m \rightarrow b \equiv a \pmod m$

Berehalakoa da, zeren $m \mid a - b \leftrightarrow m \mid b - a$.

3.- Transitiboa

$a \equiv b \pmod m$ eta $b \equiv c \pmod m \Rightarrow a \equiv c \pmod m$

Frogapena

$a \equiv b \pmod m \wedge b \equiv c \pmod m \rightarrow$

$a = b + m q_1 \wedge b = c + m q_2 \rightarrow a = c + m q_1 + m q_2 =$

$= c + m\,(q_1 + q_2) = c + m q \rightarrow a \equiv c \pmod m$

4.- m modulu batekiko kongruentziak gaiz gai batu eta ken daitezke, hau da:

$a \equiv b \pmod m \wedge c \equiv d \pmod m \rightarrow a \pm c \equiv b \pm d \pmod m$

Frogapena

$a \equiv b \pmod m \wedge c \equiv d \pmod m \rightarrow$

$$\rightarrow \begin{cases} a = b + m q_1\,, & q_1 \in Z \\ c = d + m q_2\,, & q_2 \in Z \end{cases} \rightarrow a \pm c = b \pm d + m\,(q_1 \pm q_2)\,,\ q_1 \pm q_2 \in Z \rightarrow$$

$\rightarrow a \pm c \equiv b \pm d \pmod m$

Propietate hau n kongruentzia ditugun kasura era heda daiteke, hots:

$a_i \equiv b_i \pmod m \qquad \forall\ i = 1, \ldots, n \rightarrow \sum_{i=1}^{n} a_i \equiv \sum_{i=1}^{n} b_i \pmod m$

Korolarioa

$a \equiv b + c \pmod m \rightarrow a - c \equiv b \pmod m$

Frogapena:

$$\left.\begin{array}{l} a \equiv b + c \pmod m \\ c = c \pmod m \end{array}\right\} \rightarrow a - c \equiv b \pmod m$$

5.- Kongruentzia baten edozein atali (gairi) moduluaren multiplo bat gehitu edo kendu ahal zaio, hots: $a \equiv b \pmod m \rightarrow a \equiv b \pm km \pmod m \ \forall k \in Z$.

Frogapena

$$\left.\begin{array}{l} \forall\, a \equiv b \pmod m \\ 0 \equiv km \pmod m \end{array}\right\} \rightarrow a \equiv b \pm k\,m \pmod m \quad \forall\, k \in Z$$

6.- m modulu batekiko bi kongruentzia atalez atal biderkatu ahal dira; hau da:

$$\left.\begin{array}{l} a \equiv b \pmod m \\ c \equiv d \pmod m \end{array}\right\} \rightarrow a\,c \equiv b\,d \pmod m$$

Frogapena;

$$\left.\begin{array}{l} a = b + m\,q_1 \ , \ q_1 \in Z \\ c = d + m\,q_2 \ , \ q_2 \in Z \end{array}\right\} \rightarrow a\,c = b\,d + m\,(q_1 d + q_2 b + q_1 q_2 m)$$

$q = q_1 d + q_2 b + q_1 q_2 m \in Z \rightarrow a\,c = b\,d + m\,q \ , \ q \in Z \rightarrow$

$\rightarrow a\,c \equiv b\,d \pmod m$

1. Korolarioa

a) $a_i \equiv b_i \pmod m \quad i = 1, \ldots, n \rightarrow \prod_{i=1}^{n} a_i \equiv \prod_{i=1}^{n} b_i \pmod m$

b) $a \equiv b \pmod m \rightarrow a^n \equiv b^n \pmod m$

c) $a \equiv b \pmod m \rightarrow a\,k \equiv b\,k \pmod m$

Frogapena:

a) eta b) kasuak indukzioz errez froga daitezke eta c) kasua berehalakoa da.

7.- Kongruentzia baten atal biak moduluarekin primua den zatitzaile batez zatikatu ahal dira, hau da:

$$a\,k \equiv b\,k \pmod m \ \wedge \ (k, m) = 1 \rightarrow a \equiv b \pmod m$$

Frogapena:

$a\,k \equiv b\,k \pmod m \rightarrow m \mid a\,k - b\,k \rightarrow m \mid k\,(a - b) \rightarrow$

$\rightarrow m \mid a - b \rightarrow a = b \pmod m \ , \quad (m,k) = 1$

$(m,k)=1$

MODULUARI DAGOZKION KONGRUENTZIEN PROPIETATEAK

1 - Kongruentzia baten atal biak eta modulua faktore positibo berdin batez biderkatu ahal dira, hots:

$$a \equiv b \ (m \text{ mod}) \longrightarrow a\,k \equiv b\,k \ (mk \text{ mod}) \ , \ k > 0$$

Frogapena:

$a \equiv b \ (m \text{ mod}) \longrightarrow a = b + m\,q \ , \ q \in Z \longrightarrow a\,k = b\,k + m\,q\,k, \ k > 0 \longrightarrow$
$\longrightarrow a\,k \equiv b\,k \ (mk \text{ mod})$

2 - Kongruentzia baten atal biak eta modulua zatitzaile positibo berdin batez zatikatu ahal dira, halegia:

$$a\,k \equiv b\,k \ (mk \text{ mod}) \longrightarrow a \equiv b \ (m \text{ mod})$$

Frogapena:

$a\,k \equiv b\,k \ (mk \text{ mod}) \longrightarrow a\,k = b\,k + m\,k\,q \ , \ q \in Z \longrightarrow$
$\longrightarrow a = b + m\,q \ , \ q \in Z \longrightarrow a \equiv b \ (m \text{ mod})$

3 - Bi zenbaki m modulu batekiko kongruenteak badira, orduan moduluaren edozein zatitzailearekiko kongruenteak dira, halegia:

$$a \equiv b \ (m \text{ mod}) \wedge d \mid m \longrightarrow a \equiv b \ (d \text{ mod})$$

Frogapena;

$a \equiv b \ (m \text{ mod}) \wedge d \mid m \rightarrow m \mid a - b \wedge d \mid m \rightarrow d \mid a - b \rightarrow a = b \ (d \text{ mod})$

4 - $a \equiv b \ (m \text{ mod}) \wedge d \mid (a, m) \longrightarrow d \mid b$

Frogapena:

$a \equiv b \ (m \text{ mod}) \quad a = b + m\,q \ , \ q \in Z \rightarrow b = a - m\,t \wedge d \mid (a,m) \rightarrow d \mid b$

Ondorioa:

$a \equiv b \ (m \text{ mod}) \rightarrow (a, m) = (b, m)$

5 - $a \equiv b \ (m_i \text{ mod}) \quad i = 1, \ldots, n \rightarrow a \equiv b \ (m \text{ mod})$, non $m = [m_1, \ldots, m_n]$ baita. (multiplo komunetako txikien)

Frogapena:

$a \equiv b \ (m_i \text{ mod}) \quad i = 1, \ldots, n \rightarrow m_i \mid a - b \quad i = 1, \ldots, n \rightarrow$
$\rightarrow m \mid a - b$ non $m = [m_1, \ldots m_n]$ baita $\longrightarrow a \equiv b \ (m \text{ mod})$

Korolarioa

Biz $m = m_1, \ldots, m_n$ non $(m_i, m_j) = 1 \ \forall \ i, j$. Orduan:
$a \equiv b \ (m \text{ mod})$ kongruentzia eta $a \equiv b \ (m_i \text{ mod}) \quad i = 1, \ldots, n$ kongruentzien sistema baliokideak dira.

Frogapena:

$(m_i, m_j) = 1 \quad \forall \ i,j \rightarrow [m_1, \ldots, m_n] = m_1 \cdots m_n = m$.

OHARRA - Korolario honen bidez kongruentzia bat kongruentzien sistema baten deskonposatu ahal da, non sistemako kongruentzien moduluak emandako kongruentziarena baino ttikiagoak baitira.

Aurrerago ikusiko denez $a \equiv b \ (m \text{ mod})$ kongruentzia errazenik, non $m = p_1^{\alpha_1} \cdots p_n^{\alpha_n}$ moduluaren faktore primuen deskonposaketa baita, kongruentzien ondoko sisteman deskonposatzen da:

$$a \equiv b \ (p_1^{\alpha_1} \text{ mod})$$
$$\cdots\cdots\cdots\cdots\cdots$$
$$a \equiv b \ (p_n^{\alpha_n} \text{ mod})$$

MODULU BATEKIKO HONDAR KLASEEN ERHAZTUNA

Kontsidera dezagun Z multzoa eta $m \in Z$, $m > 0$ modulu bat. Demagun Zn Rm ondoko erlazio hau:

$$a \; R_m b \leftrightarrow a \equiv b \pmod{m}$$

Kongruentziei buruz betetzen diren lehengo hiru propietateak kontsideratuz R_m baliokidetasun erlazio bat dugu; beraz partiketa honek Z / R_m zatidur multzo bat .

$$Z / R_m = Z_m \text{ idatzi ohi da.}$$

Z_m zatidur multzoaren klase bakoitza banan banan kongruenteak diren elementuetaz osatzen da. Klase bakoitzean ordezkari bat hautatuko dugu.

Izan $\bar{a}$ Z_m ren klase bat, hau da $\bar{a} \in Z_m$
Zeintzu dira $\bar{a}$ klasearen elementuak?

$a = m q + r \quad 0 \leq r < m \rightarrow a \equiv r \pmod{m} \rightarrow \bar{a} = \bar{r}$

$\bar{r}$ klasearen elementu guztiak edukitzeko q zenbakiak Z ren balio guztiak hartu behar ditu.

Beraz klase bakoitzean elementuak kopuru infinituan daude. Klase bakoitzaren elementu guztiak m zenbakiaz zatikatuz hondar bera ematen dute. Beraz, klasean kopurua m - 1 da, zeren Z_m zatidur multzoan hondar posibleak 0, 1, ..., m - 1 baitira. Honelatan ba: $Z_m = \{0, 1, \ldots, m-1\}$
Klase bakoitzaren elementuak hondarrak deitzen dira eta Z_m m moduluarekiko hondar klasean multzoa.

Z_m n ERAGIKETAK

Z_m n ondoko eragiketak definituko ditugu:

a) Batuketa $\forall \bar{a}, \bar{b} \in Z_m \qquad \bar{a} + \bar{b} = \overline{a + b}$

b) Biderkaketa $\forall \bar{a}, \bar{b} \in Z_m \qquad \bar{a} \cdot \bar{b} = \overline{a \cdot b}$

R_m baliokidetasun erlazioa biderkaketa eta batuketarekin kompatiblea da. Zeren ondoko propietate hauk betetzen baitziren

$$\left.\begin{array}{l} a \equiv b \pmod{m} \\ c \equiv d \pmod{m} \end{array}\right\} \rightarrow a + c \equiv b + d \pmod{m} \wedge ac \equiv bd \pmod{m}$$

Horrez gainera definituriko batuketa eta kenketa ondo definiturik daude, zeren klase bakoitzaren edozein elementu harturik emaitza ez baita aldatzen

1. TEOREMA - Z_m hondar klaseen multzoa, definituriko batuketa eta biderkaketarekin erhaztun trukakor bat da, unitate elementuarekin.

Frogapena:

a) $(Z_m, +)$ talde trukakor bat da.

b) $(Z_m, .)$ erditalde trukakora da eta unitate elementua du.

c) Biderkaketarekiko batuketaren propietate banakorra betetzen da.

Hiru puntu hauk errez froga daitezke.

2. TEOREMA - m zenbaki konposatua bada, orduan Z_m zeroaren zatitzaileak ditu.

Frogapena:

Biz m konposatua $m = m_1 . m_2$ non $m_1 > 1$, $m_2 > 1$ baitira.

$$\left.\begin{array}{l} m_1 \not\equiv 0 \pmod{m} \\ m_2 \not\equiv 0 \pmod{m} \end{array}\right\} \Rightarrow \overline{m_1} \neq \overline{0} \neq \overline{m_2}$$

Baina, $\overline{m_1} . \overline{m_2} = \overline{m_1 . m_2} = \overline{m} = \overline{0} \rightarrow \overline{m_1}, \overline{m_2}$ Z_m multzoan zeroren zatitzaileak dira.

3. TEOREMA - p primua bada, Z_p multzoak ez du zeroaren zatitzailerik eta kasu honetan Z_p integritate erhaztuna da.

Frogapena

Bira $\overline{a}, \overline{b} \in Z$, non $\overline{a} \neq \overline{0} \neq \overline{b}$ baitira.

$\overline{a} \neq \overline{0}, \overline{b} \neq \overline{0} \rightarrow a \not\equiv 0 \pmod{p}, \quad b \not\equiv 0 \pmod{p} \rightarrow$

$\rightarrow p \not| a \wedge p \not| b \xrightarrow{p \text{ primua}} p \not| a.b \rightarrow$

$a b \not\equiv 0 \pmod{p} \rightarrow \overline{a b} \neq \overline{0} \rightarrow \overline{a}.\overline{b} \neq 0$

Beraz Z_p multzoak ez du zeroaren zatitzailerik.

HONDARREN SISTEMA OSOA

$Z_m = \{ \bar{0}, \bar{1}, \ldots, \overline{m-1} \}$ eraztunean, har dezagun klase bakoitzetik ordezkari bat: $x_0, \ldots, x_{m-1}$. $\{ x_0, \ldots, x_{m-1} \}$ multzoari m-moduluarekiko hondarren sistema osoa deitzen zaio. Klase bakoitzetik elementu bana hartu dugunez, $x_0, \ldots, x_{m-1}$ multzoaren elementu guztiak inkongruenteak izango dira. Klase bakoitzak elementuak kopuru infinituan ditu; beraz, hondarren sistema beteak kopuru infinituan har ditzakegu. Gehien erabiltzen direnak hauk dira:

a) Hondarren sistema bete minimo ez-negatiboa: sistema hau osatzeko, klase bakoitzetik ordezkari txikien ez-negatiboa hartzen da.

b) Hondarren sistema bete minimo absolutua: Klase bakoitzetik balio absolutuan txikiena den elementua ordezkaritzat hartuz osatzen da.

Adibidez: a) Z_m eraztunean: $\{0, 1, \ldots, m-1\}$

b) Z_m eraztunean: m delakoa bakoitia bada, ondoko sistema hau dugu: $\{ -\frac{m-1}{2}, \ldots, -1, 0, 1, \ldots, \frac{m-1}{2} \}$

Sistema honetan $2\,\frac{m-1}{2} + 1$ elementu daude

m delakoa bikoitia bada, ondoko sistema hauetariko bat dukegu:

$$\{ -\tfrac{m}{2} + 1, \ldots, -1, 0, 1, \ldots, \tfrac{m}{2} \}$$

edo

$$\{ -\tfrac{m}{2}, \ldots, -1, 0, 1, \ldots, \tfrac{m}{2} - 1 \}$$

Teorema. $(a, m) = 1$ bada, x-ek m moduluarekiko hondarren sistema bete baten baliok hartzen dituenean, orduan $b \in Z$, $ax + b$ forma linealak, m moduluarekiko hondarren sistema bete baten baliok hartzen ditu. Hondarren sistema osoa $\{ x_1, \ldots, x_m \}$ (1) izanik, forma linealaren balioak ondoko hauk dira:

$$\{ ax_1 + b, \ldots, ax_m + b \} \quad (2)$$

Frogapena:

Hipotesiz, $x_1, \ldots, x_m$ direlakoak bata bestearekiko inkongruentziak dira: $x_i \not\equiv x_j \pmod{m}$ $i \neq j$.

Dakusagun, (2) delako hondarren sistema betea dela. Hau frogatzeko, ikus dezagun, (2) sistemako elementuak binan-binan inkongruenteak direla. Absurdura eramanez, suposa dezagun (2) sistemako elementu bi kongruenteak direla, hau da, $\exists\, i,j \quad m \quad ax_i + b \equiv ax_j + b \pmod{m}$, halabeharrez $ax_i \equiv ax_j \pmod{m}$. Nola $(a, m) = 1$ den, orduan $x_i \equiv x_j \pmod{m}$ eta hau hipotesiaren aurka doa. Beraz, (2) sistemako elementuak bata bestearekiko inkongruenteak dira, eta honela, hondarren sistema bete bat osatzen dute.

HONDARREN SISTEMA LABURTUA

$Z_m = \{\bar{0}, \bar{1}, \ldots, \overline{m-1}\}$ eraztunean har dezagun klase bat $\bar{a}$.

Dakigunez, $a, b \in \bar{c} \rightarrow a \equiv b \pmod{m}$

Beste alde batetik, hauxe dugu: $a \equiv b \pmod{m} \rightarrow (a, m) = (b, m)$, orduan klase bateko elementu bat m-rekin primua bada, klase horretako elementu guztiak ere moduluarekin primuak izango dira.

Har ditzagun orain Z_m eraztunean m moduluarekiko primuak diren elementuen klaseak. Adibidez $\bar{1}, \overline{m-1}$.

Horretariko klase bakoitzetik ordezkari bat hartuz, $\{x_1, \ldots, x_{\varphi(m)}\}$ multzoa osatzen da, eta multzo honi hondarren sistema laburtua esaten zaio. Orain, $\varphi(m)$ zer den ikusiko dugu. $\varphi(m)$ zenbaki bat da, eta beraren elementu guztiak m-rekin primuak direneko klasean kopurua adierazten du.

Orain arte ikusitakoarekin, $\varphi(m)$ hondarrek, hondarren sistema laburtua osatzen dutela esan dezakegu, basta besteakiko inkongruen-

teak izanik:

$$x_i \not\equiv x_j \pmod{m} \quad \text{non} \quad (x_i , m) = 1$$

$\varphi(m)$ -ri, Euler-en funtzioa esaten zaio.

$\varphi(m)$ -ri, k zenbakien kopurua ere esaten zaio, non (k,m) = 1 eta k < m baitira.

Adibidez: $\varphi (2) = 1$

$\varphi (3) = 2$

$\varphi (8) = 4$

Definizioz: $\varphi (1) = 1$

EULER -EN FUNTZIOAREN PROPIETATE MULTIPLIKATIBOA

Teorema. Euler-en φ funtzioak ondoko propietate hoak betetzen ditu:

i) $\varphi (1) = 1$

ii) $(m,n) = 1 \rightarrow \varphi (m) \varphi (n) = \varphi (mn)$

Frogapéña:

i) definizioz betetzen da.

ii) Biz (m,n) = 1. Idatz dezagun, 1 eta mn artean dauden zenbaki guztiak

$$\begin{array}{c} 1, \quad 2, \ldots, \quad k, \quad \ldots, \quad m \\ m + 1, m + 2, \ldots, m + k, \ldots , 2m \\ 2m + 1, 2m + 2, \ldots, 2m + k, \ldots, 3m \\ \ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots \\ (n - 1)m + 1, (n - 1)m + 2, \ldots, (n-1)m + k, \ldots, nm \end{array}$$

nm-rekin primuak diren zenbakien kopurua, $\varphi(m\, n)$ da.

Lerro bakoitzak hondarren sistema bete bat adierazten du.

Lehenengo lerroan $\varphi(m)$ zenbaki ditugu m-rekin primuak izanik.

Bigarren lerroan .....

.....

n-garren lerroan .....

Suposa dezagun (k,m) = 1 dela eta har dezagun k zutabea. K zutabeko elementu guztiak m moduluarekiko kongruenteak dira. Hipotesiz, (k,m) = = 1 da; orduan, zutabe honetako elementu guztiak m-rekin primuak dira, eta beren elementuak m-rekin primuak dituztenak, denetara $\varphi(m)$ zutabe direla esan dezakegu.

Dakusugun, zutabe bakoitzak zenbat elementu dituen m-rekin primuak. Har dezagun k zutabea

$$k,\ m + k,\ \ldots,\ (n-1)m + k$$

Hauek ditugu: $\{mx + k\}$; $x = 0\ (1)m - 1$ $\quad (m,n) = 1$

$\{0, 1, \ldots, n-1\}$ multzoak m moduluarekiko hondarren sistema oso bat betetzen du. x-ek multzo horretako baloreak harturik, $\{mx + n\}$; $x = 0(1)n - 1$ hondarren sistema betea osatzen du.

Orduan, zutabe bakoitzak n-rekin primuak diren zenbakiak, $\varphi(n)$ kopuruan ditu.

Dakusagun, zenbat zenbakik betetzen duten ondoko baldintza:

$$(k,m) = (k,n) = 1$$

Zenbaki hauen kopurua, $\varphi(m).\ \varphi(n) = \varphi(mn)$ da.

Korolarioa

Biz $m = p_1^{\alpha_1} \ldots p_s^{\alpha_s}$ m -ren deskonposaketa kanonikoa; orduan

$$\varphi(m) = \prod_{i=1}^{s} \varphi(p_i^{\alpha_i}) \qquad (1) \text{ dateke.}$$

Frogapena: Induzioz egiten da.

Har dezagun p^{α}, p primua izanik. Eta orain, $\varphi(p^{\alpha})$ kalkulatu nahi dugu.

Har ditzagun 1 eta p^{α} artean dauden zenbakiak. Hauetariko zenbat dira p^{α}-rekin primuak? p^{α} -rekin primuak direnak, p -rekin ere primuak izango dira. Orduan, Zenbat multiplo ditu p-ek?

$$1,\ 2,\ \ldots,\ p,\ \ldots,\ 2p,\ \ldots,\ 3p,\ \ldots,\ p^{\alpha-1}\ p.$$

Ikusten dugunez p -ek, $p^{\alpha-1}$ multiplo ditu.

Lehengo galderari erantzuna emateko, 1 eta p^{α} artean

dauden zenbakien kopuruari, p-ren multiploen kopurua kendu behar zaio, eta geratzen dena $\varphi(p^{\alpha})$ da. Beraz, $\varphi(p^{\alpha}) = p^{\alpha} - p^{\alpha-1}$.

Korolarioa

p delako primua bada, $\varphi(p) = p - 1$ da

Beste formula bat agertzen zaigu, lehengo korolarioa kontutan harturik

$$\varphi(m) = \prod_{i=1}^{s} \varphi(p_i^{\alpha_i}) = \prod_{i=1}^{s} \left(p_i^{\alpha_i} - p_i^{\alpha_i-1}\right) = \prod_{i=1}^{s} p_i^{\alpha_i}(1 - 1/p_i) =$$

$$= m \prod_{i=1}^{s} (1 - 1/p_i)$$

$$\frac{\varphi(m)}{m} = \prod_{i=1}^{s} (1 - 1/p_i)$$

Adibidea: $\varphi(24) = \varphi(2^3 \cdot 3) = (2^3 - 2^2)(3 - 1) = 8$

1, 5, 7, 11, 13, 17, 19, 23.

Teorema. Biz $(a,m) = 1$. x-ek m moduluarekiko hondarren sistema laburtu baten balioak hartzen dituenean, orduan ax forma linealak m moduluarekiko hondarren sistema laburtu baten balioak hartzen ditu.

Hondarren sistema laburtua $\{x_1, \ldots, x_h\}$, $h = \varphi(m)$ izanik, forma linealaren balioak ondoko hauk dira: $\{ax_1, \ldots, ax_h\}$

Frogapena: i) $ax_i \not\equiv ax_j \pmod{m}$. Suposa dezagun, $ax_i \not\equiv ax_j \pmod{m}$ $\xrightarrow{(a,m)=1}$ $x_i \equiv x_j \pmod{m}$. $\{x_1, \ldots, x_h\}$ delakoa hondarren sistema laburtua izanik, lortuko ondorioa hipotesiaren aurka doa; orduan, $ax_i \not\equiv ax_j \pmod{m}$.

ii) Zenbat balio hartzen ditu ax forma linealak ? $h = \varphi(m)$

iii) $(ax_i, m) = 1 \quad i = 1(1)h$

$(ax_i, m) \xrightarrow{(a,m)=1} (x_i, m) = 1$

EULER -EN TEOREMA. Biz $m > 1$ modulo bat eta biz $(a,m) = 1$. Orduan,

$a^{\varphi(m)} \equiv 1 \pmod{m}$. (1)

Frogapena: Suposa dezagun $x = \xi_1, \ldots, \xi_h$ (2) hondarren sistema laburtu minimo ez-negatibo bat dela.

Aurreko teoremak diocnez,

$ax = a\xi_1, \ldots, a\xi_h$ (3) hondarren sistema laburtu

bat da.

Bira $r_1, \ldots\ldots r_k$ (4) beraren hondar minimo ez-negatiboak.

$$\left.\begin{array}{l} a x_1 \equiv r_1 \pmod{m} \\ \vdots \\ a x_k \equiv r_k \pmod{m} \end{array}\right\} \quad (5)$$

(2) eta (4) expresioetan zenbakiak berdinak dira

$$x_1 \ldots x_k = r_1 \ldots r_k \qquad (6)$$

(5) -sistemako kongruentziak biderkatuz, zera dugu:

$$a^k x_1 \ldots x_k \equiv r_1 \ldots r_k \pmod{m} \qquad (7)$$

Baina $(x_1 \ldots x_k, m) = 1$ dela kontutan harturik eta (7)-ren simplifikatuz, $a^k \equiv 1 \pmod{m}$ $\quad k = \varphi(m)$

$$a^{\varphi(m)} = 1 \pmod{m} \qquad \text{f.n.g.e.}$$

1. Korolarioa

(Fermat-en Teorema).- Biz p delakoa zenbaki primu bat eta a $\in \mathbb{Z}$ $(a,p) = 1$ Orduan $a^{p-1} \equiv 1 \pmod{p}$ dateke.

Frogapena: p primua bada, $\varphi(p) = p - 1$ dela dakigu eta Euler -en teorema kontutan harturik: $a^{\varphi(p)} \equiv a^{p-1} \equiv 1 \pmod{p}$

2. Korolarioa

Biz p primua. Ordùan: $a^p \equiv a \pmod{p}$ $\quad \forall a \in \mathbb{Z}$

Frogapena: i) $(a,p) = 1 \xrightarrow[F.T]{} a^{p-1} \equiv 1 \pmod{p} \longrightarrow a^p \equiv a \pmod{p}$

ii) $p \mid a \longrightarrow p \mid a^p \longrightarrow p \mid a^p - a \longrightarrow a^p \equiv a \pmod{p}$

3. Korolarioa

Biz p primua. Orduan

$$(h_1 + \ldots + h_n)^p \equiv h_1^p + \ldots + h_n^p \pmod{p} \quad \forall h_1 \ldots h_n \in \mathbb{Z}_+$$

Frogapena: Bigarren korolariotik, zera dugu:

$(h_1 + \ldots + h_n)^p \equiv h_1 + \ldots + h_n \pmod{p}$. Eta gainera

$$\left.\begin{array}{l} h_1^p \equiv h_1 \pmod{p} \\ \vdots \\ h_n^p \equiv h_n \pmod{p} \end{array}\right\}$$

Beraz $h_1^p + \ldots + h_n^p = h_1 + \ldots + h_n \pmod{p}$,

eta kongruentzien propietate transitiboa aplikatuz

$$(h_1 + \ldots + h_n)^p = h_1^p + \ldots + h_n^p \pmod{p} \text{ f.n.g.l.}$$

MODULUAREKIKO PRIMUAK DIREN HONDARREN TALDE MULTIPLIKATIBOA

Har dezagun $Z_m = \{\bar{0}, \bar{1}, \ldots, \overline{m-1}\}$ non $m > 0$ baita.

Dakigunez, $(Z_m, +, .)$ delakoa eraztun bat da.

Har dezagun orain $R_m = \{\bar{1}, \ldots, \overline{m-1}\}$ multzoa, non bere elementuak m moduluarekiko primuak baitira, hots:

$$\bar{a} \in R_m \longrightarrow (a,m) = 1$$

Teorema. R_m multzoa talde abeliar multiplikatiboa da.

Frogapena: i) Bira $\bar{a}, \bar{b} \in R_m \longrightarrow \overline{a\,b} \quad R_m$?

$\bar{a}\,\bar{b} = \overline{a\,b} \in R_m \leftrightarrow (ab, m) = 1$. Dakigunez, $(ab, m)_{(a,\overline{m})=\bar{1}}(b,m) = 1$

ii) $(\bar{a}\,\bar{b})\,\bar{c} = \bar{a}\,(\bar{b}\,\bar{c})$ $\forall \bar{a}, \bar{b}, \bar{c} \in R_m$, $b \in R_m$

iii) $\bar{1}\,\bar{a} = \bar{a}$ $\forall \bar{a} \in R_m$ eta $\bar{1} \in R_m$ ze $(1,m) = 1$

iv) $\exists\, \bar{a}^{-1} \in R_m$ non $\bar{a}\,\bar{a}^{-1} = \bar{1}$ $\forall \bar{a} \in R_m$

Suposa dezagun $\bar{a} \in R_m$ dela; beraz, $(a,m) = 1$. Euler -en teorema aplikatuz,

$$a^{\varphi(m)} \equiv 1 \pmod{m}$$

$$a \cdot a^{\varphi(m)-1} \equiv 1 \pmod{m}$$

$$\bar{a} \cdot \overline{a^{\varphi(m)-1}} = \bar{1} \longrightarrow \bar{a}^{-1} = \overline{a^{\varphi(m)-1}}$$

$$(a^{\varphi(m)-1}, m) = 1 \quad \text{ze} \quad (a,m) = 1$$

v) $\forall \bar{a}, \bar{b} \in R_m$ $\bar{a}\,\bar{b} = \bar{b}\,\bar{a}$, bistakoa da.

Teorema. Biz $m = p$ primua. Z_p gorputz abeliarra da.

Frogapena: i) Z_p eraztun trukakor unitarioa, zeroren zatitzailerik gabekoa da

ii) $R_p = \{\bar{1}, \ldots, \overline{p-1}\}$; $\varphi(p) = p - 1$, talde multiplikatiboa da.

Beraz Z_p gorputz abeliarra da f.n.g.l.

Teorema. (Gauss-en Formula)

$$\sum_{\delta \mid n} (\delta) = n \qquad \forall\ n > 1$$

Frogapena: Har dezagun $N = \{1, 2, \ldots, n\}$ multzoa.

N-ren elementuen kopurua, $|N| = n$ da.

$$N_d = \{ m \mid 1 \leq m \leq n \ \wedge\ (m,n) = d \} \quad (1)$$

adierazten dugu.

Bistakoa denez $\bigcup_{d \mid n} N_d = N$ (2) da.

$N_{d_1} \cap N_{d_2} = \phi$ kontutan harturik, eta $d_1 \neq d_2$ izanik, orduan,

$$|N| = \sum_{d \mid n} |N_d| \quad (3)$$

Dakusagun, N_d-ren balioa zein den.

Biz $m \in N_d \longrightarrow (m,n) = d \rightarrow \begin{matrix} m = m_1 d \\ n = n_1 d \end{matrix}$ eta $(m_1, n_1) = 1$ (4)

$$n_1 = \frac{n}{d} \quad \text{(finkoa da).}$$

N_d-ren elementu guztiak d-ren multiploak dira: $m = m_1 d$; orduan, N_d d, 2d, 3d, ... elementuek osotzen dute, eta esan dugunez, $(m_1, n_1) = 1$ da

Beraz, $N_d = \{ m_1 d \mid (m_1, n_1) = 1,\ 1 \leq m_1 \leq n_1 = n/d \}$.

Orduan, argi dagoenez, $|N_d| = \varphi(n_1)$ da.

Beraz, $|N_d| = \varphi(n_1) = \varphi\left(\frac{n}{d}\right)$ (6).

Eta (3)-formulatik, zera ateratzen dugu

$$n = \sum_{d \mid n} \varphi\left(\frac{n}{d}\right) \quad (7)$$

δ = n/d adieraziz eta d zenbakiaren zatitzaile bat dela kontutan harturik orduan, δ ere n-ren zatitzailea da. Eta (7) formula, ondoko eran gelditzen zaigu:

$$n = \sum_{\delta \mid n} \varphi(\delta) \quad (8) \quad \text{f.n.g.l.}$$

Adibidea: $n = 48 = 2^4 \cdot 3$

Zenbat zatitzaile ditugu ? $\tau(48) = 5.2 = 10$

Zeintzu dira 48-ren zatitzaileak ? Ondokoak, prezeski:

1, 2, 3, 4, 6, 8, 12, 16, 24, 48

Orain $\varphi(1), \varphi(2), \ldots\ldots\ldots, \varphi(48)$ kalkulatu behar ditugu.

$\varphi(1)= 1, \varphi(2)= 1, \varphi(3)= 2, \varphi(4)= 2, \varphi(5)= 2, \varphi(8)= 4, \varphi(12)= 4, \varphi(16)= 8,$

$\varphi(24)= 8, \varphi(48)= 16.$

Orduan $\varphi(1) + \varphi(2) + \ldots\ldots\ldots + \varphi(48) = 48 = n$ f.m.g.l.

LAURGARREN GAIA

INKOGNITA BATEKO KONGRUENTZIAK

- Oinharrizko ezegupenak.
- Lehen graduko kongruentziak.
- Lehen graduko kongruentzien sistemak.
- p modulu primu batekiko edozein graduko kongruentziak.
- Modulu konposatu batekiko edozein graduko kongruentziak.

IV. GAIA

INKOGNITA BATEKO KONGRUENTZIAK

1. Oinharrizko ezagupenak

Inkognita bateko kongruentziak aztertzerakoan, $f(x) \equiv 0 \pmod{m}$ (1) non $f(x) = a_0x^n + a_1x^{n-1} + \ldots\ldots + a_n$, $m > 0$ baitira erako kongruentzia algebraikoak kontsideratuko ditugu.

$a_0 \not\equiv 0 \pmod{m}$ bada, n zenbakiari kongruentziaren gradua deitzen zaio.

$a_0 \equiv 0 \pmod{m}$ bada, biz j, $a_j \not\equiv 0 \pmod{m}$ baldintza betetzen duen zenbaki oso positiborik txikiena, orduan kongruentziaren gradua n-j zenbakia dateke.

$f(x_0) \equiv 0 \pmod{m}$ bada, x_0 kongruentziaren soluzio bat da.

(1) kongruentzia betetzen duten x en balio guztiak aurkitzea, kongruentzia hori askatzea da.

x_0 (1) kongruentziaren **soluzio** bat bada, x_0 rekin m moduluarekiko kongruenteak diren x guztiak $\left[x \equiv x_0 \pmod{m}\right]$ (1) kongruentziaren **soluzioak** dira, eta zenbaki hauen klasea **soluziotzat** kontsideratzen da.

m modulu batekiko, hondarren ondoko m klase hauk existitzen dira: $\overline{0}, \overline{1}, \ldots\ldots, \overline{m-1}$. Beraz, (1) kongruentziak gehienez m soluzio onhartuko ditu.

Dakusagun adibide baten bidez, nola asketu ahal den (1) erako kongruentzia bat:

Biz $x^3 - 2x^2 + 3 \equiv 0 \pmod{5}$ kongruentzia. Kasu honetan $f(x) = x^3 - 2x^2 + 3$ Kongruentzia honen soluzio posible guztiak: 0, 1, 2, 3, 4 dira. Ikus dezagun hauetariko zeintzu diren benetako soluzioak:

$f(0) = 3 \not\equiv 0 \pmod{5}$ $\qquad$ $f(3) = 12 \not\equiv 0 \pmod{5}$

$f(1) = 2 \not\equiv 0 \pmod{5}$ $\qquad$ $f(4) = 35 \equiv 0 \pmod{5}$

$f(2) = 3 \not\equiv 0 \pmod{5}$

Beraz, kongruentzia honen **soluzio** bakarra $x \equiv 4 \pmod{5}$ da

m edo n zenbakiak handiak diren kasuetan metodo hau ez da erabilgarria, zeren eragiketa askoren beharra baitu, eta hemen datza kongruentzien askaketarako teoria orokor baten beharra.

2. Lehen graduko kongruentziak

$ax+b \equiv 0 \pmod m$ (2) erako kongruentziei, non $a,b \in Z$, $a \neq 0$, eta $m \nmid a$ baitira, lehen graduko kongruentziak deitzen zaie.

Azter dezagun kongruentzia hauen soluzioen kopurua.

1. Teorema

a) $(a,m) = 1$ bada, (2) kongruentziak soluzio bakarra du.

b) $(a,m) = d > 1$ bada, (2) kongruentziak m moduluarekiko soluziorik onhartzen du baldin eta soilik baldin d/b bada, eta kasu honetan kongruentzia honek m moduluarekiko d soluzio ditu.

Frogapena

a) x i m moduluarekiko hondar-sistema oso bat korrespondi erazten badiogu, $\{ax+b\}$ forma linealak m moduluarekiko hondar-sistema oso baten balioak hartzen ditu. Beraz, existitzen da x_0 bakar bat non $ax_0+b \equiv 0 \pmod m$ baita . x_0 hau (2) kongruentziaren soluzio bakarra izango da. Hau da:

$$x \equiv x_0 \pmod m \text{ (2) kongruentziaren soluzioa da.}$$

b) $(a,m) = d > 1$ da. Beraz $\begin{matrix} a = a_1 d \\ m = m_1 d \end{matrix}$ (*) non $(a_1, m_1) = 1$

$ax+b \equiv 0 \pmod m$ kongruentzia, $ax \equiv -b \pmod m$ moduan idatziz eta (*) kontsideratuz, (2) kongruentziak soluzioa badu, halabeharrez d/b izan beharko da.

Orain froga dezagun d/b bada, (2) kongruentziak soluzioa onhartzen duela.

d/b bada $\Rightarrow b = b_1 d$.

Orduan (2) ondoko eran idatz daiteke:

$a_1 dx + b_1 d \equiv 0 \pmod{m_1 d} \iff a_1 x + b_1 \equiv 0 \pmod{m_1}$ (3)

(2) eta (3) kongruentziak baliokideak dira, zeren soluzio berdinak baitituzte.

c) kasua kontsideratuz, (3) kongruentziak m_1 moduluarekiko soluzio bakarra du. Biz soluzio hori $x \equiv x_0 \pmod{m_1}$, (2) eta (3) kongruentziak baliokideak direnez, (2) kongruentziaren soluzioak berdinak dira; baina (3) kongruentziaren soluzioak m moduluarekiko eran idatzi behar dira.

(3) kongruentziaren soluzioak ondoko hauk dira, $x = x_0 + m_1 t$, $t \in Z$:

$$\ldots\ldots, -[x_0 + (d-1)m_1], \ldots\ldots, x_0, x_0 + m_1, x_0 + 2m_1, \ldots\ldots, x_0 + (d-1)\, m_1, \ldots\ldots$$

Orain soluzio hauen artean zenbat diren m moduluarekiko inkongruenteak ikusi behar da.

$t = 0, 1, \ldots, d-1$ denean, zenbaki horik m moduluarekiko inkongruenteak

dira, zeren $0 \leq \ell < k \leq d-\ell$ denean $x_0 + km_1 \equiv x_0 + \ell m_1 \pmod{m}$ balitz, $(k-\ell)\, m_1 \equiv 0 \pmod{m}$ izango litzateke eta hau absurdua da zeren $(k-\ell)\, m_1 < m$ baita.

Honelatan ba, $x \equiv x_0 + m_1 t \pmod{m}$ $t = 0, 1, \ldots, d-1$ (2) kongruentziak dituen d soluzioak dira.

<u>$a \cdot x \equiv b \pmod{m}$ (2) kongruentziaren askaketa</u>

Aurreko teoremaren bidez badakigu (2) kongruentziaren soluzioen kopurua zein den. Dakusagun orain kongruentzia hori askatzeko bide bat. Hemen ikusiko dugun bidean Euler-en teoremaz baliatuko gara.

Kontsidera dezagun (2) kongruentzia non $(a,m) = 1$ baita.

$(a,m) = 1$ izanik, a m moduluarekiko hondar-sistema osoaren elementu bat da, beraz existizen da $a' \in \mathbb{Z}$ non $a \cdot a' \equiv 1 \pmod{m}$ baita.

Orduan $\left.\begin{array}{l} a \cdot a' \cdot x \equiv a' b \pmod{m} \\ a \cdot a' \equiv 1 \pmod{m} \end{array}\right\} \Rightarrow x \equiv a' b \pmod{m}$

Hau da, (2) kongruentzia askatzeko aski da a' hori aurkitzea. a' hori aurkitzeko Euler-en teorema erabiliko dugu: teorema horren bidez $a^{\varphi(m)} \equiv 1 \pmod{m} \Rightarrow a^{\varphi(m)-1} \cdot a \equiv 1 \pmod{m} \Rightarrow a' \equiv a^{\varphi(m)-1} \pmod{m}$.

<u>Eredua</u>

Aska dezagun $41 \cdot x \equiv 31 \pmod{51}$ kongruentzia.

$(41,51) = 1$

Orduan: $x \equiv 41' \cdot 31 \pmod{51}$

$41' \equiv 41^{\varphi(51)-1} \pmod{51}$

$\varphi(51) = \varphi(17 \cdot 3) = \varphi(17)\,\varphi(3) = 16 \cdot 2 = 32$

$41' \equiv 41^{31} \pmod{51}$

$41 \equiv -10 \pmod{51} \Rightarrow 41' \equiv (-10)^{31} \pmod{51}$

$10^{31} \equiv -5 \pmod{51} \Rightarrow 41' \equiv +5 \pmod{51}$. Beraz:

$x \equiv 155 \pmod{51} \Rightarrow x \equiv 2 \pmod{51}$ da kongruentziaren soluzioa .

Dakusagun orain (2) kongruentziaren askaketaren kasu berezi bat, hau da: $m = p$ zenbaki primu bat deneko kasua.

<u>1. Proposizioa</u>

Biz $k \cdot x \equiv b \pmod{p}$ kongruentzia, non $p \nmid k$ baita. Kongruentzia honen soluzioa ondoko hau da:

$$x \equiv (-1)^{k-1} \frac{1}{p} b \binom{p}{k} \pmod{p}$$

Frogapena

Biz $x_o = (-1)^{k-1} \frac{1}{p} b\binom{p}{k}$

Ordezkatuz: $x_o = (-1)^{k-1} \frac{p\,(p-1)\,(p-2)\ldots\ldots(p-k+1)}{p\,k!} \cdot b \Rightarrow$

$$\Rightarrow k! x_o = (-1)^{k-1} \frac{(p-1)(p-2)\ldots\ldots(p-k+1)}{(k-1)!} b \equiv$$

$$\equiv (-1)^{k-1} \frac{(-1)(-2)\ldots\ldots(k-1)}{(k-1)!} \cdot b \equiv b \pmod{p} \Rightarrow$$

$\Rightarrow x_o$ k x $\equiv b \pmod{p}$ kongruentziaren soluzio bat da

3. Lehen graduko kongruentzien sistemak

a) Kontsidera dezagun lehen graduko kongruentzien ondoko sistema hau:

$$(1) \begin{cases} a_1 x \equiv b_1 \pmod{m_1} \\ \ldots\ldots\ldots\ldots \\ a_s x \equiv b_s \pmod{m_s} \end{cases}$$

Kongruentzia guzti hauk betetzen duen zenbaki bat sistema honen soluzio bat da.

Lehengo eta behin kongruentzia hauk banan-banan eskatzen dira, gero guztiei dagozkien soluzioak kontsideratuz.

Sistema honen kongruentzieren batek soluziorik ez badu, sistema hau ez-baterakoia dela esaten da.

(1) sistemaren kongruentzia guztiak soluzio bakarra dutenean, (1) sistema eta ondoko sistema hau baliokideak dira:

$$(2) \begin{cases} x \equiv x_1 \pmod{m_1} \\ \ldots\ldots\ldots\ldots \\ x \equiv x_s \pmod{m_s} \end{cases}$$

non $x \equiv x_i \pmod{m_i}$ $i = 1,\ldots,s$, $a_i x \equiv b_i \pmod{m_i}$ kongruentziaren soluzioa baita.

(1) sistemaren kongruentzia batek, lehenengoa adibidez, d_1 soluzio onhartzen baditu, (1) sistema ondoko kongruentzien d sistemekin baliokidea da:

$$\begin{cases} x \equiv x_{11} \pmod{m_1} \\ x \equiv x_2 \pmod{m_2} \\ \cdots\cdots\cdots\cdots \\ x \equiv x_s \pmod{m_s} \end{cases} \quad \cdots\cdots\cdots\cdots\cdots \quad \begin{cases} x \equiv x_{1d_1} \pmod{m_1} \\ x \equiv x_2 \pmod{m_2} \\ \cdots\cdots\cdots\cdots\cdots \\ x \equiv x_s \pmod{m_s} \end{cases}$$

$x_{11}, x_{12}, \ldots\ldots, x_{1d_1}$ $a_1 x \equiv b_1 \pmod{m_1}$ kongruentziaren d_1 soluzioak izanik.

Modu berean (1) sistemaren kongruentzia bakoitzak $a \cdot x_i \equiv b_i \pmod{m_i}$ d_i soluzio onhartzen dituenean, (2) sistema kongruentzien $d_1 \ldots\ldots d_s$ sistemekin baliokidea da. Honela izanik, (2) eratako sistemak nola askatzen diren ikusiko dugu.

b) Modulu guztiak binan binan primuak dituzten sistemeei buruz teorema hau dugu:

2. Teorema (Hondarren txinatar teorema)

Demagun (2) kongruentzien sistema bat, eta suposa dezagun $(m_i, m_j) = 1$ $\forall i \neq j$ dela.

Biz $m = m_1 \ldots\ldots m_s = m_1 M_1 = \ldots\ldots = m_s M_s$

Bira M_i' m_i moduluarekiko M_i ren inbertsoak, hau da:

$M_i \cdot M_i' \equiv 1 \pmod{m_i}$ $i = 1, \ldots, s$

Orduan (2) sistemaren soluzio bakarra $x \equiv x_o \pmod{m}$ kongruentziaren bidez emanda, non $x_o = M_1 M_1' x_1 + \ldots\ldots\ldots + M_s M_s' x_s$ baita

x_o (2) sistemaren soluzio orokorra dela esan ohi da.

Frogapena

M_i' zenbakiak existitzen dira, zeren $\forall i = 1, \ldots, s$ $(m_i, M_i) = 1$, eta $\forall i \neq j$ m_i / M_j baitira.

Suposatuz (2) sistema eta $x \equiv x_o \pmod{m}$ kongruentzia baliokideak direla, hau da soluzio berdinak dituztela.

m_i moduluarekiko zera dugu:

$$x_o = M_1 M_1' x_1 + \ldots\ldots\ldots + M_s M_s' x_s \equiv M_i M_i' x_i \equiv x_i \pmod{m_i}$$

$$\uparrow \quad \forall i \neq j \; m_i / M_j$$

Beraz (2) sistemaren kongruentzia bakoitza $x \equiv x_o \pmod{m_i}$ kongruentziarekin ordezkatu ahal da.

Honela ba, (2) sistema eta $x \equiv x_o \pmod{m_i}$ $i = 1, \ldots, s$ (3) sistema baliokideak dira.

Baina (3) sistema eta $x \equiv x_o \pmod m$ kongruentzia baliokideak dira.

Beraz $x \equiv x_o \pmod m$ (2) sistemaren soluzio bakarra da.

Eredua

Aska dezagun ondoko sistema hau:

$$\begin{cases} x \equiv 1 \pmod 4 \\ x \equiv 3 \pmod 5 \\ x \equiv 2 \pmod 7 \end{cases}$$

Aurreko teorema erabiliz, zera dugu:

$(4,5) = (5,7) = (4,7) = 1$

$m_1 = 4,\ m_2 = 5,\ m_3 = 7$

$m = 4 \cdot 5 \cdot 7 = 140$

$M_1 = 5 \cdot 7 = 35,\quad M_2 = 4 \cdot 7 = 28,\quad M_3 = 4 \cdot 5 = 20$

Bila dezagun M_1', M_2', M_3' .

$35\ M_1' \equiv 1 \pmod 4 \Rightarrow M_1' \equiv 3 \pmod 4$

$28\ M_2' \equiv 1 \pmod 5 \Rightarrow M_2' \equiv 2 \pmod 5$

$20\ M_3' \equiv 1 \pmod 7 \Rightarrow M_3' \equiv 6 \pmod 7$

Beraz emandako sistemaren soluzio orokorra ondoko hau da:

$x_o \equiv 35 \cdot 3\ x_1 + 28 \cdot 2\ x_2 + 20 \cdot 6\ x_3 \pmod{140} \Rightarrow$

$\Rightarrow x_o \equiv 35 \cdot 3 \cdot 1 + 28 \cdot 2 \cdot 3 + 20 \cdot 6 \cdot 2 \pmod{140} \Rightarrow$

$\Rightarrow x_o \equiv 105 + 168 + 240 \equiv 513 \pmod{140} \Rightarrow$

$\Rightarrow x_o \equiv 93 \pmod{140}$

c) Modulu guztiak binan binan primuak ez dituzten kongruentzien sistemak.

Kontsidera dezagun $\begin{cases} x \equiv x_1 \pmod{m_1} \\ \cdots\cdots\cdots\cdots \\ x \equiv x_s \pmod{m_s} \end{cases}$

kongruentzien sistema non moduluak ez baitira binan binan primuak, hau da: $(m_i, m_j) = d_{ij} \geq 1$.

Biz $M = [m_1, \ldots\ldots, m_s] = p_1^{\alpha_1} \ldots\ldots p_s^{\alpha_s}$ M ren faktore primuetango deskonposaketa.

Azter dezagun (1) sistemaren askaketa.

3. Teorema

(1) sistemak soluzioa du baldin eta soilik baldin $x_i \equiv x_j \pmod{d_{ij}}$ $\forall\ i = 1, \ldots, s$ kongruentziak betetzen badira.

Baldintza hauk betetzen direnean (1) sistemaren **soluzio** bakarra $x \equiv x_o \pmod{M}$ kongruentziaren bidez ematen da non $M = [m_1, \ldots, m_s]$ eta x_o (1) sistemaren soluzio arbitrario bat baitira.

Frogapena

Suposa dezagun (1) sistemak soluzioa onhartzen duela eta biz x_o soluzio bat. Orduan, zera betetzen da:

$$\begin{cases} x_o \equiv x_1 \pmod{m_1} \\ \ldots\ldots\ldots\ldots \\ x_o \equiv x_s \pmod{m_s} \end{cases}$$

Hau da: $\begin{cases} x \equiv x_i \pmod{m_i} \\ x \equiv x_j \pmod{m_j} \end{cases}$ $\forall\, i \neq j$

eta nola d_{ij}/m_i d_{ij}/m_j den, $x_i \equiv x_j \pmod{d_{ij}}$ dukegu.

Honela beharrezko baldintza frogatua dugu.

Dakusagun orain nahiko den baldintza:

Suposa dezagun $x_i \equiv x_j \pmod{d_{ij}}$ $\forall i = 1, \ldots, s$ dela.

$x \equiv x' \pmod{m}$ non $m = q_1^{\beta_1} \ldots\ldots q_k^{\beta_k}$ baita kongruentzia emanik, ondoko kongruentzia sistema deskonposatzen da:

$$\begin{cases} x \equiv x' \pmod{q_1^{\beta_1}} \\ \ldots\ldots\ldots\ldots \\ x \equiv x' \pmod{q_k^{\beta_k}} \end{cases}$$

(1) sistemaren kongruentzia bakoitza kongruentzia primarioetako sistema batez ordezkatuko dugu. Orduan beti existituko dira $\begin{cases} x \equiv x_i \pmod{p^{\alpha}} \\ x \equiv x_j \pmod{p^{\beta}} \end{cases}$ (2)

moetako kongruentzia bi non $i \neq j$, $\beta \leq \alpha$, $d_{ij} > 1$ baitira.

Bira p/m_i, eta p/m_j; suposa dezagun $\beta \leq \alpha$ dela.

(2) sistemaren bigarren kongruentzia gainezkoa dela frogatuko dugu.

Hipotesis $x_i \equiv x_j \pmod{d_{ij}}$ kongruentzia betetzen da.

p^{β}/d_{ij}, zeren p^{α}/m_i baita eta orduan: $p^{\beta}/m_j \underset{\beta \leq \alpha}{\Rightarrow} p^{\beta}/m_i$

Beraz, $x_i \equiv x_j \pmod{p^{\beta}}$.

Honelatan ba (2) kongruentzien sistema eta $\begin{cases} x \equiv x_i \pmod{p^{\alpha}} \\ x \equiv x_j \pmod{p^{\beta}} \end{cases}$ (3)

sistema baliokideak dira.

Gainera (3) sistema eta $x \equiv x_i \pmod{p^{\alpha}}$ kongruentzia ere baliokideak dira.

Beraz, (2) sistemaren bigarren kongruentzia gainezkoa da.

Beraz (1) sistema eta $\begin{cases} x \equiv x_{i1} \ (p_1^{\alpha_1} \text{ mod}) \\ \dots\dots\dots\dots\dots \\ x \equiv x_{in} \ (p_n^{\alpha_n} \text{ mod}) \end{cases}$ (4)

sistema baliokideak dira non $x_{i1},\dots,x_{in} \in \{x_1,\dots,x_s\}$ baita eta x_{ik} $k = 1,\dots,n$ hauetariko batzu berdinak izan daitezke.

(4) sistemaren modulu guztiak binan binan primuak dira, beraz aurreko teorema kontsideratuz $x \equiv x_0$ (M mod) (1) sistemaren soluzio bat da.

Eredua

Aska dezagun $\begin{cases} x \equiv 7 \ (15 \text{ mod}) \\ x \equiv 2 \ (35 \text{ mod}) \\ x \equiv 16 \ (63 \text{ mod}) \end{cases}$ kongruentzien sistema.

Kasu honetan:

$d_{12} = (15,35) = 5$, $d_{13} = (15,63) = 3$, $d_{23} = (35,63) = 7$

eta:

$7 \equiv 2 \ (5 \text{ mod})$, $7 \equiv 16 \ (3 \text{ mod})$, $2 \equiv 16 \ (7 \text{ mod})$.

Honela aurreko teoremaren baldintzak betetzen dira, eta emandako sistemak soluzioa du.

Deskonposa dezagun kongruentzia bakoitza kongruentzia primarioetako sistema batetan:

$x \equiv 7 \ (3 \text{ mod})$ $\quad x \equiv 2 \ (5 \text{ mod})$ $\quad x \equiv 16 \ (7 \text{ mod})$

$x \equiv 7 \ (5 \text{ mod})$ $\quad x \equiv 2 \ (7 \text{ mod})$ $\quad x \equiv 16 \ (3^2 \text{ mod})$

Teoreman egiten den arabera, gainezko kongruentziak kenduz sistema hau gelditzen da: $\begin{cases} x \equiv 2 \ (5 \text{ mod}) \\ x \equiv 2 \ (7 \text{ mod}) \\ x \equiv 16 \ (3^2 \text{ mod}) \end{cases}$

eta sistema honetan moduluak binan binan primuak dira.

Orain sistema hau aurreko ereduaren sistema bezalakoa da, eta askatzeko bertan erabili den metodoa erabili behar da.

4. p modulu primu batekiko edozein graduko kongruentziak

Sail honetan $p > 2$ dela suposatuko dugu, zeren $p = 2$ kasua aztertzea berehalakoa baita.

Hemen $f(x) \equiv 0 \ (p \text{ mod})$ (1) erako kongruentziak, non $a_i \in Z$, $a_0 \not\equiv 0 \ (p\text{mod})$, p primu eta $f(x) = a_0x^n + a_1x^{n-1} + \dots\dots + a_n$ baitira, aztergai izango dira. Eta modulu primu batekiko kongruentzia algebraikoak deitzen dira.

Era honetako kongruentziei buruz ondoko teorema batzu ikus daitezke.

4. Teorema

(1) erako kongruentzia bat, gradua hertsiki p baino txikiago duen kongruentzia algebraiko batekin baliokidea da.

Frogapena

(1) kongruentziaren gradua n, p baino txikiagoa balitz frogatuta legoke. Suposa dezagun $n \geq p$ dela.

$f(x)$ polinomioa $x^p - x$ gaiaz zatituz zera dugu:

$$f(x) = (x^p - x)\cdot Q(x) + R(x) \quad \text{non grad } R(x) < p \text{ baita.}$$

Orduan (1) kongruentzia honela idatz dezakegu:

$$(x^p - x)\cdot Q(x) + R(x) \equiv 0 \pmod{p}$$

Fermat-en teoremak $x^p \equiv x \pmod{p}$ dela esaten du, beraz $x^p - x \equiv 0 \pmod{p}$ eta honela: $R(x) \equiv 0 \pmod{p}$ eta (1) kongruentzia baliokideak dira grad $R(x) < p$ izanik.

Oharrak

a) p modulu primu batekiko kongruentzia algebraiko bat askatu behar denean, koefiziente bakoitza hondar mimimo absolutuaz edo hondar minimo ez negatiboaz ordezkatzea oso komenigarria izaten da.

b) Kongruentziaren gradua guttitzeko, halaber 4. teorema momomio bakoitzean aplikatzea ere komenigarria da. Adibidez:

Biz $f(x) \equiv x^s$, $s \geq p$ izanik.

$$x^s = x^{s-p}\cdot(x^p - x) + x^{s-p+1} \equiv x^{s-(p-1)} \pmod{p}$$
$$x^p - x \equiv 0 \pmod{p}$$

$s-(p-1) \geq p$ bada, berdintsu egiten da berriz ere.

Suposa dezagun $s = k(p-1) + r$, $0 \leq r < p-1$ dela. Kasu honetan,

$$x^s = x^{s-(p-1)} \equiv x^{s-2(p-1)} \equiv \ldots\ldots \equiv x^{s-k(p-1)} \equiv x^r \pmod{p}$$

Hau da: $s \equiv r \pmod{p-1}$ bada, $x^s \equiv x^r \pmod{p}$ dateke.

Eredua

Dakusagun $87\cdot x^{31} + 24\, x^{26} - 10\, x^8 + 3\, x - 1 \equiv 0 \pmod{7}$ kongruentzia. Hemen $p = 7$ da.

$87 \equiv 3 \pmod{7}$, $24 \equiv 3 \pmod{7}$, $-10 \equiv -3 \pmod{7}$

Orduan, emandako kongruentzia eta ondokoa baliokideak dira:

$$3\cdot x^{31} + 3\, x^{25} - 3\, x^8 + 3\, x - 1 \equiv 0 \pmod{7}$$

$31 \equiv 1 \pmod{6}$, $25 \equiv 1 \pmod{6}$, $8 \equiv 2 \pmod{6}$.

Beraz emandako kongruentzia eta ondokoa baliokideak dira:

$$3x+3x-3\cdot x^2+3x-1 \equiv 0 \pmod 7 \iff$$

$$\iff -3x^2+9x-1 \equiv 0 \pmod 7 \iff$$

$$\iff -3x^2+2x-1 \equiv 0 \pmod 7$$

Kongruentzia honek ez du soluziorik, zeren ez baita betetzen 0, ± 1, ± 2, ± 3 x en balioentzat. Beraz, emandako kongruentziak ere ez du soluziorik.

5. Teorema

$$(1) \quad f(x) = a_n x^n + a_{n-1}x^{n-1} + \ldots\ldots + a_0 \equiv 0 \pmod p$$

(1) kongruentziak n soluzio baino gehiago baditu, orduan f(x)-en koefiziente guztiak p ren multiploak direteke.

Frogapena

Eman dezagun (1) kongruentziak $x_0,\ldots\ldots,x_n$ n+1 soluzio dituela, hau da $f(x_k) \equiv 0 \pmod p$, $k = 0,\ldots\ldots,n$ eta $x_i \not\equiv x_j \pmod p$ $\forall i \neq j$ dira.

Idatz dezagun f(x) Newton-en formularen bidez, hau da:

$$\begin{aligned} f(x) &= a_n x^n + a_{n-1}x^{n-1} + \ldots\ldots\ldots + a_0 = \\ &= b_n\cdot(x-x_0)\cdot(x-x_1)\ldots\ldots\ldots(x-x_{n-1}) + \\ &+ b_{n-1}\cdot(x-x_0)\ldots\ldots\ldots\ldots(x-x_{n-2}) + \\ &+ \ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots + \\ &+ b_1\cdot(x-x_0) + b_0 \end{aligned}$$

non

$$(2) \quad \begin{cases} a_n = b_n \\ a_{n-1} = b_{n-1} + \dot{b}_n \\ a_{n-2} = b_{n-2} + \dot{b}_{n-1} + \dot{b}_n \\ \ldots\ldots\ldots\ldots\ldots\ldots \\ a_0 = b_0 + \dot{b}_1 + \ldots\ldots\ldots + \dot{b}_n \end{cases} \quad \text{baitira.}$$

Beraz:

$$f(x_0) \equiv b_0 \equiv 0 \pmod p$$

$$f(x_1) \equiv b_1(x_1-x_0) \equiv 0 \pmod p \Rightarrow b_1 \equiv 0 \pmod p \quad \text{zeren } p \not| x_1-x_0$$

$$f(x_2) \equiv b_2(x_2-x_0)\cdot(x_2-x_1) \equiv 0 \pmod p \Rightarrow$$

$$\Rightarrow b_2 \equiv 0 \pmod p \quad \text{zeren } p \not| x_2-x_0 \text{ eta } p \not| x_2-x_1$$

$$\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots$$

$$f(x_n) = b_n\cdot(x_n-x_0)\ldots\ldots\ldots(x_n-x_{n-1}) \equiv 0 \pmod p \Rightarrow$$

$$\Rightarrow b_n \equiv 0 \pmod p$$

Honelatan ba, b_i guztiak p ren multiploak dira eta (2) erlazioak kontsideratuz, a_i f(x) en koefiziente guztiak ere p ren multiploak dira.

1. Korolarioa (Lagrage-ren teorema)

$a_n x^n + a_{n-1} x^{n-1} + \ldots\ldots + a_0 \equiv 0 \pmod{p}$ non p primu eta $n \geq 1$ baita, n graduko kongruentzia algebraiko bat, p moduluarekiko n soluzio desberdin gehienez onhartzen ditu.

Frogapena

Absurdura eramanez eta 5. teorema erabiliz, berez dario.

2. Korolarioa (Wilson-en teorema)

p zenbaki primu guztientzat ondoko kongruentzia hau betetzen da:

$$(p-1)! + 1 \equiv 0 \pmod{p}$$

Frogapena

p = 2 kasurako teorema berehalakoa da.

Froga dezagun p > 2 den kasurako:

Kontsidera dezagun $(x-1)\cdot(x-2),\ldots\ldots(x-p+1) - (x^{p-1} - 1) \equiv 0 \pmod{p}$ (3) kongruentzia. Kongruentzia honen gradua p-2 da.

Fermat-en teoremaren bidez $x^{p-1} \equiv 1 \pmod{p}$ $x = 1,2,\ldots\ldots,p-1$ kongruentziak ditugu. Beraz $x = 1,2,\ldots,p-1$ zenbakiak (3) kongruentziaren p-1 soluzio desberdinak dira, eta 5. teoremaren bidez kongruentzia honen koefiziente guztiak p ren multiploak dira. Bereziki gai independentea ere p ren multiploa izango da. Hau da:

$(-1)^{p-1} \cdot 1\cdot 2 \ldots\ldots (p-1) + 1 \equiv 0 \pmod{p} \xrightarrow[\text{p bakoitia}]{}$

$\Longrightarrow 1\cdot 2 \ldots\ldots (p-1) + 1 \equiv 0 \pmod{p}$

$\Longrightarrow (p-1)! + 1 \equiv 0 \pmod{p}$

Eredua

p = 7 primua da. Beraz, kongruentzia hau dugu:

$$6! + 1 \equiv 0 \pmod{7} \iff 721 \equiv 0 \pmod{7}$$

Oharra

Dakusegun p zenbaki konposatua bada, ez dela horregatik betetzen Wilson-en teorema:

p konposatua izanik, p ren zatitzaile primu minimo bat q existitzen da.

Hau da: q/p eta $1 < q < p$.

$q/p \Rightarrow q/(p-1)!$ eta Wilson-en teorema beteko balitz halabeharrez q/1 eta hau absurdua da.

Honela ba, Wilson-en teorema zenbaki primuen karakterizapen bat dela

kontsidera dezakegu.

5. Modulu konposatu batekiko edozein graduko kongruentziak

Biz $f(x) \equiv 0 \pmod m$ (1), non $f(x) = a_n x^n + \ldots\ldots\ldots + a_0$, $a_i \in Z$, eta m zenbaki konposatu bat baitira. Kongruentzia hau m modulu konposatu batekiko n graduko kongruentzia algebraikoa deitzen da.

6. Teorema

a) $m = [m_1, \ldots\ldots, m_s]$ bada, orduan $f(x) \equiv 0 \pmod m$ kongruentzia,

$$(2)\quad \begin{cases} f(x) \equiv 0 \pmod{m_1} \\ \ldots\ldots\ldots\ldots\ldots \\ f(x) \equiv 0 \pmod{m_s} \end{cases}$$

kongruentzien sistemarekin baliokidea dateke.

b) $(m_i, m_j) = 1$ bada, ($m = m_1 \ldots\ldots m_s$) eta $T_1, \ldots\ldots, T_s$ zenbakiek (2) sistemaren kongruentzia bakoitzeko soluzioen kopurua adierazten badute, orduan $T = T_1 \ldots\ldots T_s$ zenbakiak (1) kongruentziaren soluzioen kopurua adierazten du.

Frogapena

a) (1) kongruentzia betetzen bada $f(x)$ m ren multiplo bat dateke, beraz $m_1, \ldots\ldots, m_s$ zenbakien multiploa ere zeren $m = [m_1, \ldots\ldots, m_s]$ baita, eta honela (2) kongruentzien sistema betetzen da.

Alderantzizko errazonamendua ere berdintsua da.

b) Bira $x_{11}, \ldots\ldots, x_{1T_1}$

$\ldots\ldots\ldots\ldots$

$x_{s1}, \ldots\ldots, x_{sT_s}$ zenbakiak

$f(x) \equiv 0 \pmod{m_1}$

$\ldots\ldots\ldots\ldots\ldots\ldots$

$f(x) \equiv 0 \pmod{m_s}$ kongruentzien soluzioak errespektiboki.

$(m_i, m_j) = 1$ denez, (2) sistemaren soluzio bakarra

$$x \equiv x_0 = M_1 M_1' x_1 + \ldots\ldots\ldots + M_s M_s' x_s \pmod m$$

izango da, non x_i $f(x) \equiv 0 \pmod{m_i}$ $i = 1, \ldots\ldots, s$ kongruentziaren soluzio bat baita.

Beraz (1) kongruentziaren soluzio guztiek x_i bakoitzari $x_{i1}, \ldots\ldots, x_{iT_i}$ T_i balio guztiek korrespodi eraziz lortzen dira.

Honelaten ba, (1) kongruentziaren soluzioen kopurua $T = T_1 \ldots\ldots T_s$ izango da.

Ondorioa

$f(x) \equiv 0 \pmod m$ erako kongruentziak non $m = p_1^{\alpha_1} \cdot \ldots \cdot p_s^{\alpha_s}$ baita eta

$$\begin{cases} f(x) \equiv 0 \pmod{p_1^{\alpha_1}} \\ \ldots\ldots\ldots \quad \ldots\ldots\ldots \\ f(x) \equiv 0 \pmod{p_s^{\alpha_s}} \end{cases}$$

kongruentzien sistema baliokideak dira.

$\forall i = 1, \ldots, s$ $f(x) \equiv 0 \pmod{p_i^{\alpha_i}}$ kongruentziaren soluzioen kopurua T_i bada, $f(x) \equiv 0 \pmod m$ kongruentziaren soluzioen kopurua $T = \prod_{i=1}^{s} T_i$ dateke.

Modulu primario batekiko kongruentzien askapena

Azter ditzagun hemen, (1) $f(x) \equiv 0 \pmod{p^\alpha}$ erako kongruentziak, non p primua baita.

Suposa dezagun (1) kongruentziak soluzioren bat onhartzen duela eta biz x_0 horietariko soluzio bat, hau da $f(x_0) \equiv 0 \pmod{p^\alpha}$

Orduan zera ikusten da: $f(x) \equiv 0 \pmod{p^\alpha}$ kongruentziaren edozein soluzio, $f(x) \equiv 0 \pmod p$ kongruentziaren soluzio bat da.

Honela izanik (1) kongruentziaren soluzioak aurkitzeko, ondoko pausu hauk segitzen dira:

1) $f(x) \equiv 0 \pmod p$ kongruentziaren soluzioak aurkitzen dira.
2) $f(x) \equiv 0 \pmod p$ kongruentziaren soluzioen artean, $f(x) \equiv 0 \pmod{p^2}$ kongruentziaren soluzioak aukeratzen dira .

Prozesu hau bukatzerakoan (1) kongruentziaren soluzio guztiak edukiko dituzu .

7. Teorema

Biz x_0, $f(x) \equiv 0 \pmod{p^{\alpha-1}}$ kongruentziaren soluzio bat non $\alpha > 1$ eta p primua baitira.

$f'(x_0) \not\equiv 0 \pmod p$ bada, orduan $x \equiv x_0 \pmod{p^{\alpha-1}}$ hondar klasean $f(x) \equiv 0 \pmod{p^\alpha}$ kongruentziaren soluzio bakar bat existitzen da.

Frogapena

Teorema honen frogapena hasi aurretik, ohar gaitezen $p^{\alpha-1}$ moduluarekiko hondar klase batetan p klase exaktuki daudela.

Eman dezagun teoremaren hipotesiak betetzen direla eta kontsidera dezagun $x \equiv x_0 \pmod{p^{\alpha-1}}$ klasearen elementuak: $x = x_0 + p^{\alpha-1} t$, $t \in Z$.

Zenbaki hauk $f(x) \equiv 0 \pmod{p^\alpha}$ kongruentziaren soluzioak dira. Dakusagun t ren zeintuz baliorentzat betetzen den, ondoko kongruentzia hau:

$f(x_0 + p^{\alpha-1}t) \equiv 0 \ (p^\alpha \text{ mod})$.

f n graduko polinomio bat bada, polinomio hau Taylor-en bidez x_0 puntuan t rekiko berreduretan bilakatuz zera dugu:

$$f(x_0) + \frac{f'(x_0)}{1!} p^{\alpha-1} t + \frac{f''(x_0)}{2!} \cdot p^{2(\alpha-1)} t^2 + \ldots\ldots + \frac{f^{n)}(x_0)}{n!} \cdot p^{n(\alpha-1)} t^n \equiv$$

$$\equiv 0 \ (p^\alpha \text{ mod}) \qquad (3)$$

$\alpha \geq 2 > 1 \Rightarrow 2(\alpha - 1) \geq \alpha$, beraz:

$$p^{2(\alpha-1)}, \ldots\ldots\ldots\ldots\ldots, p^{n(\alpha-1)} \equiv 0 \ (p^\alpha \text{ mod})$$

Orduan (3) kongruentzia honela gelditzen da:

$$f'(x_0) \cdot p^{\alpha-1} t \equiv -f(x_0) \ (p^\alpha \text{ mod})$$

Eta x_0 $f(x) \equiv 0 \ (p^{\alpha-1} \text{ mod})$ kongruentziaren soluzio bat denez zera dugu:

$$p^{\alpha-1} / f'(x_0) \cdot t \cdot p^{-1} \ , \ p^{\alpha-1} / -f(x_0) \ , \ p^{\alpha-1} / p^\alpha \Rightarrow$$

$$\Rightarrow f'(x_0) \cdot t \equiv \frac{-f(x_0)}{p^{-1}} \ (p \text{ mod}) \qquad (4)$$

Azken kongruentzia hau lineala da eta nola hipotesiz $f'(x_0) \not\equiv 0 \ (p \text{ mod})$ den $\Rightarrow (f'(x_0), p) = 1$ eta halabeharrez (4) kongruentziak $t \equiv t_0 \ (p \text{ mod})$ soluzio bakarra du. Hau da: $t = t_0 + p \cdot t'$, $t' \in Z$

t ren balio hau $x = x_0 + p^{\alpha-1} t$ ekuazioan ordezkatuz, zera dugu:

$x = x_0 + p^{\alpha-1}(t + p \cdot t') = (x_0 + p^{\alpha-1} t_0) + p^\alpha t' = x_1 + p^\alpha t'$, $t' \in Z$

Beraz, $x = x_1 + p^\alpha \cdot t'$, $t' \in Z$, p^α moduluarekiko hondarren klase hau:

$x \equiv x_1 \ (p \text{ mod})$ adierazten du.

1. Korolarioa

Biz x_0 $f(x_0) \equiv 0 \ (p \text{ mod})$ kongruentziaren soluzio bat; $f'(x_0) \not\equiv 0 \ (p \text{ mod})$ baldintza betetzen bada, orduan $x \equiv x_0 \ (\text{mod})$ klasean $f(x) \equiv 0 \ (p^\alpha \text{ mod})$ $\forall \alpha > 1$ kongruentziaren soluzio bakar bat dukegu.

Frogapena

Aurreko teorema $f(x) \equiv 0 \ (p^\alpha \text{ mod})$ kongruentziari aplikatuz: $x \equiv x_0 \ (p \text{ mod})$ hondarren klasean $f(x) \equiv 0 \ (p^2 \text{ mod})$ kongruentziaren soluzio bakar bat dago. Behin eta berriro aipatutako teorema hau aplikatuz, $x \equiv x_0 \ (p \text{ mod})$ klasean $f(x) \equiv 0 \ (p^\alpha \text{ mod})$ kongruentziaren soluzio bakar bat dukegu.

8. Teorema

Biz x_0 $f(x) \equiv 0 \ (p^{\alpha-1} \text{ mod})$ kongruentziaren soluzio bat eta suposa dezagun $f'(x_0) \equiv 0 \ (p \text{ mod})$ dela. Orduan:

a) $f(x_0) \equiv 0 \ (p^\alpha \text{ mod})$ bada, $x \equiv x_0 \ (p^{\alpha-1} \text{ mod})$ hondar klasearen zenbaki guztiak $f(x) \equiv 0 \ (p^\alpha \text{ mod})$ (6) kongruentziaren soluzioak dirateke, eta $f(x) \equiv 0 \ (p^\alpha \text{ mod})$ kongruentziaren p soluzio dukegu.

b) $f(x_0) \not\equiv 0 \ (p^\alpha \text{ mod})$ bada, $x \equiv x_0 \ (p^{\alpha-1} \text{ mod})$ klasean ez dago $f(x) \equiv 0 \ (p^\alpha \text{ mod})$ kongruentziaren soluzio bat ere ez.

Frogapena

Eman dezagun teoremaren hipotesiak betetzen direla eta bila ditzagun $x \equiv x_0 (p^{\alpha-1} \text{ mod})$ (5) klasean $f(x) \equiv 0 \ (p^\alpha \text{ mod})$ kongruentziaren soluzioak.

(5) klasearen zenbakiak $x = x_0 + p^{\alpha-1}.t$, $t \in Z$ dira.

(6) kongruentzian ordezkatuz, eta aurreko teoreman bezala eginez (6) kongruentzia honela idatz dezakegu:

$$f'(x_0).t \equiv \frac{-f(x_0)}{p^{-1}} \ (p \text{ mod}) \quad (7)$$

a kasua:

$f(x_0) \equiv 0 \ (p^\alpha \text{ mod}) \Rightarrow p \mid f(x_0) \Rightarrow p \Big/ \frac{f(x_0)}{p^{-1}}$ eta teoremaren hipotesiaz $f'(x_0) \equiv 0 \ (p \text{ mod})$ dugunez, (7) kongruentzia $\forall t \in Z$ betetzen da.

Beraz, $\forall t \in Z$ $f(x) \equiv 0 \ (p^\alpha \text{ mod})$ kongruentziaren soluzio bat existitzen da.

b kasua:

$f(x_0) \not\equiv 0 \ (p^\alpha \text{ mod}) \Rightarrow p^\alpha \nmid f(x_0) \Rightarrow f(x_0) \equiv 0 \ (p \text{ mod})$ eta honela (7) kongruentzia bakarrik betetzen da $t = 0$ den kasurako. Beraz, $x \equiv x_0 \ (p^{\alpha-1} \text{ mod})$ klasean ez dago $f(x) \equiv 0 \ (p^\alpha \text{ mod})$ kongruentziaren soluziorik.

Eredua

Azter dezagun $f(x) = x^3 + 2 \cdot x + 2 \equiv 0 \ (125 \text{ mod})$ kongruentzia.

$125 = 5^3$ da, beraz:

Lehenengo, $x^3 + 2 \cdot x + 2 \equiv 0 \ (5 \text{ mod})$ kongruentziaren soluzioak aurkitu behar dira.

5 moduluarekiko hondarren sistema 0, ± 1, ± 2 hartuz, $x^3 + 2 \cdot x + 2 \equiv 0 \ (5 \text{ mod})$ kongruentziaren soluzioak $x \equiv 1, -2 \ (5 \text{ mod})$ dira.

Orain $x^3 + 2x + 2 \equiv 0 \ (5^2 \text{ mod})$ kongruentziaren soluzioak aurkitu behar dira.

$f'(x) = 3 \cdot x^2 + 2$

$f'(1) = 5 \equiv 0 \pmod 5$ eta $f(1) \equiv 0 \pmod{5^2}$, beraz 8. teorema erabiliz $x \equiv 1 \pmod 5$ klasean ez dago $x^3+2\cdot x+2 \equiv 0 \pmod{5^2}$ kongruentziaren soluziorik. Orduan klase horretan ez dago ere $x^3 + 2x + 2 \equiv 0 \pmod{5^3}$ kongruentziaren soluziorik.

$f'(-2) = 12 + 2 \not\equiv 0 \pmod 5$. Orduan 7. teorema aplikatuz $x \equiv -2 \pmod 5$ klasean $f(x) \equiv 0 \pmod{5^2}$ eta $f(x) \equiv 0 \pmod{5^3}$ kongruentzien soluzio bat dago.

$x \equiv -2 \pmod 5$ klasearen zenbakiak ondoko erakoak dira:

$$x = -2 + 5t, \quad t \in Z.$$

$f(x) = f(-2+5t) = (-2+5t)^3 + 2(-2+5t) + 2 \equiv 0 \pmod{5^2} \Rightarrow$

$\Rightarrow 70t - 10 \equiv 0 \pmod{5^2} \Rightarrow$

$\Rightarrow 14t - 2 \equiv 0 \pmod 5 \Rightarrow$

$\Rightarrow -t \equiv 2 \pmod 5 \Rightarrow$

$\Rightarrow t \equiv -2 \pmod 5$

Beraz, $t = -2 + 5t'$, $\forall t' \in Z$ eta $x = -2 + 5t$ berdintzetan t ren balio hori ordezkatuz:

$x = -2 + 5(-2 + 5t') = -12 + 5^2 t'$, $t' \in Z \Rightarrow x \equiv -12 \pmod{5^2}$, $f(x) \equiv 0 \pmod{5^2}$ kongruentziaren soluzio bat da.

5 soluzio hauen artean bila ditzagun $f(x) \equiv 0 \pmod{5^3}$ kongruentziaren soluzioak.

$f(x) \equiv 0 \pmod{5^2}$ kongruentziaren soluzioak aurkitzeko egin den bezalaxe eginez, $f(x) \equiv 0 \pmod{5^3}$ kongruentziaren soluzioa $x \equiv -12 \pmod{5^3}$ da.

BOSTGARREN GAIA

BIGARREN GRADUKO KONGRUENTZIAK

- Modulu primu batekiko bigarren mailako kongruentziak.
- Berrekadur honderrak.
- Hondar koadratikoak.
- Legendre-ren sinboloa.
- Elkarrekikotasun koadratikoa.
- Jacobi-ren sinboloa.
- Bigarren graduko kongruentzien ebazketa.

BIGARREN GRADUKO KONGRUENTZIAK

1.- Modulu primu batekiko bigarren graduko kongruentziak

$f(x) \equiv 0 \pmod p$ bigarren graduko kongruentzia bada, orduan $f(x) = ax^2+bx+c$ eta $(a,p) = 1$ dira.

Suposa dezagun $p > 2$ dela, $p = 2$ balioarentzat ez baita zailtasunik azaltzen.

$p > 2$ eta p primua $\Longrightarrow p$ bakoitia da.

Gainera , ondokoa dugu : $4af(x) = (2ax+b)^2 + 4ac-b^2$

u zenbakia , $f(x) \equiv 0 \pmod p$ kongruentziaren soluzio izango da,baldin eta soilik baldin

$$2au+b \equiv v \pmod p \text{ bada,}$$

non v, $v^2 \equiv b^2+4ac$ kongruentziaren soluzio baita.

Gainera, $(2a,p) = 1$ suposatzen badugu,v soluzio bakoitzarentzat existitzen da u bat eta soilik bat, $2au+b \equiv v \pmod p$ kongruentziaren soluzio dena.

Beraz, bigarren graduko kongruentziaren askaketaren arazoa,

$$x^2 \equiv a \pmod p$$

erako kongruentziaren askaketara eraman dezakegu.

Baldin $x^n \equiv a \pmod m$ kongruentzia badugu,non $n > 1$ baita, orduan, n. graduko kongruentzia binomikoa dugula esango dugu.

Lehenik, $m = p$ kasurako, kongruentzia binomikoei buruzko teorema general batzu azalduko ditugu, gero $n = 2$ kasua sakonkiago aztertzera iragaiteko.

Berrekadur hondarrak

1 Definizioa

Baldin $x^n \equiv a \pmod p$ delako kongruentziak soluzioa badu,orduan a,p moduluarekiko n-garren hondarra dela diogu.

2 Definizioa

Izan bitez m 0 zenbaki osoa eta a edozein zenbaki oso, zeinentzat $(a,m)=1$ den. Izan bedi h, $a^h \equiv 1 \pmod m$ betetzen

duten zenbaki oso positiboetariko txikiena.

Orduan a, m moduluarekiko n berretzailekoa de a esango dugu.

Kontutan izaten badugu lehenago ikusiriko Euler-en teorema-gatik $a^{\phi(m)} \equiv 1 \pmod m$ dugula, zera esan dezakegu:

$\forall a \in Z \ , \ (a,m) = 1 \quad \exists h \leq \phi(m)$, non a, m moduluarekiko h berretzailekoa den.

$\phi(m) = q\,h + r \qquad 0 \leq r < h$ izanik, orduan, $h > 0$, $a^h \equiv 1 \pmod m$ betetzen duen zenbaki txikiena izanik, halabeharrez $r = 0$ izan behar dela ikusten dugu.

Hemendik, berehala irtetzen da lehen propietatea.

1 Teorema

a zenbakia, m moduluarekiko h berretzailekoa bada, orduan

$$m \mid \phi(m)$$ gertatzen da.

Gainera, $a^j \equiv a^k$ da, baldin eta soilik baldin $h \mid j-k$ bada.

Frogapena.-

Suposa dezagun $j > k$ dela (Bestela ere, berdin frogatuko genuke)

$(a,m) = 1 \Rightarrow a^j \equiv a^k \pmod m$ eta $a^{j-k} \equiv 1 \pmod m$, baliokideak dira. Beraz, h zenbakiaren definizioa kontuan harturik, $h \mid j-k$ izan behar da.

2 Teorema

a zenbakia, m moduluarekiko h berretzailekoa bada, orduan a^k, $\frac{h}{(h,k)}$ berretzailekoa da m moduluarekiko.

Frogapena.-

Aurreko teoremaren arabera, $(a^k)^j \equiv 1 \pmod m$ da, baldin eta soilik baldin $h \mid kj$ bada.

Baina $h \mid kj$ b.s.b. $\frac{h}{(h,k)} \Big/ \frac{k}{(h,k)}$ bada.

Beraz, $h \mid kj$ b.s.b. $\frac{h}{(h,k)} \Big/ j$ bada.

Ondorioz, $(a^k)^j \equiv 1 \pmod m$ betetzen duten $j > 0$ zenbaki osoetariko txikiena, $j = \frac{h}{(h,k)}$ da.

3 Definizioa

a, m moduluarekiko $\phi(m)$ berretzailekoa bada, orduan, a zenbakia m moduluarekiko erro primitiboa dela esango dugu.

3 Teorema

p zenbakia primua bada,orduan p moduluarekiko $\phi(p-1)$ erro primitibo existitzen dira.

Erro primitiboak dituzten zenbaki bakarrak,ondokoak dira:

$$p^e \quad , \quad 2p^e \quad , \quad 2 \quad , 4$$ (p zenbakia primu bakoitia izanik).

Frogapena.-

Edozein a , $1 \leq a \leq p-1$ izanik , h/ p-1 betetzen duen h berretzaileren batena da,p moduluarekiko.

a zenbakia h berretzailekoa bada,orduan $(a^k)^h \equiv 1 \pmod p \quad \forall k$

Eta $1 , a , a^2, \ldots, a^{h-1}$ desberdinak dira p moduluarekiko.

Ba dakigu,n. graduko kongruentzia batek ezin duela n soluzio baino gehiago eduki, modulua zenbaki primu bat delarik.

Beraz, $1 , a , a^2,\ldots,a^{h-1}$, $x^h \equiv 1 \pmod p$ kongruentziaren soluzio guztiak dira.

2 Teorema aplikatuz,zenbaki horietariko $\phi(h)$, p moduluarekiko h berretzailekoak dira,Besteak berretzaile txikiagotakoak dira.

h berretzailekoa den edozein zenbaki oso a ere, $x^h \equiv 1 \pmod p$ kongruentziaren soluzio da.

Beraz, h/p-1 betetzen duen h bakoitzarentzat,p moduluarekiko h berretzailekoak diren eta $1 \leq a \leq p-1$ betetzen duten $\phi(h)$ zenbaki oso a egongo dira,edo ez da bat ere egongo.

Denota dezagun $\Psi(h)$ sinboloarekin,h berretzailekoak diren a zenbaki osoen kopurua.

Orduan, $\Psi(h) \leq \phi(h)$ izango da, h/p-1 betetzen duen h bakoitzarentzat, eta

$$\sum_{h/p-1} \Psi(h) = p-1$$

Baina $\sum_{h/p-1} \Psi(h) = p-1$ denez,

$$\left.\begin{array}{l}\sum_{h/p-1}(\Psi(h)-\phi(h))=0\\ \text{eta } \Psi(h)\leq\phi(h)\quad \forall h\ ,\ h/p-1\end{array}\right\}\Rightarrow \phi(h)=\Psi(h)\ \forall h\ m\ h/p-1$$

Partikularki, $\phi(p-1)=\Psi(p-1)>0$.

Honekin,teoremaren lehen partea frogaturik gelditzen da.

Erraz ikusten denez,$n>2$ denean, $\phi(n)$ bakoitia da.

Defini dezagun $m=2^f\cdot\prod_{i=1}^{k} p_i^{e_i}$ (p_i zenbaki primu desberdinak izanik ; $f\geq 0$, $e_i>0$, $k\geq 1$)

Baldin (a,m)=1 bada,orduan,

$$a^{\phi(p_i^{e_i})}\equiv 1\ (p_1^{e_1}\ \text{mod})\ \text{eta}\ a^{\phi(m/p_1^{e_1})}\equiv 1\ (m/p_1^{e_1}\ \text{mod})$$

ditugu.

Suposa dezagun orain $k\geq 2$ edo $f\geq 2$ sirela.

Orduan, $\phi(p_1^{e_1})$ eta $\phi(m/p_1^{e_1})$ bikoitiak dira eta beraz,

$$a^{\frac{1}{2}\phi(p_1^{e_1})\cdot\phi(m/p_1^{e_1})}\equiv 1\ (p_1^{e_1}\ \text{mod})$$

$$a^{\frac{1}{2}\phi(p_1^{e_1})\cdot\phi(m/p_1^{e_1})}\equiv 1\ (m/p_1^{e_1}\ \text{mod})$$

$$a^{\frac{1}{2}\phi(p_1^{e_1})\cdot\phi(m/p_1^{e_1})}\equiv 1\ (m)$$

$$m=p_1^{e_1}.m/p_1^{e_1}$$

Honekin zera ikusten dugu;,Erro primitiboak eduki ditzakeen m bakarrak, p^e, $2p^e$, 2 eta 4 direla (p zenbaki primu bakoitia izanik).

4 Teorema

Suposa dezagun m zenbakiak erro primitibo bat duela : g.

Orduan: $g^j\equiv g^k$ (m mod), b.s.b. $j\equiv k$ ($\phi(m)$ mod) bada.

Bereziki:$g^j\equiv 1$ (m mod),b.s.b. $\phi(m)/j$ bada.

$g,g^2,\ldots,g^{\phi(m)}$ multzoa, m moduluarekiko hondar-sistema laburtua da. Beraz,(a,m) = 1 betetzen duen edozein zenbaki a osorentzat,g^j bat eta bakarrik bat existitzen da,ondoko propietatearekin:

$$g^j\equiv a\ (m\ \text{mod})$$

Frogapena.-

Teorema honen lehen partea,1 Teoremaren kasu berezi bat baino ez da. 1 Teorema aplikatuz, $g,g^2,\ldots,g^{\phi(m)}$ potentziak,m moduluarekiko binake inkongruenteak direla ondoriozta dezakegu. Beraz,Beraz,m moduluarekiko hondar-sistema laburtua osatzen dute.

5 Teorema

Baldin p zenbaki primua eta (a,p) = 1 badira,orduan:

$a^{(p-1)/(n,p-1)} \equiv 1 \pmod p$ bada, $x^n \equiv a \pmod p$ kongruentziak (n,p-1) soluzio ditu.

$a^{(p-1)/(n,p-1)} \not\equiv 1 \pmod p$ bada, $x^n \equiv a \pmod p$ kongruentziak ez du soluziorik.

Frogapena,-

Izan dezagun $b=(n,p-1)$

$x^n \equiv a \pmod p$ kongruentziak u soluzioa badu,orduan:

$a^{(p-1)/b} \equiv u^{n(p-1)/b} \equiv u^{(p-1)/(\frac{p}{b})} \equiv 1 \pmod p$ izango da.

Beraz, $a^{(p-1)/b} \not\equiv 1 \pmod p$ den kasuan, $x^n \equiv a \pmod p$ kongruentziak ezin dezake soluziorik eduki.

Aitzitik,suposa dezagun orain, $a^{(p-1)/b} \equiv 1 \pmod p$ dela;

4 Teorema eta 3 Teorema kontutan harturik, $\exists$ p moduluarekiko g erro primitiboa eta $\exists$ j berretzailea,non

$$g^j \equiv a \pmod p \text{ baita.}$$

Honela, $g^{j(p-1)/b} \equiv a^{(p-1)/b} \equiv 1 \pmod p$.

Orduan ,4 Teorema aplikatuz,

$$j(p-1)/b \equiv 0 \pmod p \text{ dugu.} \longrightarrow b/j$$

Jakina da halaber, $x^n \equiv a \pmod p$ kongruentziaren edozein soluzio,g zenbakiaren berredura gisara idatz daitekeela;adibidez, g^y.

Beraz, $x^n \equiv a \pmod p$ kongruentziaren x soluzioak,existitzen badira, $g^{yn} \equiv g^j \pmod p$ kongruentziaren y soluzioekin korrespondentzian daude.

Azken kongruentziak,1 Teoremaren arauera,soluzioak izango ditu, b.s.b. $yn \equiv j \pmod{p-1}$ kongruentziak soluzioak baditu.

$b/j \longrightarrow yn \equiv j \pmod{p-1}$ kongruentziak soluzioak ditu.

Zehazkiago esanez, (n,p-1) soluzio ditu.

Beraz, $x^n \equiv a \pmod p$ kongruentziak ere (n,p-1) soluzio ditu.

Korolarioa

Baldin p delakoa zenbaki primua bada,eta (a,p)=1,orduan:

Baldin $a^{(p-1)/2} \equiv 1 \pmod{p}$ bada, orduan $x^2 \equiv a \pmod{p}$ kongruentziak soluzio bi ditu.

Baldin $a^{(p-1)/2} \equiv -1 \pmod{p}$ bada, orduan, $x^2 \equiv a \pmod{p}$ kongruentziak ez du soluziorik.

Frogapena.-

Fermat-en teorema aplikatuz,

$$(a^{(p-1)/2}-1)(a^{(p-1)/2}+1) \equiv a^{p-1} - 1 \equiv 0 \pmod{p}$$

Hortik, $a^{(p-1)/2} \equiv \pm 1 \pmod{p}$ izan behar dela ateratzen dugu.

Hondar koadratikoak . Legendre-ren sinboloa

Definizioa

$(a,m)=1$ betetzen duen edozein zenbaki a,m moduluarekiko hondar koadratikoa dela esango dugu, $x^2 \equiv a \pmod{m}$ kongruentziak soluziorik badu.

$x^2 \equiv a \pmod{m}$ kongruentziak ez badu soluziortik, a, m moduluarekiko ez-hondar koadratikoa dela esango dugu.

Kontsidera dezagun orain ondoko kongruentzia:

$$x^2 \equiv a \pmod{p} \quad ,(a,p) = 1 \quad (p, \text{zenbaki primua izanik})$$

Ikus ditzagun kongruentzia honekiko zenbait erresultatu :

A) a, p moduluarekiko hondar koadratikoa bada, orduan $x^2 \equiv a \pmod{p}$ kongruentziak soluzio bi ditu.

Frogapena.-

Bistakoa da, definizioa eta aurreko korolarioa kontutan izanik.

B) p moduluarekiko hondar-sistema laburtuak, $\frac{p-1}{2}$ hondar koadratiko eta $\frac{p-1}{2}$ ez-hondar koadratiko ditu. Lehenengoak, $1^2, 2^2, \ldots, \left(\frac{p-1}{2}\right)^2$ zenbakiekin kongruente dira.

Frogapena.-

Jakina, p moduluarekiko hondar-sistema laburtuaren hondarretarik,

$$-\frac{p-1}{2}, \ldots, -2, -1, 1, 2, \ldots, \frac{p-1}{2} \quad \text{(hondar-sistema laburtua)}$$

zenbakien karratuarekin kongruenteak direnak (hau da, $1^2, 2^2, \ldots, \left(\frac{p-1}{2}\right)^2$ zenbakiekin kongruente direnak), eta berak bakarrik izango dira hondar koadratikoak.

Bestalde, $1^2, 2^2, \ldots, \left(\frac{p-1}{2}\right)^2$ ez dira kongruenteak p moduluarekiko.

Suposa dezagun aitzitik, $k^2 \equiv l^2 \pmod{p}$ dela, $0 < k < l \leq \frac{p-1}{2}$

Orduan, $x^2 . l^2 \pmod{p}$ kongruentziak lau soluzio litzeke:

$$x = l, -l, k, -k,$$

Hau, A) sailean azaldurikoaren aurka doa eta beraz, ezinezkoa da.

C) a zenbaki osoa, p moduluarekiko hondar koadratikoa bada, orduan ondokoa dugu:

$$a^{(p-1)/2} \equiv -1 \pmod{p}$$

Frogapena.-

Fermat-en teoremaren arauera, $a^{p-1} \equiv 1 \pmod{p}$ da

Beraz, $(a^{(p-1)/2} - 1)(a^{(p-1)/2} + 1) \equiv 0 \pmod{p}$

$$\left.\begin{array}{l} p/\ (a^{(p-1)/2} - 1)(a^{(p-1)/2} + 1) \\ p \text{ primua} \end{array}\right\} \Rightarrow \begin{array}{ll} p/\ (a^{(p-1)/2} - 1) & (1) \\ p/(a^{(p-1)/2} + 1) & (2) \end{array}$$

Eman dezagun (1) eta (2) gertatzen direla:

$$\left.\begin{array}{l} p/\ (a^{(p-1)/2} - 1) \\ p/\ (a^{(p-1)/2} + 1) \end{array}\right\} \Rightarrow p/\ a^{(p-1)/2} + 1 - (a^{(p-1)/2} - 1) = 2$$

Hori ezinezkoa denez, (1) ala (2) izango ditugu, baina ez biok batera.

Beraz, $a^{(p-1)/2} \equiv 1 \pmod{p}$ ala $a^{(p-1)/2} \equiv -1 \pmod{p}$, baina ez biok.

Bestalde, edozein hondar koadratikok, ondoko kongruentzia betetzen du, x-en batentzat:

$$a \equiv x^2 \pmod{p}$$

Beraz, $a^{(p-1)/2} \equiv 1 \pmod{p}$ ere betetzen du, zeren eta

$$a^{(p-1)/2} \equiv (x^2)^{(p-1)/2} \equiv x^{p-1} \equiv 1 \pmod{p}$$

Gainera, hondar koadratikoek, kongruentzia honen soluzio guztiak agertzen dituzte, kongruentzia $\frac{p-1}{2}$ gradukoa denez, ezin baitu $\frac{p-1}{2}$ soluziotik gora eduki.

Ondorioz, ez-hondar koadratikoek, $a^{(p-1)/2} \equiv -1 \pmod{p}$ kongruentzia bete beharko dute halabeharrez.

Legendre-ren sinboloa

Definizioa

p delakoa zenbaki primu bakoitia eta (a,p)=1 izanik,Legendre-ren sinboloa $\left(\frac{a}{p}\right)$, honela definitzen da:

$$\left(\frac{a}{p}\right) = \begin{cases} 1, & \text{a p moduluarekiko hondar koadratikoa bada} \\ -1, & \text{a p moduluarekiko ez-hondar koadrat. bada} \end{cases}$$

Oharra.- $\left(\frac{a}{p}\right)$ honela irakurten da : a-ren p-rekiko sinboloa. a,sinboloaren zenbakitzailea dela eta b,sinboloaren izendatzailea dela esan ohi da.

Ondoren ikusiko ditugun propietateak, sinbolo honen erabilera praktikoa posibilitatuko dute eta beraz, $x^2 \equiv a \pmod p$ kongruentziaren askagarritasunaren problema konpontzea.

6 Teorema

Baldin p zenbakia primu bakoitia bada eta (a,p)=1=(b,p) bada, orduan:

(i) $\left(\frac{a}{p}\right) \equiv a^{(p-1)/2} \pmod p$

(ii) $\left(\frac{a}{p}\right).\left(\frac{b}{p}\right) = \left(\frac{ab}{p}\right)$, $\left(\frac{ab\ldots l}{p}\right) = \left(\frac{a}{p}\right).\left(\frac{b}{p}\right) \ldots \left(\frac{l}{p}\right)$

(iii) $a \equiv b \pmod p \Longrightarrow \left(\frac{a}{p}\right) = \left(\frac{b}{p}\right)$

(iv) $\left(\frac{a^2}{p}\right) = 1$, $\left(\frac{1}{p}\right) = 1$, $\left(\frac{-1}{p}\right) = (-1)^{(p-1)/2}$

Frogapena.-

(i) Bistakoa da, C) saila kontutan harturik.

(ii) $\left(\frac{ab\ldots l}{p}\right) \equiv (ab\ldots l)^{(p-1)/2} \pmod p \equiv a^{(p-1)/2}.b^{(p-1)/2}\ldots l^{(p-1)/2}$

$\equiv a^{(p-1)/2}.b^{(p-1)/2}\ldots l^{(p-1)/2} \pmod p = \left(\frac{a}{p}\right)\left(\frac{b}{p}\right)\ldots\left(\frac{l}{p}\right)$

(iii)Bistakoa da, zeren klase bereko zenbakiak,guztiak dira hondar koadratiko edo guztiak ez-hondar koadratiko.

(iv) $\left(\frac{a^2}{p}\right) = \left(\frac{a}{p}\right).\left(\frac{a}{p}\right) = 1$

Bestalde, $1 \equiv 1^2$ da. Beraz, 1 hondar koadratikoa da.Nahikoa da orduan Legendre-ren sinboloaren definizioa begiratzea,

$\left(\frac{1}{p}\right) = 1$ dela ondorioztatzeko .

Azkenez, $\left(\frac{-1}{p}\right) = (-1)^{(p-1)/2}$ dela , (i) begiratuz ateratzen dugu, a $=\pm 1$ eginez.

Oharra.- Ikusiriko propietateak aplikatuz,

$$\left(\frac{ab^2}{p}\right)_{(ii)} = \left(\frac{a}{p}\right)\cdot\left(\frac{b^2}{p}\right)_{(iv)} = \left(\frac{a}{p}\right)$$

Hau da, Legendre-ren sinboloaren zenbakitzailean ager daitezkeen karratuak,ez ditugu kontutan hartuko.

7 Teorema (Gauss-en Lema)

Izan bitez p zenbaki bakoitia eta (a,p)=1. Kontsidera ditzagun a, 2a , 3a ,...,$\frac{(p-1)}{2}$a zenbaki osoak eta beren p moduluarekiko hondar ez-negatibo txikienak. Hauetariko n, $\frac{p}{2}$ baino haundiago badira,orduan, $\left(\frac{a}{p}\right) = (-1)^n$

Frogapena.-

Suposa dezagun $r_1,\ldots,r_n$, $\frac{p}{2}$ zenbakia baino haundiago diren hondarrak direla eta $s_1,..,s_k$ beste guztiak.

$r_i \neq s_j$ $\quad i,j \quad i=1,\ldots,n \quad j=1,\ldots,k$

$r_i \neq 0 \quad i=1,\ldots,n$

$s_j \neq 0 \quad j=1,\ldots,k$ $\qquad$ Gainera, $n + k = \frac{p-1}{2}$

Bestalde, $0 < p-r_i < \frac{p}{2} \quad i=1,\ldots,n$

$p - r_i \neq p - s_j \quad i=1,\ldots,n \quad j=1,\ldots,k$

Gainera, $p-r_i \neq s_j \quad i=1,\ldots,n \quad j=1,\ldots,k$

Azken hau frogatzeko, suposa dezagun $p-r_i=s_j$ dela.

$$\left.\begin{array}{l} r_i \equiv \rho\, a \quad 1 \leq \rho \leq \frac{p-1}{2} \\ s_j \equiv \delta\, a \quad 1 \leq \delta \leq \frac{p-1}{2} \end{array}\right\} \text{(1) } r_i, s_j \text{ hondarren definiziotik.}$$

$p-r_i \equiv p - \rho a = s_j \equiv \delta a \Longrightarrow p - \rho a = \delta a \pmod p \Longrightarrow$

$-\rho a \equiv \delta a \pmod p \Longrightarrow (\delta + \rho)a \equiv 0 \pmod p \xrightarrow{(a,p)=1}$

$\delta + \rho \equiv 0 \pmod p$ (Ezinezkoa, (1) baldintzak ikusirik)

Beraz, $p-r_1$, $p-r_2$,...; $p-r_n$,s_1, s_2,...,s_k ezberdinak dira binan-binan,eta ondokoa betetzen dute:

$$\begin{array}{l} 1 \leq p - r_i < \frac{p}{2} \quad i=1,\ldots,n \\ 1 \leq s_j < \frac{p}{2} \quad j=1,\ldots,k \end{array} \qquad n + k = \frac{p-1}{2}$$

Honek esan nahi duena,zera da: halabeharrez,aipaturiko zenbakiak, $1, 2, \ldots, \frac{p-1}{2}$ zenbakiak izan behar direla,beste ordenaren baten beharbada.Biderkaketak trukatze-propietatea duenez,

$$(p-r_1)(p-r_2)\ldots(p-r_n)s_1s_2\ldots s_k = 1.2\ldots \frac{p-1}{2}$$

$$(-r_1)(-r_2)\ldots(-r_n)s_1s_2\ldots s_k \equiv 1.2\ldots\frac{p-1}{2} \pmod p$$

$$(-1)^n r_1r_2\ldots r_n s_1s_2\ldots s_k \equiv 1.2\ldots \frac{p-1}{2} \pmod p$$

Kontutan izanik $r_1,\ldots,r_n,s_1,\ldots,s_k$ direlakoak nola definitu ditugun,

$$(-1)^n a.2a\ldots\frac{p-1}{2}a \equiv 1.2\ldots\frac{p-1}{2} \pmod p$$

$$(2,p) = (3,p)=\ldots=(\frac{p-1}{2},p) = 1$$

$$(-1)^n.a^{(p-1)/2} \equiv 1 \pmod p \xrightarrow{6(i)\ tma.} (-1)^n \equiv a^{(p-1)/2} \equiv \left(\frac{a}{p}\right) \pmod p$$

Gainera,nola $\left(\frac{a}{p}\right) = \pm 1$ eta $-1 \not\equiv 1 \pmod p$ den ,ondokoa dugu:

$$\left(\frac{a}{p}\right) = (-1)^n \qquad \text{(fngl)}$$

8 Teorema

Baldin p zenbakia primu bakoitia eta $(a,2p) = 1$ badira,orduan :

$$\left(\frac{a}{p}\right) = (-1)^{\sum_{j=1}^{\frac{p-1}{2}}\left[\frac{ja}{p}\right]} \quad \text{eta} \quad \left(\frac{2}{p}\right) = (-1)^{(p^2-1)/8} \quad \text{ditugu.}$$

Frogaoena.-

Aurreko teoreman erabiliriko notazioarekin jarraituko dugu.

$r_i, s_j \quad i=1,\ldots,n \quad j=1,\ldots,k$,

ja $j=1,\ldots,\frac{p-1}{2}$ direlakoak, p zenbakiaren artean zatitzerakoan lorturiko hondar positibotariko txikienak dira.

Zatiketa horren zatiduna, $q=\left[\frac{ja}{p}\right]$ izango da.

Beraz, $(a,p)=1$ izanik,

$$\sum_{k=1}^{\frac{p-1}{2}} ja = \sum_{j=1}^{\frac{p-1}{2}} p\cdot\left[\frac{ja}{p}\right] + \sum_{j=1}^{n} r_j + \sum_{j=1}^{k} s_j \qquad \text{eta}$$

$$\sum_{j=1}^{\frac{p-1}{2}} j = \sum_{j=1}^{n}(p-r_j) + \sum_{j=1}^{k} s_j = np - \sum_{j=1}^{n} r_j + \sum_{j=1}^{k} s_j \qquad \text{ondorioztatzen da.}$$

Espresio bion kendura,ondokoa da:

$$(a-1)\sum_{j=1}^{\frac{p-1}{2}} j = p\left(\sum_{j=1}^{\frac{p-1}{2}}\left[\frac{ja}{p}\right] - n\right) - 2\sum_{j=1}^{n} r_j$$

Baina, $\sum_{j=1}^{\frac{p-1}{2}} j = \frac{p^2-1}{8}$

Beraz, $(a-1)\frac{p^2-1}{8} \equiv \sum_{j=1}^{\frac{p-1}{2}} \left[\frac{ja}{p}\right] - n \ (2 \text{ mod}) \qquad (1)$

Kasu bi bereiztuko ditugu:

a) a bakoitia bada, orduan (1) ondoko eran gelditzen zaigu :

$$n \equiv \sum_{j=1}^{\frac{p-1}{2}} \left[\frac{ja}{p}\right] (2 \text{ mod})$$

b) a= 2 bada, (1) ondoko eran gelditzen da:

$n = \frac{p^2-1}{8} (2 \text{ mod})$, $\left(\left[\frac{2j}{p}\right] = 0 \ , 1 \leq j \leq \frac{p-1}{2}\right.$ baita)

Orain, 7 Teorema aplikatuz, guztiz frogatua geldi̇tzen da teorema hau.

Elkarrekikotasun koadratikoa

9 Teorema

Baldin p,q zenbakiak bakoitiak badira, orduan:

$$\left(\frac{p}{q}\right) \cdot \left(\frac{q}{p}\right) = (-1)^{\frac{(p-1)}{2} \cdot \frac{(q-1)}{2}}$$

(Hondar koadratikoen elkarrekikotasun legea)

Frogapena.-

Dakigunez, $\left(\frac{a}{p}\right) = (-1)^{\sum_{j=1}^{\frac{p-1}{2}} \left[\frac{ja}{p}\right]} \qquad (2)$

Ipin dezagun $p_1 = \frac{p-1}{2}$ eta $q_1 = \frac{q-1}{2}$

Kontsidera ditzagun , $x=1,2,\ldots,p_1$ $q= 1,2,\ldots, \frac{q-1}{2}$ balioak independienteki harturik lortzen diren $p_1 q_1$ zenbaki-bikoteak

$qx \neq py \quad \forall x= 1,\ldots,p_1 \quad \forall y= 1,\ldots,q_1$

Hau ikusteko, suposa dezagun $px = qy$ dela $\Longrightarrow$ $py = \dot{q}$ .Hau ezinezkoa da, zeren eta $(p,q) = (y,q) = 1 \quad (0 < y < q$ baita)

Beraz, $p_1 q_1 = S_1 + S_2$ egin dezakegu, non

S_1, $qx < py$ betetzen duten (x,y) bikoteen kopurua eta

S_2, $py < qx$,, ,, ,, ,, ,, ,, baitira

Bistakoa denez, S_1, $x < \frac{p}{q} y$ betetzen duten bikoteen kopurua da.

y jakin bakoitzarentzat, x-ek har ditzakeen balioak ondokoak dira, beraz: $x= 1,2,\ldots, \frac{p}{q} y$

$\left(\frac{p}{q} y \leq \frac{p}{q} q_1 < \frac{p}{2}\right.$ denez, $\left[\frac{p}{q} y\right] \leq p_1$ dugu)

Beraz, $S_1 = \sum_{y=1}^{q_1} \left[\frac{p}{q} y\right]$

Era berean frogatzen da, $S_2 = \sum_{x=1}^{p_1} \left[\frac{p}{q} x\right]$ dela.

Baina orduan, (2) expresioa kontutan izanik,

$\left(\frac{p}{q}\right) = (-1)^{S_1}$, $\left(\frac{q}{p}\right) = (-1)^{S_2}$ dugu.

Orduan, $\left(\frac{p}{q}\right)\cdot\left(\frac{q}{p}\right) = (-1)^{S_1}(-1)^{S_2} = (-1)^{S_1+S_2} = (-1)^{p_1 q_1}$.

Oharra.- Azken teorema honek, 6 Teorema eta 8 Teoremaren bigarren partearekin batera, $\left(\frac{a}{p}\right)$ sinboloaren kalkulu praktikoa zerbait errazten du. Ikus dezagun adibide bat.

1 Adibidea

$$\left(\frac{-42}{61}\right) = \left(\frac{-1}{61}\right)\cdot\left(\frac{2}{61}\right)\cdot\left(\frac{3}{61}\right)\cdot\left(\frac{7}{61}\right)$$

$$\left(\frac{-1}{61}\right) = (-1)^{60/2} = 1$$

$$\left(\frac{2}{61}\right) = (-1)^{\frac{61^2-1}{2}} = -1$$

$$\left(\frac{3}{61}\right) = \left(\frac{61}{3}\right)(-1)^{(2/2)(60/2)} = \left(\frac{1}{3}\right) = 1$$

$$\left(\frac{7}{61}\right) = \left(\frac{61}{7}\right)\cdot(-1)^{(6/2)(60/2)} = \left(\frac{5}{7}\right)\left(\frac{7}{5}\right)(-1)^{(4/2)(6/2)} = \left(\frac{2}{5}\right) = (-1)^{24/8} = 1$$

Beraz, $\left(\frac{-42}{61}\right) = 1$

Kalkulu-bide hau ez da laburrena, baina erabil daitezkeen propietateak hobeto azaltzeko hautatu dugu.

$\left(\frac{-42}{61}\right)$ sinboloaren kalkulurako biderik laburrena, ondokoa da:

$$\left(\frac{-42}{61}\right) = \left(\frac{19}{61}\right) = \left(\frac{69}{19}\right).1 = \left(\frac{4}{19}\right) = 1$$

2 Adibidea

Sinbolo honek, aplikapena du halaber beste problema moeta batetan; Adibidez, aurki ditzagun 3 zenbakia hondar koadratikotzat duten p zenbaki primu bakoiti guztiak.

$x^2 \equiv 3 (p \bmod)$

$$\left(\frac{3}{p}\right) = \left(\frac{p}{3}\right)(-1)^{\frac{p-1}{2}\frac{q-1}{2}} = \left(\frac{p}{3}\right)(-1)^{\frac{p-1}{2}}$$

$$\left(\frac{p}{3}\right) = \begin{cases} \left(\frac{1}{3}\right) = 1 \text{ , } p \equiv 1 \ (3 \bmod) \text{ bada} \\ \left(\frac{2}{3}\right) = -1, \ p \equiv 2 \ (3 \bmod) \text{ bada} \end{cases}$$

$(-1)^{(p-1)/2} = \begin{cases} 1 \ , \ p \equiv 1 \ (4 \text{ mod}) \text{ bada} & (p= 4m-1) \\ -1 \ . \ p \equiv 3 \ (4 \text{ mod}) \text{ bada} & (p= 4m-3) \end{cases}$

Beraz, $\left(\frac{3}{p}\right)= 1$ b.s.b. $\begin{cases} p\equiv 1 \ (3 \text{ mod}) \text{ eta } p\equiv 1 \ (4 \text{ mod}) \\ p\equiv 2 \ (3 \text{ mod}) \text{ eta } p\equiv 3 \ (4 \text{ mod}) \end{cases}$ bada

Hau da, $\left(\frac{3}{p}\right)= 1$ b.s.b. $P\equiv 1(12 \text{ mod})$ edo $p\equiv 11(12 \text{ mod})$ bada

(Azken hau, sistema biok askatuz lortzen da).

Jacobi-ren sinboloa

Legendre-ren sinboloaren kalkuluan arintasun haundiagoa lortzearren, Jaconi-ren sinboloa kontsideratzen da, Legendre-rena baino generalagoa berau .

Definizioa

Izan bedi $(P,Q) = 1$, $Q > 0$, Q bakoitia, non

$Q = q_1 q_2 \ldots q_s$ delakoa, Q-ren faktore primuetango deskonposaketa kanonikoa baita.

(q_i-ak ez dira halabeharrez ezberdinak)

Orduan, $\left(\frac{P}{Q}\right)$ Jacobi-ren sinboloa, honela dago definiturik:

$$\left(\frac{P}{Q}\right) = \prod_{j=1}^{s}\left(\frac{P}{q_j}\right) \text{, non} \left(\frac{P}{q_j}\right) \text{ Legendre-ren sinboloa baita.}$$

Q zenbakia primu bakoitia bada, Jacobi-ren sinboloa eta Legendre-rena, berdinak dira.

Oharra.- Kontuz ibili behar da, sinbolo biak ez nahasteko, zeren eta

$\left(\frac{P}{Q}\right) = \pm 1$ bistakoa denez, baina:

$\left(\frac{P}{Q}\right) = 1 \not\longrightarrow P$, Q moduluarekiko hondar koadratikoa.

Adibidea: $\left(\frac{2}{9}\right) = 1$ baina $x^2 \equiv 2(9 \text{ mod})$ delako kongruentziak ez du soluziorik.

a zenbakia, Q moduluarekiko hondar koadratikoa izango da, soilik ondokoa gertatzen bada:

(a,Q) = 1 eta a, Q zatitzen duten p zenbaki primu guztiekiko hondar koadratikoa bada.

$\left(\frac{a}{Q}\right) = -1$ bada, orduan a ezda Q moduluarekiko honder koadratikoa. Legendre-ren sinboloaren propietateak erabilirik, propietate hor - dintsuak ditugu Jacobi-ren sinboloarentzat.

10 Teorema

Suposa dezagun Q , Q' zenbaki bakoiti positiboak direla eta $(P,Q)=1$ dela. Orduan,

(i) $\left(\frac{P}{Q}\right)\cdot\left(\frac{P}{Q'}\right)=\left(\frac{P}{QQ'}\right)$

(ii) $\left(\frac{P}{Q}\right)\cdot\left(\frac{P'}{Q}\right)=\left(\frac{PP'}{Q}\right)$

(iv) $\left(\frac{P^2}{Q}\right)=\left(\frac{P}{Q^2}\right)=1$

(v) $P'\equiv P\ (Q \bmod) \Longrightarrow \left(\frac{P'}{Q}\right)=\left(\frac{P}{Q}\right)$

(vi) $\left(\frac{1}{Q}\right)=1 \quad \left(\frac{-1}{Q}\right)=(-1)^{(Q-1)/2} \quad , \left(\frac{2}{Q}\right)=(-1)^{(P^2-1)/8}$

Frogapena.-

(i) Bistakoa da, jacobi-ren sinboloaren definizioa kontutan i-zanik.

(ii) Bistakoa da, definizioa eta 6 (ii) Teorema aplikatuz.

(iii) $\left(\frac{P^2}{Q}\right)=\left(\frac{P}{Q}\right)\left(\frac{P}{Q}\right)=\left(\frac{P}{Q^2}\right)=(\pm 1)(\pm 1)=1$

(iv) $\frac{P'P^2}{Q'Q^2}, \equiv \left(\frac{P'}{Q'}\right)\cdot\left(\frac{P^2}{Q^2}\right) \underset{(ii)}{=} \left(\frac{P'}{Q'}\right)\left(\frac{P}{Q^2}\right)\left(\frac{P}{Q^2}\right) \underset{(ii)}{=} \left(\frac{P}{Q'}\right)$

(v) $P'\equiv P\ (Q \bmod)$

$P'=p_1'\cdot p_2'\cdot\ldots\cdot p_r'$, $P=p_1\cdot p_2\cdot\ldots\cdot p_s$. P'eta P-ren faktore primuetango deskonposaketa kanonikoak dira.

$Q=q_1\cdot q_2\cdot\ldots\cdot q_s$ Q-ren faktore primuetango deskonposaketa kanonikoa da.

$P\equiv P'(Q \bmod) \Longrightarrow P\equiv P'(q_j \bmod) \quad j=1,\ldots,s \Longrightarrow$

$\left(\frac{P'}{q_j}\right)=\left(\frac{P}{q_j}\right) \quad j=1,\ldots,s$ Beraz,

$\left(\frac{P'}{Q}\right)=\left(\frac{P'}{q_1}\right)\cdot\ldots\cdot\left(\frac{P'}{q_s}\right)=\left(\frac{P}{q_1}\right)\cdot\ldots\cdot\left(\frac{P}{q_s}\right)=\left(\frac{P}{Q}\right)$

(vi) $\left(\frac{1}{Q}\right) = \left(\frac{1}{q_1}\right).....\left(\frac{1}{q_s}\right) = 1^s = 1$

$$\left(\frac{(-1)}{Q}\right) = \prod_{j=1}^{s} \left(\frac{-1}{q_j}\right) = \prod_{j=1}^{s} (-1)^{(q_j-1)/2} = (-1)^{\sum_{j=1}^{s} \frac{q_j-1}{2}}$$

Baina a eta b zenbaki bakoitiak badira, zera dugu:

$$\frac{ab-1}{2} - \left(\frac{a-1}{2} + \frac{b-1}{2}\right) = \frac{(a-1)(b-1)}{2} \equiv 0 \ (2 \text{ mod})$$

Eta hemendik, $\frac{a-1}{2} + \frac{b-1}{2} \equiv \frac{ab-1}{2}$ (2 mod) dugu.

Azken berdintza hau errepikatuz lortzen duguna, zera da :

$$\sum_{j=1}^{s} \frac{q_j-1}{2} \equiv \frac{1}{2}\left(\prod_{j=1}^{s} q_j - 1\right) \equiv \frac{Q-1}{2} \ (2 \text{ mod})$$

Eta horrela, $\left(\frac{-1}{Q}\right) = (-1)^{\frac{Q-1}{2}}$

$$\left(\frac{2}{Q}\right) = \prod_{j=1}^{s}\left(\frac{2}{q_j}\right) = (-1)^{\sum_{j=1}^{s} \frac{(q_j^2-1)}{8}}$$

Baina a eta b zenbaki bakoitiak badira, orduan:

$$\frac{a^2b^2-1}{8} - \left(\frac{a^2-1}{8} + \frac{b^2-1}{8}\right) = \frac{(a^2-1)(b^2-1)}{8} \equiv 0 \ (8 \text{ mod})$$

Horrela, $\frac{a^2-1}{8} + \frac{b^2-1}{8} \equiv \frac{a^2b^2-1}{8}$ (2 mod)

Hau errepikatuz, $\sum_{j=1}^{s} \frac{q_j^2-1}{8} \equiv \frac{Q^2-1}{8}$ (2 mod)

Eta horrela, $\frac{2}{Q} = \prod_{j=1}^{s}\left(\frac{2}{q_j}\right) = (-1)^{\sum_{j=1}^{s} \frac{q_j^2-1}{8}} = (-1)^{\frac{Q^2-1}{8}}$

11 Teorema

P,Q zenbaki bakoiti positiboak eta (P,Q) = 1 badira, orduan:

$$\left(\frac{P}{Q}\right).\left(\frac{Q}{P}\right) = (-1)^{\frac{P-1}{2}.\frac{Q-1}{2}}$$

Frogapena.-

$P = \prod_{i=1}^{r} p_i$, $Q = \prod_{j=1}^{s} q_j$ P eta Q-ren faktore primuetango deskonposaketa kanonikoak badira, orduan:

$$\left(\frac{P}{Q}\right) = \prod_{j=1}^{s}\left(\frac{P}{q_j}\right) = \prod_{j=1}^{s}\prod_{i=1}^{r}\left(\frac{p_i}{q_j}\right) = \prod_{j=1}^{s}\prod_{i=1}^{r}\left(\frac{q_j}{p_i}\right).(-1)^{\frac{p_i-1}{2}.\frac{q_j-1}{2}} =$$

$$= \left(\frac{P}{Q}\right).(-1)^{\sum_{j=1}^{s}\sum_{i=1}^{r}\frac{p_i-1}{2}\frac{q_j-1}{2}}$$

Baina, $\sum_{j=1}^{s}\sum_{i=1}^{r}\frac{p_i-1}{2}\frac{q_j-1}{2} = \sum_{i=1}^{r}\frac{p_i-1}{2}\sum_{j=1}^{s}\frac{q_j-1}{2}$ da.

Eta $\sum_{i=1}^{r} \frac{p_i-1}{2} \equiv \frac{P-1}{2}$ (2 mod) , $\sum_{j=1}^{s} \frac{q_j-1}{2} \equiv \frac{Q-1}{2}$ =(2 mod)

(10 Teoreman erabiliriko metodo berberarekin)

Beraz, $\left(\frac{P}{Q}\right) = \left(\frac{Q}{P}\right) \cdot (-1)^{\frac{P-1}{2} \cdot \frac{Q-1}{2}}$ (fngl)

Oharra.- Ikusten dugunez, Jacobi-ren sinboloak ere elkarrekikotasunaren propietatea betetzen du.

Jacobi-ren sinboloa, Legendre-ren sinboloaren hedapena da,Q zenbaki konposatuarentzat $\left(\frac{P}{Q}\right)$ definituz.

Lehen begiradan ba dirudi logikoago gerta daitekeela Jacobi-ren sinboloaren beste era batetara definitzea:

$$\left(\frac{P}{Q}\right) = \begin{cases} 1, & P \text{ Q moduluarekiko hondar koadratikoa bada} \\ -1, & P \text{ Q moduluarekiko ez-hondar koadratikoa bada} \end{cases}$$

Baina honela egingo bagenu,elkarrekikotasunaren legea ez litzateke beteko (Adibidez,P = 5 eta Q = 9 harturik). Eta lege honek duen garrantzia ikusirik,egin dena beste hau izan da:Hondar koadratikoekiko erlazioa alde batera utzirik,elkarrekikotasunaren legea kontutan hartu.

1 Adibidea ikusi dugunean,elkarrekikotasunaren legea erabili dugu, $\left(\frac{p}{q}\right)$-tik $\left(\frac{q}{p}\right)$-ra iragateko,baina bakarrik p orimua izanik.Orain ez dugu jadanik mugaketa hori.

3 Adibidea

$$\left(\frac{105}{317}\right) = \left(\frac{317}{105}\right) = \left(\frac{2}{105}\right) = 1$$

Hemendik ondorioztatzen dugu, 105 zenbakia ,317 modulu orimuarekiko hondar koadratikoa dela.

4 Adibidea

Jacobi-ren eta Legendre-ren sinbolnen erabilera ondo argitzeko, ikus dezagun ondoko kongruentziak soluziorik duenentz:

$$x^2 = 219 \ (383 \text{ mod})$$

$$\left(\frac{219}{383}\right) = -\left(\frac{383}{219}\right) = -\left(\frac{164}{219}\right) = -\left(\frac{41}{219}\right) = -\left(\frac{219}{41}\right) = -\left(\frac{14}{41}\right) =$$

$$= -\left(\frac{2}{41}\right) \cdot \left(\frac{7}{41}\right) = -\left(\frac{7}{41}\right) = -\left(\frac{41}{7}\right) = -\left(\frac{-1}{7}\right) = 1$$

Beraz, aipaturiko kongruentziak soluzioa du.; Ikusi dugunez, soluzioa badu,halabeharrez soluzio bi ditu.

Bigarren graduko kongruentzien askaketa

Modulu orimu batekiko bigarren graduko kongruentzien askaketa

$x^2 \equiv a \pmod{p}$ (1) $(a,p) = 1$; p zenbakia orimu bakoitia izanik.

(a) $p = 4N - 1$

a hondar koadratikoa denentz jakiteko, lehenik $\left(\frac{a}{p}\right) = 1$ dela konprobatu behar da.

Hori frogatuz gero, Euler-en adierazpidea aplikaturik,

$$a^{(p-1)/2} \equiv 1 \pmod{p} \quad \text{dugu.}$$

$p = 4N - 1 \Rightarrow \frac{p-1}{2} = 2N - 1 \Longrightarrow a^{2N-1} \equiv 1 \pmod{p} \Longrightarrow x = a^{2N} \pmod{p}$

$\Rightarrow a \equiv a^{2N} \pmod{p}$

Beraz, (1) expresioa kontutan izanik, $x^2 \equiv a^{2N} \pmod{p}$

$$x \equiv \pm a^{N} \pmod{p}$$

Adibidea.- $x^2 \equiv 1 \pmod{19}$

$19 = 4.5 - 1$ 19 zenbakia orimu bakoitia da eta $N = 5$.

$\left(\frac{11}{19}\right) = -\left(\frac{19}{11}\right) = -\left(\frac{8}{11}\right) = -\left(\frac{2}{11}\right) = 1$ Soluzioa existitzen da.

$$x \equiv \pm 11^{5} \pmod{19} = \pm 7 \pmod{19}$$

Beraz, kongruentziaren soluzioa, $x = \pm 7 \pmod{19}$ da.

(b) $p = 4N + 1$

Edozein p zenbaki bakoiti orimu,ondoko eraren batetakoa izango da : $p = 8N+1$, $p = 8N+3$, $p = 8N+5$, $p = 8N+7$

Baina $p = 4N+1$ denez gero, $p = 8N+1$ edo $p = 8N+5$ izan beharko da.

b1) $p = 8N+5$

Suposa dezagun $\left(\frac{a}{p}\right) = 1$ dela konprobatu dugula.

Euler-en adierazpidearen arauera, $a^{(p-1)/2} \equiv 1 \pmod{p}$

$\frac{p-1}{2} = 4N+2 \Longrightarrow a^{4N+2} \equiv 1 \pmod{p}$ (2)

$\left(\frac{2}{p}\right) = (-1)^{\frac{p^2-1}{8}} \underset{p=8N+5}{=} (-1)^{\frac{5^2-1}{8}} = -1 \Longrightarrow 2$ ez-hondar koadratikoa da.

Beraz, Euler-en adierazpidea berriro aplikatuz,

$2^{(p-1)/2} \equiv -1 \pmod{p} \Longrightarrow 2^{4N+2} \equiv -1 \pmod{p}$ (3)

(2) ekuazioetik, $a^{2N+1} \equiv \pm 1 \pmod{p}$ dugu.

-- $a^{2N+1} \equiv -1 \pmod{p}$ Kongruentzia hau (3) kongruentziagatik biderkatuz ondokoa dugu:

$a^{2N+1}.2^{4N+2} \equiv 1 \pmod{p} \Longrightarrow a \equiv a^{2N+2}.2^{2N+1} \pmod{p}$ $s = 0, 1$

-- $a^{2N+1} \equiv 1 \pmod{p} \Longrightarrow a \equiv a^{2N+2} \pmod{p} \longrightarrow$

$\Longrightarrow x^2 \equiv a^{2N+2} \pmod{p} \longrightarrow x \equiv \pm a^{N+1} \pmod{p}$

Beraz, $p = 8N+5$ bada, $x^2 \equiv a \pmod{p}$ kongruentziak ondoko soluzioak ditu:

$$x = \pm a^{N+1}.2^{(2N+1)s} \pmod{p} \quad s = 0,1$$

Praktikan, ondokoa egin ohi da : a^{N+1} kongruentziaren soluzio denentz begiratu. Horrela bada, amaitu dugu. Bestela, soluzioa $a^{N+1}.2^{2N+1}$ da.

Adibidea.- $x^2 \equiv 5 \pmod{29}$ 29 zenbakia primu bakoitia da.

$29 = 8.3 + 5 \qquad N=3$

$\left(\frac{5}{29}\right) = \left(\frac{29}{5}\right) = \left(\frac{4}{5}\right) = 1$ Soluzioa existitzen da.

$a^{N+1} = 5^4$; a^{N+1} soluzio ote da?

$5^4 \equiv -13 \pmod{29}$ eta $(-13)^2 = 169 \not\equiv 5 \pmod{29} \Longrightarrow 5^4$ ez da kongruentziaren soluzio.

Beraz, soluzioa ondokoa izango da: $x = \pm 5^4.2^7 \pmod{29}$

b2) $p = 8N + 1$

$p = 8N + 1 \Longrightarrow \frac{p-1}{2} = 4N$

$\left(\frac{a}{p}\right) = 1$ bada, Euler-en adierazpidea aplikatuz, $a^{(p-1)/2} \equiv 1 \pmod{p}$ dugu $\Longrightarrow a^{4N} \equiv 1 \pmod{p}$ (4)

$\left(\frac{2}{p}\right) = (-1)^{\frac{p^2-1}{8}} \equiv 1 \pmod{p} \Longrightarrow 2$ hondar koadratikoa da eta beraz, ez du balio.

Ez-hondar koadratiko bat, b, bilatu behar dugu (Existitzen dela ba dakigu, $\frac{p-1}{2}$ ez-hondar koadratiko baitaude).

b ez-hondar koadratiko hori bada $\Longrightarrow b^{(p-1)/2} \equiv 1 \pmod{p}$

$$b^{4N} \equiv -1 \pmod{p} \quad (5)$$

Suposa dezagun, $p = 2^k.h + 1$ dela $(h \equiv 1(2 \bmod), k \geq 3)$

Beraz, $N = 2^{k-3}.h$ da.

Honekin, (4) honela idatziko dugu : $a^{2^{k-1}.h} \equiv 1(p \bmod)$

(5) honela idatziko dugu : $a^{2^{k-1}.h} \equiv -1(p \bmod)$

$$k-1 \geq 2 \Rightarrow \begin{cases} a^{2^{k-2}.h} \equiv \pm 1(p \bmod) & (6) \\ b^{2^{k-1}.h.s} \equiv \pm 1(p \bmod) \quad s=0,1 & (7) \end{cases}$$

S-ren balioa. (6) eta (7) espresioek zeinu berdina edukitzeko eran hartuko dugu. Orduan, kongruentzia biak biderkatuz,

$$a^{2^{k-2}.h} b^{2^{k-1}.h.s} \equiv 1(p \bmod) \quad k - 2 \geq 1 \longrightarrow$$

$$\Longrightarrow a^{2^{k-3}.h} . b^{2^{k-2}.h.s} = \pm 1(p \bmod) \; ; \; s_2 = h.s \text{ eginik},$$

$$a^{2^{k-3}.h} . b^{2^{k-2}.s_2} \equiv \pm 1(p \bmod) \text{ dugu.} \quad (8)$$

s-ren balioa, (7) eta (8) espresioek zeinu berdina edukitzeko eran hautatuko dugu. Orduan :

$$2^{k-2}s_2 + 2^{k-1}s_2 = 2^{k-2}(s_2 + 2s_2) \quad \text{Dei dezagun} \quad s_3 = 3s_2.$$

Orduan, $a^{2^{k-3}h} . b^{2^{k-2}s_3} \equiv 1 \; (p \bmod)$

$K \geq 3$ bada, prozesu hau jarrai dezakegu oraindik;Erro kalkulatua ateraz,ondokoa geratzen da:

$$a^{2^{k-4}h} . b^{2^{k-3}s_3} \equiv \pm 1 \; (p \bmod)$$

Azken urratzsean,zera edukiko dugu:

$$a^h . b^{2s_k} \equiv 1 \; (p \bmod) \text{ , non } s_k \in \mathbb{Z} \text{ baita.}$$

H zenbakia bakoitia denez,aurreko kasoen arrazonamendu berdintsua egingo dugu hemen ere:

$$a^{h+1} . b^{2s_k} \equiv a(p \bmod) \Longrightarrow x^2 \equiv a^{h+1} . b^{2s_k}(p \bmod) \Longrightarrow$$

$$\Longrightarrow x \equiv \pm a^{(h-1)/2} . b^{s_k} (p \bmod) \quad (\tfrac{h-1}{2} \in \mathbb{Z}, \text{h zenbakia bakoitia baita}).$$

Oharra.- Praktikan, $a^{\frac{h+1}{2}}$, $a^{\frac{h+1}{2}} . b$, $a^{\frac{h+1}{2}} . b^2$,... zenbakiak kongruentziaren soluzio direnentz ikusten da.

Adibidea.-

Adibidea.- $x^2 \equiv 5 \pmod{41}$

$41 = 8.5 + 1$, $N = 5$.

$\left(\frac{5}{41}\right) = \left(\frac{41}{5}\right) = \left(\frac{1}{5}\right) = 1$ kongruentziak soluzioa du.

Edozein ez-hondar koadratiko b aurkitu behar dugu orain. Teoriaz dakigunez, 2 hondar koadratikoa da eta beraz,ez du balio.

$\left(\frac{-1}{p}\right) = 1 \Longrightarrow$ -1 ere hondar koadratikoa da.

$\left(\frac{3}{41}\right) = \left(\frac{41}{3}\right) = \left(\frac{2}{3}\right) = (-1)^{\frac{3^2-1}{8}} = -1 \Longrightarrow$ 3 ez-hondar koadratikoa da. Beraz, b=3 har dezakegu.

$41 = 2^3.5$,h = 5 , a = 5

Orduan,ikusi duguna aplikatuz, soluzioa ondokoa izango da:

$$x \equiv \pm 5^3.3^s k \pmod{41}$$

$5^2 = 25$ $5^3 \equiv 125 \equiv 2 \pmod{41}$

Beraz, $x = \pm 2.3^s k \pmod{41}$

Soluzioak, $x = 2 , 2.3 , 2.3^2, 2.3^3, \ldots$ zenbakien artean bilatu beharko ditugu.

2 , 6 , 18 zenbakiek ez dute kongruentzia betetzen .

$x = 2.3^3 \equiv 13 \pmod{41}$ $13^2 \equiv 5 \pmod{41}$

Beraz, kongruentziaren soluzio biak ondokoak dira:

$$x = \pm 13 \pmod{41}$$

Modulu konposatu batekiko bigarren graduko kongruentzien askaketa

Orain arte, p modulu primuarekiko bigarren kongruentziak baino ez ditugu aztertu.Has gaitezen,ba, edozein modulu konpodaturekiko bigarren graduko kongruentziak azaltzen.

Has gaitezen, $x^2 \equiv a(p^\alpha \bmod)$ erako kongruentziak azaltzen, $(a,p) = 1$ eta p zenbakia, primu bakoitia izanik.

12 Teorema

Kontsidera dezagun $x^2 \equiv a \ (p^\alpha \bmod)$; $\alpha > 0$, $(a,p) = 1$, (1) p zenbakia,orimu bakoitia izanik.

$f(x) = x^2 - a$ eginez, $f'(x) = 2x$

$x \equiv x_1 (p \text{ mod})$, $x^2 \equiv a (p \text{ mod})$ kongruentziaren soluzio bada,

orduan $(x_1, p) = 1$, ($(a,p)=1$ baita).

p bakoitia
$(x,p)=1$ $\Big\}\rightarrow (2x_1, p) = 1 \longrightarrow p \nmid f(x_1)$

Beraz, kasu honetan,(1) kongruentziaren soluzioa lortzeko,

IV. kapituluan azalduriko prozedura erabil daiteke.

Honetatik,ondokoa ondorioztatzen dugu:

(a) a zenbakia,p moduluarekiko hondar koadratikoa bada,orduan

(1) kongruentziak soluzio bi ditu.

(b) a zenbakia p moduluarekiko ez-hondar koadratikoa bada,

orduan (1) kongruentziak ez du soluziorik.

Kontsidera dezagun orain:

$$x^2 \equiv a(2^{\alpha} \text{ mod}) \ , \alpha > 0, \quad (a,2) = 1 \quad (2)$$

Kasu honetan, $f'(x) = 2x_1 = 2$ .Orduan,aurreko orozedura aplika ezin daitekeenez,beste metodo bat aurkitu beharko dugu.

Lehenik, ikus dezagun, (2) kongruentziak soluzioa edukizteko baldintza beharrezkoa zein den.

(2) kongruentziak soluziorik badu,orduan $(a,2) = 1$ denez,

$(x,2) = 1$ izan behar du $\Longrightarrow 8 / x^2 - 1$

Hau dela eta, kongruentzia ondoko eran jarririk,

$$(x^2-1) + 1 \equiv a \ (2^{\alpha} \text{ mod}),$$

erraz ikusten dugu,kongruentzia honek soluziorik eduki dezan,

$a \equiv 1 \ (4 \text{ mod})$ $\alpha = 2$ edo eta $a \equiv 1 \ (8 \text{ mod})$ $\alpha \geq 3$ izan behar dela.

Orain, baldintza hauk betetzen direla suoosaturik,ikus dezagun soluzioen bilakuntzaren eta soluzioen kopuruaren problema.

Ikusi dugunagatik, $\alpha \leq 3$ denean,edozein zenbaki bakoitik kongruentzia betetzen du.

Beraz, $x^2 \equiv a(2 \text{ mod})$ kongruentziak,soluzio bat du:

$$x \equiv 1 \ (2 \text{ mod})$$

$x^2 \equiv a \ (4 \text{ mod})$ kongruentziak soluzio bi ditu:

$$x \equiv 1 \ (4 \text{ mod}) \quad \text{eta} \quad x \equiv 3 \ (4 \text{ mod})$$

$x^2 \equiv a \ (8 \text{ mod})$ kongruentziak ,lau soluzio ditu:

$x \equiv 1(8 \text{ mod})$, $x \equiv 3(8 \text{ mod})$, $x \equiv 5(8 \text{ mod})$ eta $x \equiv 7 \ (8 \text{ mod})$

Oharra.- $\alpha = 4,5,\ldots$ kasuak aztertzeko,komenigarri da zenbaki bakoiti guztiak progresio aritmetiko bitan batzea:

$$x = \pm(1+4t_3) \quad (3)$$

Ikus dezagun adibidez, (3) expresioko zenbat zenbakik betetzen duten $x^2 \equiv a(32 \text{ mod})$ kongruentzia.

$(x_4+8t_4)^2 \equiv a \ (32 \text{ mod}) \qquad t_4 = t_4'-2t_5$

Beraz, $x = \pm (x_5+16t_5)$

Prozesu hau jarraituz, edozein $\alpha>3$ zenbakirentzat,(2) kongruentzia betetzen duten x-en balioak,honela ipin daitezke:

$$x = \pm (x_\alpha - 2^{\alpha-1}t_\alpha)$$

Balio hauek, $x^2 \equiv a(2^\alpha \text{ mod})$ kongruentziaren lau soluzio ezberdin osotzen dituzte:

$$x = x_\alpha \ (2^\alpha \text{mod}) \quad , \quad x = x_\alpha + 2^{\alpha-1} (2^\alpha \text{ mod})$$
$$x = -x_\alpha \ (2^\alpha \text{mod}) \quad , \quad x = -x_\alpha - 2^{\alpha-1} (2^\alpha \text{ mod})$$

Adibidea.-

$x^2 \equiv 57 \ (64 \text{ mod})$ kongruentziak,lau soluzio ditu,

$57 \equiv 1 \ (8 \text{ mod})$ baita.

$x = \pm(1 + 4t_3)$ jarririk,ondokoa lortzen dugu:

$(1+4t_3)^2 \equiv 57 \ (16 \text{ mod}) \ , \ 8t_3 \equiv 56 \ (16 \text{ mod})$

$t_3 \equiv 1 \ (2 \text{ mod}) \Longrightarrow t_3 = 1 + 2t_4 \Longrightarrow x = \pm (5+8t_4)$

$(5+8t_4)^2 \equiv 57 \ (32 \text{ mod}) \ , \ 5.16t_4 \equiv 32 \ (64 \text{ mod})$

$t_4 \equiv 0 \ (2 \text{ mod}) \Longrightarrow t_4 = 2t_5 \Longrightarrow x = \pm(5+16t_5)$

$(5+16t_5)^2 \equiv 57 \ (64 \text{ mod}) \ , \ 5.32t_5 \equiv 32 \ (64 \text{ mod})$

$t_5 \equiv 1 (2 \text{ mod}) \longrightarrow t_5 = 1+2t_6 \Longrightarrow x = \pm (21+32t_6)$

Beraz, $x^2 \equiv 57(64 \text{ mod})$ kongruentziaren soluzioak, hauk dira:

$$x = \pm 21 \ , \pm 53 \ (64 \text{ mod})$$

13 Teorema

Hemen ikusiriko guztia,teorema batetan bil daiteke:

$x^2 \equiv a(2^\alpha \text{ mod}) \ (a,2) = 1$ kongruentziaren askagarriatsumerako baldintza beharrezkoak,ondokoak dira:

$a \equiv 1 \pmod{\ }$, $\alpha = 2$ bada, eta

$a \equiv 1 \pmod{8}$, $\alpha \geq 3$ bada.

Baldintza hauk betetzen badira, soluzioen kopurua ondokoa da:

1, $\alpha = 1$ bada.

2, $\alpha = 2$ bada.

4, $\alpha \geq 3$ bada.

Era berean beste teorema general bat aipa dezakegu,12 Teorema eta 13 Teorema,Teorema bakar batean bilduz;

14 Teorema

$x^2 = a \pmod{m}$ $m = 2^{\alpha} p_1^{\alpha_1} p_2^{\alpha_2} \ldots p_k^{\alpha_k}$, $(a,m)=1$ kongruentziarentzat, askagarritasun-baldintzak ondokoak dira :

$a \equiv 1 \pmod{4}$, $\alpha = 2$ bada eta

$a \equiv 1 \pmod{8}$, $\alpha \geq 3$ bada.

$$\left(\frac{a}{p_1}\right) = 1, \quad \left(\frac{a}{p_2}\right) = 1, \ldots\ldots, \quad \left(\frac{a}{p_k}\right) = 1.$$

Baldintza hauk guztiok betetzen badira,soluzioen kopurua ondokoa da:

2^k , $\alpha = 0$ bada , eta $\alpha = 1$ bada;

2^{k+1}, $\alpha = 2$ bada;

2^{k+2}, $\alpha \geq 3$ bada.

SEIGARREN GAIA

ERRO PRIMITIBOAK

ETA INDIZEAK

- Teorema batzu.
- p eta 2p moduluarekiko erro primitiboak.
- p eta 2p moduluarekiko indizeak.
- Aurreko teoriaren ondorio batzu.

ERRO PRIMITIBOAK ETA INDIZEAK

I.TEOREMA BATZU.

Definizioa

Bira $a,m \in \mathbb{Z}$ zenbakiak non $(a,m)=1$ baita.
Biz δ ondoko propietatea betetzen dituen zenbakien arteko txikiena:

$$a^{\nu} \equiv 1 \pmod{m}. \qquad (\delta = \min.\nu).$$

δ zenbakia beti existitzen da, zeren Eulerren teoremaz:

$$a^{\varphi(m)} \equiv 1 \pmod{m}.$$

a zenbakia, m moduluarekiko berretzaileari dagokiola esango dugu.

Teorema

a zenbakia, m moduluarekiko δ berretzaileari baldin badagokio, $1 = a^{0}, a^{1}, \ldots\ldots a^{\delta-1}$ zenbakiak ez dira m moduluarekiko kongruenteak.

Frogapena:

Eman dezagun, absurdura eramanez:

$a^{l} \equiv a^{k} \pmod{m}$ $\quad 0 \leq k < l < \delta$; orduan:

$a^{l-k} \equiv 1 \pmod{m}$ $\quad$ non $0 \leq l-k < \delta$ baita

eta hau δ definizioaren aurka dago.

Teorema

a zenbakia, m moduluarekiko δ berretzaileari baldin badagokio, orduan:

$a^{\nu} \equiv a^{\nu'} \pmod{m}$ $\quad$ baldin eta soilik baldin:

$\nu \equiv \nu' \pmod{\delta}$ $\quad$ bada

Bereziki $(\nu' = 0)$ $a^{\nu} \equiv 1$ baldin eta soilik baldin ν, δ zenbakiz zatigarria bada.

Frogapena:

Honela idatz dezakegu:

$\nu = \delta q + r$ non $0 \leq r < \delta$ baita.

$\nu' = \delta q_1 + r_1$ non $0 \leq r_1 < \delta$ baita.

Dakigunez:

$a^{\delta} \equiv 1 \pmod{m}$, orduan eta aurreko propietateaz baliatuz:

$a^{\nu} = (a^{\delta})^{q} a^{r} \equiv a^{r} \pmod{m}$

$a^{\nu'} = (a^{\delta})^{q_1} a^{r_1} \equiv a^{r_1} \pmod{m}$

Beraz:

$a^{\nu} \equiv a^{\nu'} \pmod{m} \Leftrightarrow a^{r} \equiv a^{r_1} \pmod{m} \Leftrightarrow a^{r-r_1} \equiv 1 \pmod{m}$

$\Leftrightarrow r - r_1 = 0$ (zeren $r - r_1 < \delta$ baita) $\Leftrightarrow r = r_1 \Leftrightarrow$

$\Leftrightarrow \nu - \nu' = \delta(q - q_1) \Leftrightarrow \nu \equiv \nu' \pmod{\delta}$

Bereziki:

$a^{\nu} \equiv a^{0} \pmod{m} \Leftrightarrow \nu \equiv 0 \pmod{\delta} \Leftrightarrow \nu = k\delta \Leftrightarrow$

ν, δ zenbakiz zatigarria bada.

Korolarioa

$a^{\varphi(m)} \equiv 1 \pmod{m}$ denez, $\varphi(m)$ δ zenbakiz zatigarria da, beraz a zenbakia, m moduluarekiko δ berretzaileari baldin badagokio, δ k $\varphi(m)$ zenbakiaren zatitzailea izan behar du. $\varphi(m)$ bera ere $\varphi(m)$ ren zatitzailea da eta gainera handiena.

Definizioa

$\varphi(m)$ berretzaileari dagozkion zenbakiak (existitzen ba dira), m moduluarekiko erro primitiboak deitzen dira.

2. p^{α} ETA $2p^{\alpha}$ MODULUAREKIKO ERRO PRIMITIBOAK.

Biz p , zenbaki primo ezpare bat eta $\alpha \geq 1$

Teorema

x zenbakia, m moduluarekiko ab berretzaileari baldin badagokio, x^{a} b berretzaileari dagokio.

Frogapena:

Demagun x^a, δ berretzaileari dagokiola, orduan:

$$(x^a)^\delta \equiv 1 \pmod{m} \Rightarrow x^{a\delta} \equiv 1 \pmod{m}.$$

Beraz, a δ ab zenbakiz zatigarria da, halabeharrez δ, b zenbakiz zatigarria izango da, hots: b/δ. Gainera:

$$x^{ab} \equiv 1 \pmod{m} \Rightarrow (x^a)^b \equiv 1 \pmod{m}$$

hots, b, δ zenbakiz zatigarria da: $/b$

Honela, zera dugu: b/δ eta $\delta/b \Rightarrow \delta = b$

Teorema

m moduluarekiko, x zenbakia a berretzaileari eta y zenbakia, b berretzaileari baldin badagozkie, non $(a,b) = 1$ baita, orduan xy zenbakia ab berretzaileari dagokio.

Frogapena:

Demagun xy, δ berretzaileari dagokiola, hots:

$$(xy)^\delta \equiv 1 \pmod{m}$$ eta hemendik:

$$x^{b\delta} y^{b\delta} \equiv 1 \pmod{m}$$ $(y^{b\delta} \equiv 1$ denez $) \Rightarrow x^{b\delta} \equiv 1 \pmod{m}$

orduan $b\delta$, a zenbakiz zatigarria da eta $(a,b) = 1$ denez δ, a zenbakiz zatigarria izango da.

Era berean, δ, b zenbakiz zatigarria dela frogatzera heltzen gara.

a/δ eta b/δ, bestetik $(a,b) = 1$ ab/δ

Gainera:

$$(xy)^{ab} \equiv 1 \pmod{m}$$

ab, δ zenbakiz zatigarria da eta honela hau dugu:

ab/δ eta $\delta/ab \Rightarrow \delta = ab$.

Teorema

p moduluarekiko erro primitiboak existitzen dira.

Frogapena:

Demagun 1, 2,..... p-1 zenbakiek, m moduluarekiko berretzaile ezberdinei dagozkiela

Biz $\mathcal{N} = [\delta_1, \delta_2 \ldots \delta_r]$ non $\mathcal{N} = g_1^{\alpha_1} g_2^{\alpha_2} \ldots\ldots g_k^{\alpha_k}$ bere deskonposaketa kanonikoa baita.

Hohela izanik, $g_s^{\alpha_s}$ deskonposaketaren elementu bakoitzak, gu-

txienez δ_j zenbakiren bat zatitu behar du. Beraz:

$$\delta_j = a g_s^{\alpha_s}$$

Biz ξ_j, 1, 2,.....p - 1 suzezioaren zenbaki bat, non ξ_j , δ_j berretzaileari baitagokio.

Lehen ikusi dugunez $\eta_j = \xi_j^{a}$, $g_s^{\alpha_s}$ berretzaileari dagokioke eta $g = \eta_1 \eta_2 \cdots \eta_k$, $\tau = g_1^{\alpha_1} g_2^{\alpha_2} \cdots g_\kappa^{\alpha_\kappa}$ berretzaileari dagokioke.

$\forall j = 1, 2.....r, \delta_j$ τ zenbakia zatitzen duenez, 1, 2.....p - 1 zenbakiak $x^\tau \equiv 1$ (p mod.) kongruentziaren soluzioak izango dira:

$$\forall \xi_j \in 1, 2.....p-1 \;,\; \exists \delta_j \ni \xi_j^{\delta_j} \equiv 1 \quad (\text{p mod.})$$

$$\delta_j / \tau \Rightarrow \quad \tau = k\delta_j \Rightarrow \xi_j^{\tau} = ((\xi_j)^{\delta_j})^{\kappa} \equiv 1 \quad (\text{p mod.})$$

Bestetik, eta aurreko gaian ikusi dugunez, zera izan behar dugu:

$$p - 1 \leq \tau$$

Baina τ k , $p - 1 = \varphi(p)$ zenbakia zatitu behar du, orduan:

$$\tau = p - 1 = \varphi(p).$$

Lehen frogatu dugunez $g = \eta_1 \eta_2 \cdots \eta_\kappa$ zenbakia, $\tau = \varphi(p)$ berretzaileari dagokio, hots, g zenbakia p moduluarekiko erro primitibo bat da.

Teorema

Biz, p moduluarekiko erro primitibo bat: g . Hemendik t zenbaki bat determina dezakegu, non $(g + pt)^{p-1} = 1 + pu$ berdintzaz definiturik gelditzen den u zenbakia ez baita p moduluz zatigarria.

Gainera, edozein $\alpha > 1$ zenbakirentzat, g + pt zenbakia p^α moduluarekiko erro primitiboa da.

Frogapena:

g, p moduluarekiko erro primitiboa denez:

$$g^{\varphi(p)} \equiv 1 \quad (\text{p mod.}) \iff g^{p-1} \equiv 1 \quad (\text{p mod.}) \iff$$

$$\exists\, t_o \ni g^{p-1} = 1 + pt_o \qquad (1)$$

$$(g + pt)^{p-1} = 1 + p(t_o + g^{p-2}t + pt) = 1 + pu \qquad (2)$$

non t eta u zenbakiek, p moduluarekiko hondar sistema osoa kurritzen baitute. Beraz, posible da t zenbaki bat determinatzea bertan, u zenbakia p moduluz zatigarria ez delarik.

gainera t zenbaki honentzat:

$$\left.\begin{array}{l} (g + pt)^{p^{\alpha-1}(p-1)} \equiv (1 + pu)^{p} = 1 + p^{2}u_{2} \\ (g + pt)^{p^{2}(p-1)} \equiv (1 + p^{2}u_{2})^{p} = 1 + p^{3}u_{3} \\ - \; - \; - \; - \; - \; - \; - \; - \; - \; - \; - \; - \; - \\ - \; - \; - \; - \; - \; - \; - \; - \; - \; - \; - \; - \; - \end{array}\right\}$$

non u_2, u_3, ... ez baitira p moduluz zatigarriak.

Demagun $g + pt$ zenbakia, p^{α} moduluarekiko δ berretzaileari dagokiola. Beraz:

$$(g + pt)^{\delta} \equiv 1 \quad (p^{\alpha} \text{mod.}) \Rightarrow (g + pt)^{\delta} \equiv 1 \quad (p \text{ mod.})$$
$$\Rightarrow \; p - 1/\delta \Rightarrow \delta = k (p - 1).$$

Bestetik δ zenbakiak $\varphi(p^{\alpha}) = p^{\alpha-1}(p - 1)$ zatitzen du $\Rightarrow$

$\delta = p^{r-1}(p - 1)$ non $r = \{ 1, 2, \ldots\ldots \alpha \}$ baita

$(g + pt)^{\delta} = (g + pt)^{p^{r-1}(p-1)} \equiv 1 + p^{r}u_{r} \equiv 1 \quad (p^{\alpha} \text{mod.})$

$p^{r}u_{r} \equiv 0 \quad (p \text{ mod.}) \Rightarrow p^{r} \equiv 0 \quad (p^{\alpha} \text{mod.}) \Rightarrow r = \alpha \Rightarrow$

$\delta = \varphi(p^{\alpha})$.

Orduan, $g + pt$ zenbakia, p^{α} moduluarekiko erro primitiboa izango da.

Teorema

Biz g_1, p^{α} moduluarekiko erro primitiboa. Orduan g_1, $g_1 + p^{\alpha}$ zenbakien arteko ezparea dena, $2p^{\alpha}$ moduluarekiko erro primitiboa da. $(\alpha \geq 1)$

Frogapena:

Bistakoa da, zenbaki ezpare batek kongruentzia baustariko bat betetzen badu, bestea ere bete behar duela:

$$x^{\nu} \equiv 1 \quad (p^{\alpha} \text{mod.}) \qquad x^{\nu} \equiv 1 \quad (2p^{\alpha} \text{mod.})$$

$\varphi(p^{\alpha}) = \varphi(2p^{\alpha})$ da, zeren

$\varphi(2p^{\alpha}) = \varphi(2)\,\varphi(p^{\alpha}) = \varphi(p^{\alpha})$

Beraz, zenbaki ezpare bat p^{α} moduluarekiko erro primitiboa bada, $2p^{\alpha}$ moduluarekiko erro primitiboa izango da, eta alderantziz.

Derrigorrez, g_1 eta $g_1 + p$ zenbakien artean bata parea eta bestea ezparea izan behar dute. Honegatik ezparea den zenbakia $2p^{\alpha}$ moduluarekiko erro primitiboa izango da.

Teorema

Bira $c = \varphi(m)$ eta $g_1, g_2 \ldots\ldots g_\kappa$, c zenbakiaren zatitzaile primo ezberdin guztiak. Biz g zenbakia non $(g, m) = 1$ baita. Orduan, g m moduluarekiko erro primitiboa da baldin eta soilik baldin kongruentzia hauetarik ez baditu bat ere betetzen.

$$g^{\frac{c}{q_1}} \equiv 1 \quad (m \text{ mod.}) \qquad g^{\frac{c}{q_2}} \equiv 1 \quad (m \text{ mod.}) \ldots\ldots\ldots$$

$$\ldots\ldots\ldots \quad g^{\frac{c}{q_\kappa}} \equiv 1 \quad (m \text{ mod.})$$

Frogapena:

g_j m moduluarekiko erro primitiboa denez, c berretzaileari dagokio eta honegatik aurreko kongruentziarik ezin dira bete, zeren eta:

$$c/g_j \leq c \qquad \forall\, j = 1, \ldots\ldots k \text{ baita}$$

Demagun orain aurreko kongruentziarik ez direla betetzen eta g zenbakia δ berretzaileari dagokiola.

Demagun, halaber $\delta < c$ dela.

Biz g, c/δ zenbakiaren zatitzaile primo bat:

$$c/\delta = gu \Rightarrow c/g = u\,\delta \Rightarrow g^{\frac{\delta}{q}} \equiv g^{u\delta} \equiv 1 \quad (p \text{ mod.})$$

$g^{\frac{c}{q}} \equiv 1$ (m mod.) eta hau eman dugunaren aurka dago

$\Rightarrow \quad c = \delta$

Beraz, g zenbakia, m moduluarekiko erro primitiboa da.

1. Adibidea

Biz $m = 41 \Rightarrow \varphi(41) = 40 = 2^3 5$

40 zenbakiaren zatitzaile primoak 5 eta 2 dira, gainera

$$40/5 = 8 \qquad 40/2 = 20$$

Orduan, g zenbakia non $(g, 41) = 1$ baita, 41 moduluarekiko erro primitiboa izango da baldin eta soilik baldin, g zenbakiak ez baditu ondoko kongruentziak betetzen:

$$g^8 \equiv 1 \quad (41 \text{ mod.}), \qquad g^{20} \equiv 1 \quad (41 \text{ mod.})$$

Froga dezagun ea 2,3,4,5,6..... zenbakiek betetzen duten ala ez aurreko kongruentziak

$$2^8 \equiv 10 \quad (41 \text{ mod.}) \qquad 3^8 \equiv 1 \quad (41 \text{ mod.}) \qquad 4^8 = 18 \quad (41 \text{ mod})$$

$2^{20} \equiv 1 \pmod{41}$ $\qquad$ $4^{20} \equiv 1 \pmod{41}$

$5^{8} \equiv 18 \pmod{41}$ $\qquad$ $6^{8} \equiv 10 \pmod{41}$

$5^{20} \equiv 1 \pmod{41}$ $\qquad$ $6^{20} \equiv 40 \pmod{41}$

Dakusagunez 2,3,4,5 zenbakiek ez dira erro primitiboak (41 mod) zeren eta kongruentzia bietatik, gutxienez bat betetzen baitute. Aldiz, 6 zenbakia erro primitiboa da, zeren ez baititu betetzen kongruentzia bietatik bat ere.

2. Adibidea

Biz: $m = 1681 = 41^2$.

6 zenbakia, 41 moduluarekiko erro primitiboa denez, honela idatz dezakegu:

$$6^{40} = 1 + 41\,(3 + 41p)$$

$$(6 + 41t)^{40} = 1 + 41\,(3 + 41p + 6^{39}t + 41t) = 1 + 41u.$$

u zenbakia, 41 zenbakiz zatigarria izan ez dadin, nahikoa zaigu $t = 0$ hartzea.

Beraz eta aurreko teoremaz: $6 + 41.0 = 6$ zenbakia, 1681 moduluarekiko erro primitiboa izango da.

3. Adibidea

Biz: 3362 = 2.1681 zenbakia.

Lehen frogatu dugunez eta 6 zenbakia, 1681 moduluarekiko erro primitiboa denez, 3362 moduluarekiko erro primitibotzat har dezakegu, hain zuzen, 6 eta 6 + 1681 zenbakien arteko ezparea dena, hots, 1687 zenbakia.

3. p^{α} ETA $2p^{\alpha}$ MODULUAREKIKO INDIZEAK.

Demagun, p zenbaki primo ezpare bat dela. $\alpha \geq 1$ $m = p^{\alpha}$ edo $2p^{\alpha}$, $c = \varphi(m)$, eta g m moduluarekiko erro primitiboa izanik.

Teorema

ν zenbakiak, $\nu = 0,1,\ldots\ldots c-1$, c moduluarekiko hondar mi-

nimo negatiboak kurritzen baditu, orduan g zenbakiak m moduluarekiko hondar sistema laburtua kurrituko du.

Frogapena:

g , m moduluarekiko primoak diren c zenbaki kurritzen ditu, gainera eta lehen ikusi dugunez zenbaki hauk ez dira m moduluarekiko kongruenteak, hots, hondar sistema laburtu bat osotzen dute.

Definiziioa

Biz a , m zenbakiarekiko primo den zenbaki bat: $(a, m) = 1$ $a \equiv g^{\nu} \pmod{m}$ kongruentzia ematen bada (non $\nu \geq 0$ baita) ν zenbakia, m moduluarekiko a zenbakiaren g oinarrizko indizea dela esaten da, eta honela idatzi:

$$\nu = \text{ind}_g . a \qquad \text{edo} \qquad \nu = \text{ind}. a$$

Har dezagun kontutan, indize eta logaritmoaren kontzeptuak paraleloak direla eta gure kasuan erro primitiboak, logaritmoaren oinarriak betetzen duen paper berdintsua betetzen duela.

Aurreko teoreman ikusi dugunez, edozein zenbaki primorentzat: a $0,1, \ldots, c-1$ zenbaki artean indize bakar bat existitzen da.

ν indizea ezagutuz gero, a zenbakiaren indize guztiak determina ditzakegu ondoko adierazpenaren bidez:

$$\nu \equiv \nu' \pmod{c}$$

ν indize bera duten zenbaki guztiek, m moduluarekiko klase bat osotzen dute.

Teorema

$$\text{ind}. a.b.\ldots.p \equiv \text{ind}.a + \text{ind}.b + \ldots\ldots + \text{ind}.p \pmod{c}$$

Bereziki:

$$\text{ind}. a^n \equiv n.\text{ind}. a \pmod{c}$$

Frogapena:

Bira:

$$a \equiv g^{ind.a} \pmod{m} \quad , \quad b \equiv g^{ind.b} \pmod{m} \quad \ldots\ldots\ldots$$

$$\ldots\ldots\ldots\ldots \quad p \equiv g^{ind.p} \pmod{m}$$

hau guztia biderkatuz:

$$a.b.\ldots\ldots\ldots p \equiv g^{ind.a + ind.b + \ldots + ind.p} \pmod{m} \quad \text{hots'}$$

$$\text{ind}. a.b.\ldots\ldots\ldots p \equiv \text{ind}. a + \text{ind}. b + \ldots\ldots + \text{ind}. p \pmod{c}$$

Indize taulak

Bi taula moeta egin dezakegu; bata edozein zenbakirentzat indizea ezagutzeko, eta bestea indizea ezagutuz, zeintzu diren indize honi dagozkion zenbakiak jakiteko.

Dakusagun hau adibide baten bidez.

Har dezagun $m = 41$ modulua. Lehen ikusi dugunez 6 zenbakia modulu honekiko erro primitiboa da eta honegatik oinarritzat har dezakegu.

Honela ba, idatz ditzagun:

$6^0 \equiv 1$	$6^8 \equiv 10$	$6^{16} \equiv 18$	$6^{24} \equiv 16$	$6^{32} \equiv 37$
$6^1 \equiv 6$	$6^9 \equiv 19$	$6^{17} \equiv 26$	$6^{25} \equiv 14$	$6^{33} \equiv 17$
$6^2 \equiv 36$	$6^{10} \equiv 32$	$6^{18} \equiv 33$	$6^{26} \equiv 2$	$6^{34} \equiv 20$
$6^3 \equiv 11$	$6^{11} \equiv 28$	$6^{19} \equiv 34$	$6^{27} \equiv 12$	$6^{35} \equiv 38$
$6^4 \equiv 25$	$6^{12} \equiv 4$	$6^{20} \equiv 40$	$6^{28} \equiv 31$	$6^{36} \equiv 23$
$6^5 \equiv 27$	$6^{13} \equiv 24$	$6^{21} \equiv 35$	$6^{29} \equiv 22$	$6^{37} \equiv 15$
$6^6 \equiv 39$	$6^{14} \equiv 21$	$6^{22} \equiv 5$	$6^{30} \equiv 9$	$6^{38} \equiv 8$
$6^7 \equiv 29$	$6^{15} \equiv 3$	$6^{23} \equiv 30$	$6^{31} \equiv 13$	$6^{39} \equiv 7$

N	0	1	2	3	4	5	6	7	8	9
0		0	26	15	12	22	1	39	38	30
1	8	3	27	31	25	37	24	33	16	9
2	34	14	29	36	13	[4]	17	5	11	7
3	23	28	10	18	19	21	2	32	35	6
4	20									

I	0	1	2	3	4	5	6	7	8	9
0	1	6	36	11	25	27	39	29	10	19
1	32	28	4	24	21	3	18	26	33	34
2	40	35	5	30	16	14	2	12	31	22
3	9	13	37	[17]	20	38	23	15	8	7

Lehen taula, zenbakiaren indizea ezagutzeko da eta 2.a zenbakia ezagutzeko. Lerroaren zenbakiak, hamarkadak ematen dizkigu eta

sutabearen zenbakiek unitateak.

Adibidez, 25 zenbakiaren indizea ezagutu nahi dugu:Har dezagun horretarako lerroetatik 3.a eta sutabeetatik 6.a. 4 zenbakia lortzen dugu, beraz:

ind. 25 = 4

Beste taula era berean erabiliko dugu: Zein zenbakik du 33 indizetzat ? Har dezagun hau jakiteko 4. lerroa eta 4. sutabea:

33 = ind. 17

4. AURREKO TEORIAREN ONDORIO BATZU.

Bira p zenbaki primo ezpare bat, $\alpha \geq 1$ $m = p^{\alpha}$ edo $2p^{\alpha}$ eta $c = \varphi(m)$. Biz $(n, c) = d$

Teorema

$x^n \equiv a \pmod{m}$ (1) kongruentziak soluzioa du baldin eta soilik baldin ind. a d zenbakiaren multiploa bada. Gainera, kongruentzia honek soluzio bat badu, orduan d soluzio ditu.

Frogapena:

(1) kongruentzia ondorengoarekin baliokidea da:

$n.\text{ind. } x \equiv \text{ind. } a \pmod{c}$ (2)

eta badakigu kongruentzia honek soluzioa duela baldin eta soilik baldin, ind. a d zenbakiaren multiploa denean.

(2) kongruentziak soluzioa badu, ind. x aldagaiarentzat, c moduluarekiko ezkongruenteak diren d zenbaki lortzen ditugu eta hauei dagozkie, x aldagaiarentzat, m moduluarekiko ezkongruenteak diren d zenbaki.

Teorema

m moduluarekiko hondar sistema laburtuan, n graduko c/d hondarrak daude.

Frogapena:

0,1..... c - 1 zenbakiak, sistema laburraren, hondarren indize minimoak dira, eta hauen artean d zenbakiaren c/d multiploak daude.

1. Adibidea

Biz $x^{8} \equiv 23 \pmod{41}$

$(8, 40) = 8$ eta ind. 23 = 36

36, 8 zenbakiz zatigarria denez, emandako kongruentziak ez du soluziorik.

2. Adibidea

Biz $x^{12} \equiv 37 \pmod{41}$

$(12, 40) = 4$ eta ind. 37 = 32

32, 4 zenbakiz zatigarria da, beraz aurreko kongruentziak 4 soluzio ditu. Aurki ditzagun soluzio hauk:

$x^{12} \equiv 37 \pmod{41}$

$12.\text{ind. } x \equiv \text{ind. } 37 \pmod{40}$

$12.\text{ind. } x \equiv 32 \pmod{40}$

$\text{ind. } x \equiv 6 \pmod{10}$

ind. x = 6,16,26,36 eta taulan begiraturik:

$x \equiv 39,18,2,23. \pmod{41}$

3. Adibidea

1,4,10,16,18,23,25,31,37,40 zenbakien indizeak, 4 zenbakiaren multiploak dira, horregatik zenbaki hauk hondar bikoadratiko guztiak (edo n graduko hondarrak non $(n, 40) = 4$ baita) dira. 41 moduluarekiko. Eta 40/4 = 10 zenbaki dugu.

Teorema

a zenbakia, m moduluarekiko n graduko hondarra da, baldin eta soilik baldin:

$a^{\frac{c}{d}} \equiv 1 \pmod{m}$ bada

Frogapena:

Lehen, teorema baten ikusi dugunez a zenbakia n graduko hondarra da baldin eta soilik baldin:

$\text{ind. } a \equiv 0 \pmod{d} \iff c/d.\text{ind. } a \equiv 0 \pmod{c}$

(kongruentzia hauk baliokideak direlako) $\iff a^{\frac{c}{d}} \equiv 1 \pmod{m}$

Teorema

a zenbakia, m moduluarekiko, δ berretzaileari dagokio baldin eta soilik baldin:

$$(\text{ind. } a,\ c) = c/\delta \qquad \text{bada:}$$

Bereziki, a zenbakia m moduluarekiko erro primitiboa da baldin eta soilik baldin:

$$(\text{ind. } a,\ c) = 1 \qquad \text{bada.}$$

Frogapena:

a zenbakia, δ berretzaileari dagokio, hots, δ ondoko propietatea betetzen dutenetatik, $c = \varphi(m)$ zenbakiaren zatitzaile txikiena da:

$$a^{\delta} \equiv 1 \pmod{m} \iff \delta \cdot \text{ind. } a \equiv 0 \pmod{c}$$ hots:

$$\text{ind. } a \equiv 0 \pmod{c/\delta}$$

Beraz, δ berretzailea c/δ, ind. a zenbakiaren zatitzaile bihurtzen duten c zenbakiaren zatitzaile guztietatik txikiena da, hots, c/δ, c zenbakiaren zatitzaile handiena da, non c/δ k, ind. a zenbakia zatitzen baitu, hots:

$$c/\delta = (\text{ind. } a,\ c).$$

Bigarren partea derrigorrezkoa da, zeren eta:

$$c/\delta = c/\varphi(m) = 1 \qquad \text{baita.}$$

Teorema

m moduluarekiko hondar sistema laburraren, δ berretzaileari dagozkionak $\varphi(\delta)$ zenbaki dira.

Bereziki $\varphi(c)$ erro primitiboak izango ditugu.

Frogapena:

Har ditzagun m moduluarekiko hondar sistema laburraren indize minimoak: 0,1..... c - 1

Zenbaki hauen artean, zeintzu dira c/δ zenbakiaren multiploak ? Erraz ikus daiteke $c/\delta .y$ eratako zenbakiak direla, non $y = 0,1..... \delta - 1$ baita. Eta honela zera dugu:

$$(c/\delta .y,\ c) = c/\delta \iff (y, \delta) = 1.$$

Azkeneko baldintza hau $\varphi(\delta)$ zenbakiek betetzen dute eta hemendik frogatu nahi genuena.

1. Adibidea

41 moduluarekiko hondar sistema laburraren, 10 berretzaileari dagozkionak, ondoko baldintza betetzen dutenak izango dira:

$$(\text{ind. } a,\ 40) = 40/10 = 4$$

esate baterako: 4,23,25,31 zenbakiak dira. Guztiz $4 = \varphi(10)$ zenbaki ditugu.

2. Adibidea

41 moduluarekiko hondar sistema laburraren erro primitiboak honela determinaturik gelditzen dira:

$$(\text{ind. } a,\ 40) = 1$$, hots,

6,7,11,12,13,15,17,19,22,24,26,28,29,30,34,35 zenbakiak.

Beraz $16 = \varphi(40)$ erro primitibo dugu.

2^{α} Moduluarekiko indizeak

Azter dezagun $m = 2^{\alpha}$ kasu berezia.

- Biz $\alpha = 1 \Rightarrow 2^{\alpha} = 2 \wedge \varphi(2) = 1$

  - 1 zenbakia, 2 moduluarekiko erro primitiboa da:

    $$-1 \equiv 1 \pmod 2$$

  $1^{\circ} = (-1)^{\circ} = 1$ zenbakiak, 2 moduluarekiko hondar sistema laburra osotzen du.

- Biz $\alpha = 2 \Rightarrow 2^{\alpha} = 4 \wedge \varphi(4) = 2$

  $3 \equiv -1 \pmod 4$ erro primitiboa da, eta

  $(-1)^{\circ} = 1$, $(-1)^{1} \equiv 3 \pmod 4$ zenbakiek hondar sistema laburra osotzen dute.

- Biz $\alpha \geq 3 \Rightarrow 2^{\alpha} \geq 8 \wedge \varphi(2^{\alpha}) = 2^{\alpha-1}$

  Ikus dezagun, nola kasu honetan ez diren erro primitiboak existitzen eta nola zenbaki ezpare batek berretzaileari baldin badagokio, orduan:

  $$2^{\alpha-2} = 1/2.\ \varphi(2^{\alpha}).$$

  Biz x zenbaki ezparea:

  $$x = 1 + 2t$$
  $$x^{2} = 1 + 4t$$
  $$x^{4} = 1 + 8t$$
  $$- \quad - \quad - \quad -$$

$x^{2^{\alpha-2}} = 1 + 2^{\alpha} t_{\alpha-2} \equiv 1 \quad (2^{\alpha} \text{ mod. })$

Demagun halaber, nola $2^{\alpha-2}$ berretzaileari dagozkion zenbakiak existitzen direla, esate baterako 5 zenbakia:

$5 = 1 + 4$

$5^2 = 1 + 8 + 16$

$5^4 = 1 + 16 + 32u_2$

\- - - - - -

\- - - - - -

$5^{2^{\alpha-3}} = 1 + 2^{\alpha-1} + 2^{\alpha} u_{\alpha-3}$

Dakusagunez, $5^1, 5^2, \ldots\ldots 5^{2^{\alpha-3}}$ ez dira 2^{α} moduluarekiko kongruenteak.

Erraz ikus daiteke:

$5^0 , 5^1 , \ldots\ldots 5^{2^{\alpha-2}-1}$

$-5^0 , -5^1 \ldots\ldots -5^{2^{\alpha-2}-1}$

zenbakiek, 2^{α} moduluarekiko hondar sistema laburra osotzen dutela. Izan ere: $2.2^{\alpha-2} = \varphi(2^{\alpha})$ zenbaki dugu, lerro bakoitzeko zenbakiak 2^{α} moduluarekiko ezkongruenteak dira beren artean eta goiko lerrokoak, era berean, behekoekin ezkongruenteak dira.

Hemendik aurrera, honela idatziko dugu:

$c = 1, \quad c_0 = 1, \quad \alpha = 0$ edo $\alpha = 1$ bada

$c = 2, \quad c_0 = 2^{\alpha-2} \quad \alpha \geq 2$ bada.

beraz, beti dugu: $c.c_0 = \varphi(2^{\alpha})$

Demagun ν eta ν_0 zenbakiek, nork berea, c eta c_0 moduluarekiko, $\nu = 0, \ldots\ldots c - 1$; $\nu_0 = 0, \ldots\ldots c_0 - 1$ hondar minimo positiboak kurritzen dituztela.

Orduan, $(-1)^{\nu}.5^{\nu_0}k$, 2^{α} moduluarekiko hondar sistema laburra kurritzen du.

Teorema

$(-1)^{\nu}.5^{\nu_0} \equiv (-1)^{\nu'}.5^{\nu_0'} \quad (2^{\alpha} \text{mod. }) \iff$

$\nu \equiv \nu' \quad (c \text{ mod. })$ eta $\nu_0 \equiv \nu_0' \quad (c_0 \text{mod. })$.

Frogapena:

$\alpha = 0$ kasuan begi bistakoa da, orduan demagun $\alpha > 0$

Bira r eta r_0, c eta c_0 moduluekiko ν eta ν_0 zenbakien hondar minimo positiboak eta r', r_0' ν' eta ν_0' zenbakienenak

Orduan:

$$(-1)^{\nu}.5^{\nu_0} \equiv (-1)^{\nu'}.5^{\nu'_0} \ (2^{\alpha} \text{mod.}) \iff$$

$$(-1)^{r}.5^{r_0} \equiv (-1)^{r'}.5^{r'_0} \ (2^{\alpha} \text{mod.}), \text{ hots,}$$

$r = r'$ eta $r_0 = r'_0$.

Definizioa

$a \equiv (-1)^{\nu}.5^{\nu_0} \ (2^{\alpha} \text{mod.})$ bada, orduan ν eta ν_0 sistema 2^{α} moduluarekiko a zenbakiaren indize sistema deitzen dugu.

Propietatea

Lehen ikusi dugunez, 2^{α} zenbakiarekiko primoa den edozein a zenbakik, (derrigorrez ezparea izan behar duenak) ν' eta ν'_0 indize sistema bakar bat du, lehen aipaturiko $c.c_0 = \varphi(2^{\alpha})$ bikoteen artean.

ν', ν'_0 sistema ezagutuz, posible da a zenbakiaren indize sistema guztiak ezagutzea, eta hauk ondorengo propietatea betetzen dituzten bikote guztiak izango dira:

$$\nu \equiv \nu' \ (c \text{ mod.}) \qquad \nu_0 \equiv \nu'_0 \ (c_0 \text{mod.}).$$

Ikusten denez, ν, ν_0 indize sistematzat duten zenbaki guztiek 2^{α} moduluarekiko zenbaki klase bat osotzen dute.

Teorema

Biderketaren indizeak, c eta c_0 moduluekiko, faktoreen indizeen batuketaz kongruenteak dira.

Frogapena:

Bira: $\nu(a), \nu_0(a); \ldots\ldots\ldots \nu(p), \nu_0(p)$

a..... p zenbakien indize sistemak.

Zera dugu:

$$a \ldots\ldots p \equiv (-1)^{\nu(a)+\ldots+\nu(p)} . 5^{\nu_0(a)+\ldots+\nu_0(p)}.$$

beraz, $\nu(a) + \ldots\ldots + \nu(p)$ eta $\nu_0(a) + \ldots\ldots \nu_0(p)$ a..... p biderketaren indizeak dira.

4. EDOZEIN MODULU KONPOSATUREKIKO INDIZEAK

Biz $m = 2^{\alpha} p_1^{\alpha_1} p_2^{\alpha_2} \ldots\ldots\ldots p_k^{\alpha_k}$, m zenbakiaren deskonposaketa

kanonikoa.

Bira c eta c_o aurrean definitutako zenbakiak, $c_s = \varphi(p_s^{\alpha_s})$ eta g_s, p^{α_s} moduluarekiko erro primitibo txikiena.

Definizioa

$a \equiv (-1)^{\nu} \cdot 5^{\nu_o} \pmod{2^{\alpha}}$

$a \equiv g_1^{\nu_1} \pmod{p_1^{\alpha_1}} \ldots\ldots\ldots\ldots a \equiv g_k^{\nu_k} \pmod{p_k^{\alpha_k}}$

hau guztia gertatzen bada, $\nu, \nu_o, \nu_1 \ldots \nu_k$ sistema, m moduluarekiko a zenbakiaren indize sistema deitzen da

Definizioaren ondorioa

Definizioaren bidez, ba dakusagu ν, ν_o 2^{α} moduluarekiko a zenbakiaren indize sistema dela, bai eta $\nu_1 \ldots \nu_k$ zenbakiak, $p_1^{\alpha_1} \ldots\ldots\ldots p_k^{\alpha_k}$ moduluekiko a zenbakiaren indizeak direla ere.

Arrazoi honegatik, m zenbakiarekiko, primoa den edozein a zenbakik, indize sistema bakar bat izango du: $\nu', \nu_o' \ldots \nu_k'$

a zenbakiaren: $\nu, \nu_o, \nu_1 \ldots \nu_k$ indize sistema guztiak honela lortzen ditugu:

$\nu \equiv \nu' \pmod{c}$, $\nu_o \equiv \nu_o' \pmod{c_o}$

$\nu_1 \equiv \nu_1' \pmod{c_1} \ldots\ldots\ldots \nu_k \equiv \nu_k' \pmod{c_k}$

Beraz, $\nu, \nu_o \ldots \nu_k$ indize sistema berbera duten zenbaki guztiek, m moduluarekiko zenbaki klase bat osotzen dute

Teorema

$c, c_o, c_1 \ldots\ldots\ldots c_k$ moduluekiko, biderketaren indizeak, faktoreen indizeen batuketaz kongruenteak dira.

Frogapena:

m moduluarekiko $\nu, \nu_o \ldots \nu_k$ a zenbakiaren indizeak eta 2^{α}, $p_1^{\alpha_1}, \ldots\ldots\ldots p_k^{\alpha_k}$ moduluekiko a zenbakiaren indizeak berdinak dira eta hemendik nahi genuena

Ondorio garrantsitsua

Biz: $\tau = \varphi(2^{\alpha})$ $\alpha \leq 2$ bada, eta

$\tau = 1/2\ \varphi(2^{\alpha})$ $\alpha > 2$ bada.

Biz $h = [\tau, c_1, \ldots\ldots c_k]$

m zenbakiarekiko, primoa den edozein a zenbakik ondoko kongruentzia betetzen du:

$a^h \equiv 1$ eta hau 2^{α}, $p_1^{\alpha_1} \ldots\ldots p_k^{\alpha_k}$ modulu guztiekiko.

Beraz, a zenbakia ezin daiteke m moduluarekiko erro primitiboa izan, $h < \varphi(m)$ bada.

Baina hau $\alpha \geq 2$ eta $K \geq 1$ denean gertatzen da, beraz $m > 1$ bada, bakar bakarrik $m = 2,4,p_1^{\alpha_1},2p_1^{\alpha_1}$ denean existitzen dira erro primitiboak.

Gaiaren lehen zatian frogatu dugunez, kasu hauetan beti existitzen dira erro primitiboak.

Honela ba, zera esan dezakegu, $m > 1$ bada, m moduluarekiko erro primitiboak existitzen dira baldin eta soilik baldin $m = 2,4,p^{\alpha},2p^{\alpha}$ bada.

HIZTEGIA

Euskara-gaztelania:

aldagai.....variable

alderantzizko.....inverso

askaketa.....resolución

askagarritasun.....resolubilidad

askagarritasun baldintzak.....condiciones de resolubilidad

askatu.....resolver

atal.....miembro

azpiindize.....subindice

baldin eta soilik baldin.....si y solo si

balio.....valor

baliokide.....equivalente

bali kidetasun.....equivalencia

berretzaile.....exponente

berrekadur hondar.....resto potencial

bete.....verificar

binan binan primuak.....primos entre sí

binan binan inkongruenteak.....incongruentes entre sí

bsb.....sii

deskonposaketa.....descomposición

deskonposaketa kanoniko.....descomposición canónica

elkartu (elementu elkartuak).....asociado (elementos asociados)

eraztun.....anillo

eraztun trukakor.....anillo conmutativo

eratorpen.....recurrencia

Euler-en funtzio.....función de Euler

exaktuki.....exactamente

elkarrekikotasun.....reciprocidad

erresultatu.....resutado

erro.....raiz

erro primitibo.....raiz primitiva

ez-baterakoi.....incompatible

ez-hondar.....no-resto

faktore.....factor

f.n.l.g. .....c.q.d.

forma lineala.....forma lineal

funtzio multiplikatibo.....función multiplicativa

gai.....término

gai independiente.....término independiente

g aiz gai.....término a término

gainezko, kongruentzia.....superflua, congruencia

gorputz abeliarra.....cuerpo abeliano

gradu.....grado

holabeharrez.....necesariamente

hamarkada.....decena

hondar.....resto

hondar klase.....clase de restos

hondar-sistema laburtu.....sistema reducido de restos

hondar-sistema labur.....sistema reducido de restos

hondar-sistema osoa.....sistema completo de restos

indize.....índice

indize-sistema.....sistema de índices

indize taula.....tabla de índices

inkognita.....incógnita

inkongruente.....incongruente

integritate eremu.....dominio de integridad

izendatzaile.....denominador

koadratiko.....cuadrático/a

kongruente.....congruente

kongruentzia.....congruencia

kongruentzi-sistema.....sistema de congruencias

kopuru.....cantidad

korrespondentzia.....correspondencia

kunplitu.....verificar, cumplir

kuritu.....recorrer

laburtu.....simplificar

laburtezin.....irreducible

lagro.

lerro.....fila

M-ren faktore primuetango deskonposaketa.....descomposición de M en factores primos

Möbius-en funtzio.....función de Möbius

modulu.....módulo

multiplo, zenbaki baten.....múltiplo, de un número

multiplikatibo.....multiplicativo/a

polinomio.....polimomio

primario.....primario

primu.....primo

soluzio.....solución

soluzio orokor.....solución general

talde.....grupo

talde trukakor.....grupo conmutativo

talde multiplikatibo.....grupo multiplicativo

unitate.....unidad

x en parte osoa.....parte entera de x

x en parte frakzionari.....parte fraccionaria de x

x en parte zatitzaile.....parte fraccionaria de x

zatidura multzo.....conjunto cociente

zatigarri.....divisible

zatitzaile.....divisor

zenbaki-bikote.....par de números

zenbakitzaile.....numerador

zeroren zatitzaile.....divisor de cero

zutabe.....columna

Gaztelania-euskara:

anillo.....eraztun

anillo conmutativo unitario.....eraztun trukakor unitario

asociado (elementos asociados).....elkartu (elementu elkartuak)

bicuadrático.....bikoadratiko

clase de restos.....hondar klase

cantidad.....kopuru

columna.....zutabe

condiciones de resolubilidad.....askagarritasun baldintzak

congruencia.....kongruentzia

congruente.....kongruente

conjunto cociente.....zatidura-multzo

correspondencia.....korrespondentzia

c.q.d. .....f.n.g.l.

cuadrado.....karratu (zenbaki baten)

cuadrático.....koadratiko

cuerpo abeliano.....gorputz abeliarra

decena.....hamarkada

denominador .....izendatzaile

descomposición.....deskonposaketa

descomposición canónica.....deskonposaketa kanonik

descomposición de M en factores primos.....M-ren faktore primu-tango deskonposaketa

divisible.....zatigarri

divisor.....zatitzaile

divisores de cero.....zeroren zatitzaileak

dominio de integridad.....integritate eremu

equivalencia.....baliokidetasun

equivalente.....baliokide

exactamente.....exaktuki

exponente.....berretzaile

factor.....faktore

fila.....lerro

forma lineal.....forma lineale

función de Möbius.....Möbius-en funtzioa

función de Euler.....Euler-en funtzioa

función multiplicativa.....funtzio multiplikatibo

grado.....gradu

grupo.....talde

grupo conmutativo.....talde trukakor

grupo multiplicativo.....talde multiplikatibo

impar.....bakoiti, ezpare

incógnita.....inkognita

incompatible.....ez-bateragarri

incongruente.....inkongruente, ezkongruente

incongruentes entre sí.....binen binan inkongruenteak, bata bestearekiko inkongruenteak

índice.....indize

inverso.....alderantzizko, inbertsu

irreducible.....laburtezin, irreduzible

miembro a miembro.....gaiz gai, atalez atal

módulo.....modulu

múltiplo, de un número.....multiplo, zenbaki baten

multiplicativo.....multiplikatibo

negativamente.....halbeherrez

no-resto.....ez-hondar

numerador.....zenbakitzaile

par.....bikoiti, pare

parte entera de x.....x en parte osoa

parte fraccionaria de x.....x en parte frakzionari, x en parte zatitzaile

par de números.....zenbaki-bikote

polinomio.....polinomio

potencia.....berretzaile

primario.....primario

primo.....primu, primo

primos entre sí.....binan binan primuak

raiz.....erro

raizprimitiva.....erro primitibo

reciprocidad.....elkarrekikotasun

recorrer.....kurritu

recurrencia.....eratorpen

resolución.....askaketa

resolubilidad.....askagarritasun

resolver.....askatu

resto.....hondar

resto potencial.....berrekadur hondar

resultado.....erresultatu

simplificar.....laburtu

sistema completo de restos.....hondar-sistema oso

sistema reducido de restos.....hondar-sistema laburtu,
hondar-sistema labur

sistema de congruencias.....kongruentzi-sistema

sistema de índices.....indize-sistema

si y solo si.....baldin eta soilik baldin

sii.....bsb

solución.....soluzio

solución general.....soluzio orokor

subíndice.....azpiindize

superflua, congruencia.....gainezko, kongruentzia

término.....atal, gai

término independiente.....gai independentea

tabla de índices.....indize taula

unidad.....unitate

valor.....balio, balore

variable.....aldagai

verificar.....kunplitu, bete

BIBLIOGRAFIA

Algebra Moderna . Lentin Rivaud. Ed. Aguilar.

Algebra. Michel Queysanne. Collection U.

Lecciones de Algebra moderna . Dubreil. Ed. Reverté. S.A.

Fundamentos de la teoría de los números. I. Vinogradov. Ed. Mir.

Introducción a la teoría de los números. Niven y Zuckerman. Ed. Limusa.