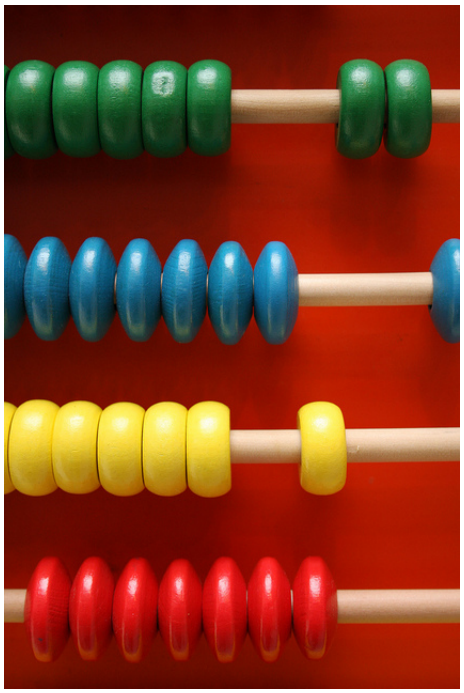
MATEMATIKARAKO SARRERA

OCW 2015



Leire Legarreta Solaguren
EHU-ko Zientzia eta Teknologia Fakultatea
Matematika Saila

5 GAIA: KONGRUENTZIAK

Kongruentziak. Zatigarritasunaren irizpideak. Kongruentzia linealak. Euler-ren ρ funtzioa. Ondarren txinatar teorema.

1 Kongruentziak

Kongruentzien lengoaiak balio digu zatigarritasunaren problemak ebazteko. Jadanik lengoai hau Gauss-ek aztertu zuen 1801. urtean Disquisitiones Arithmaticae liburuan.

Definizioa. *Izan bedi n zenbaki osoa eta positiboa. Orduan, a eta b zenbaki osoak n moduluarekiko kongruenteak direla esango dugu, eta $a \equiv b (mod\, n)$ bidez adieraziko dugu, n zenbakiagatik zatitzerakoan hondar berdina ematen baldin badute. Kasu honetan n zenbakiari, kongruentziaren modulua deitzen zaio.*

Adibideak. *Ondokoak kasu berezi batzuk dira:*

(i) *Edozein zenbaki osoa $n = 1$ zenbakiagatik zatitzerakoan 0 hondarra ematen du, hau da, zenbaki oso guztiak 1 moduluarekiko kongruenteak dira.*

(ii) *Baldin eta $n = 2$ bada, hondar posible bakarrak 0 eta 1 dira. 0 hondarra ematen dutenak, zenbaki bikoitiak dira eta 1 hondarra ematen dutenak, zenbaki bakoitiak dira.*

(iii) *Baldin eta $n = 5$ bada, $9 \equiv 19 (mod\, 5)$, $-13 \equiv 2 (mod\, 5)$ edo $5 \equiv -5 (mod\, 5)$. Orokorrean, zenbaki oso guztiak 5 klaseetan $(mod\, 5)$ bana daitezke.*

Proposizioa. *$a \equiv b (mod\, n)$ baldin eta soilik baldin $a - b$, n-ren multiploa bada.*

Froga 1.1. *Baldin eta $a \equiv b (mod\, n)$ bada, idatz dezakegu:*

$$a = q_1 n + r \quad eta \quad b = q_2 n + r \quad non\ 0 \leq r < n.$$

Aurreko adierazpen bien kenketa eginez, $a - b = (q_1 - q_2)n$ dugu, eta bukatu dugu. Alderantziz, demagun orain $a - b$, n-ren multiploa dela. Demagun gainera,

$$a = q_1 n + r_1 \quad eta \quad b = q_2 n + r_2 \quad non\ 0 \leq r_1, r_2 < n.$$

Berriro aurreko bi adierazpenen kenketa eginez, $a - b = (q_1 - q_2)n + (r_1 - r_2)$ lortzen da, eta $r_1 - r_2$ isolatuz, $r_1 - r_2 = (a - b) - (q_1 - q_2)n$, n-ren multiploa dela lortzen da. Ondorioz, r_1 eta r_2-ren definizioegatik aukera bakarra, $r_1 - r_2 = 0$ edo $r_1 = r_2$ da (nahi genuena).

Propietateak. *Izan bitez $n > 1$ zenbaki osoa eta positiboa eta a, b, c, d, k zenbaki osoak. Ondoko propietateak betetzen dira:*

(i) *Propietate erreflexiboa:* $a \equiv a (mod\ n)$.

(ii) *Propietate simetrikoa: baldin eta* $a \equiv b (mod\ n)$ *bada, orduan* $b \equiv a (mod\ n)$.

(iii) *Propietate iragankorra: baldin eta* $a \equiv b (mod\ n)$ *eta* $b \equiv c (mod\ n)$ *badira, orduan* $a \equiv c (mod\ n)$.

(iv) *Baldin eta* $a \equiv b (mod\ n)$ *eta* $c \equiv d (mod\ n)$ *badira, orduan*

$$a + c \equiv b + d (mod\ n) \quad \text{eta} \quad ac \equiv bd (mod\ n).$$

(v) *Baldin eta* $a \equiv b (mod\ n)$ *bada, orduan*

$$a \pm k \equiv b \pm k (mod\ n) \quad \text{eta} \quad ak \equiv bk (mod\ n).$$

(vi) *Baldin eta* $a \equiv b (mod\ n)$ *bada, orduan* $a^m \equiv b^m (mod\ n)$, *edozein* m *zenbaki oso positiborentzat.*

(vii) *Baldin eta* $a \equiv b (mod\ n)$ *eta* $p(x)$, x *aldagaiko eta koefiziente osoko funtzio polinomikoa bada, orduan* $p(a) \equiv p(b) (mod\ n)$.

Froga 1.2. *i), ii) eta iii) propietateak berehalakoak dira, eta horregatik "kongruentea izatea* n *moduluarekiko" baliokidetasun erlazioa da* $\mathbb{Z}$ *multzo gainean.*

iv) Baldin eta $a \equiv b (mod\ n)$ *eta* $c \equiv d (mod\ n)$ *badira, orduan* $a - b = q_1 n$ *eta* $c - d = q_2 n$. *Aurreko adierazpen biak batuz,* $(a + c) - (b + d) = (q_1 + q_2)n$ *lortzen da, eta hau,* n*-ren multiploa da, edo baliokideki* $a + c \equiv b + d (mod\ n)$. *Modu berdinean, nola* $a = b + q_1 n$ *eta* $c = d + q_2 n$ *diren, berdintza biak biderkatuz*

$$ac = (b + q_1 n)(d + q_2 n) = bd + (bq_2 + dq_1 + q_1 q_2 n)n$$

dugu, hau da, $ac - db$, n*-ren multiploa da.*

v)-a iv)-ren ondorioa da, $k \equiv k (mod\ n)$ *izateagatik. vi)-a iv)-tik ondorioztatzen da ere,* $a \equiv b (mod\ n)$ *kongruentzia beragatik biderkatzerakoan* m *aldiz. Eta vii)-a, iv), v) eta vi)-ren ondorioa da.*

Ariketa. *Kalkulatu ondoko* n *zenbakiaren hondarra* 12 *zenbakiagatik zatitzerakoan.*

$$n = 1! + 2! + 3! + \cdots + 99! + 100!.$$

Kongruentzia lengoaian, 0 *eta* 12 *artean dagoen* r *zenbaki oso bat aurkitu behar da, zeinentzat* $n \equiv r (mod\ 12)$, *hau da,* n *erreduzitu behar da* 12 *modulura. Lehenengo eta behin,* $4! = 24 \equiv 0 (mod\ 12)$, *eta ondorioz* $k \geq 4$ *bada,*

$$k! = k(k-1) \ldots 6 \cdot 5 \cdot 4! \equiv k(k-1) \ldots 6 \cdot 5 \cdot 0 \equiv 0 (mod\ 12).$$

Beraz, $n \equiv 1! + 2! + 3! (mod\ 12)$, *eta ondorioz* $n \equiv 9 (mod\ 12)$.

Ariketa. *Edozein $k \geq 1$-rako,* $7 \mid (5^{2k} + 3 \cdot 2^{5k-2})$.

$5^{2k} + 3 \cdot 2^{5k-2}$, *7-gatik zatitzerakoan hondarra* 0 *ematen duela frogatu behar da. Ondoko kongruentziak* 7 *moduluarekiko ditugu:*

$$5^{2k} + 3 \cdot 2^{5k-2} \equiv 5^{2k} + (-2^2) \cdot 2^{5k-2} \equiv 5^{2k} - 2^{5k} \equiv 25^k - 32^k (\textit{mod}\ 7),$$

$3 \equiv -2^2 (\textit{mod}\ 7)$ *izateagatik eta aurreko iv) propietatea aplikatuz. Nola* $25 \equiv 4 (\textit{mod}\ 7)$ *eta* $32 \equiv 4 (\textit{mod}\ 7)$ *diren, aurreko vi) propietatea aplikatuz,*

$$5^{2k} + 3 \cdot 2^{5k-2} \equiv 25^k - 32^k \equiv 4^k - 4^k \equiv 0 (\textit{mod}\ 7)$$

lortzen da.

Propietateak. *Baldin eta* $ak \equiv bk (\textit{mod}\ n)$ *bada, orduan* $a \equiv b (\textit{mod}\ \frac{n}{d})$, *non* $d = zkh(k, n)$ *den.*

Froga 1.3. *Nola* $d = zkh(k, n)$ *den, idatz dezakegu* $k = dk'$ *eta* $n = dn'$, *non* $zkh(k', n') = 1$ *den. Hipotesiagatik,* $ka - kb = qn$ *da,* q *zenbaki osoren batentzat. Hau da,* $dk'a - dk'b = qdn'$, *eta orain* d*-gatik zatituz,* $k'a - k'b = qn'$ *dugu. Beraz,* $n' \mid k'(a - b)$, *hau da,* $a \equiv b (\textit{mod}\ n')$.

Korolarioa. *Baldin eta* $ak \equiv bk (\textit{mod}\ n)$ *eta* k *eta* n *elkarrekiko lehenak badira, orduan* $a \equiv b (\textit{mod}\ n)$.

Korolarioa. *Baldin eta* $ak \equiv bk (\textit{mod}\ p)$, p *zenbaki lehena izanik eta* $p \nmid k$ *bada, orduan* $a \equiv b (\textit{mod}\ p)$.

Ariketak. *Aurreko emaitzeen aplikazio batzuk ondokoak dira:*

(i) $6 \equiv 4 (\textit{mod}\ 2)$ *alda daiteke* $3 \equiv 2 (\textit{mod}\ \frac{2}{d})$, *non* $d = zkh(2, 2)$ *den; hau da,* $3 \equiv 2 (\textit{mod}\ 1)$.

(ii) $44 \equiv 8 (\textit{mod}\ 9)$ *alda daiteke* $11 \equiv 2 (\textit{mod}\ \frac{9}{d})$, *non* $d = zkh(4, 9)$ *den, hau da,* $11 \equiv 2 (\textit{mod}\ 9)$.

Ariketa. *Zenbaki oso bat era hamartarrean* 9*-gatik zatigarria da baldin eta soilik baldin bere digitu guztien batura* 9*-gatik zatigarria bada. Hain zuzen ere, idatzi* n *era hamartarrean,*

$$n = a_0 + a_1 \cdot 10 + a_2 \cdot 10^2 + \cdots + a_k \cdot 10^k,$$

non a_i*-k,* $0 \leq a_i \leq 9$ *tartean dauden. Nola* $10 \equiv 1 (\textit{mod}\ 9)$, *aurreko propietate bategatik,* $10^i \equiv 1 (\textit{mod}\ 9)$ *eta ondorioz* $a_i \cdot 10^i \equiv a_i (\textit{mod}\ 9)$. *Beraz,* $n \equiv a_1 + a_2 + \cdots + a_n (\textit{mod}\ 9)$.

2 Zatigarritasunaren irizpideak

Teorema. *(Fermat-en Teorema Txikia.) Baldin eta p zenbaki lehena eta $p \nmid a$ badira, orduan*

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

Froga 2.1. *Har ditzagun a-ren lehenengo $p-1$ multiplo desberdin guztiak: $a, 2a, \ldots, \ldots \ldots, (p-1)a$. Hauek binaka ez kongruenteak dira p moduluarekiko. Hain zuzen ere, baldin eta $sa \equiv ta (mod\ p)$ bada, $s \neq t$ izanik, orduan a-gatik kantzelatuz, $s \equiv t (mod\ p)$ lortuko genuke, eta hau ezinezkoa da, s eta t, p baino txikiagoak direlako. Beraz, binaka ez kongruenteak p moduluarekiko direnez gero, horiek p-gatik zatitzerakoan $p-1$ hondar desberdin lortzen dira. Gainer, horretariko hondar bat ere ez da 0. Kontrako kasuan, baldin eta $sa \equiv 0 (mod\ p)$ bada, orduan a kantzelatuz, $s \equiv 0 (mod\ p)$ lortuko genuke, eta hau ezinezkoa da, $1 \leq s \leq p-1$ delako. Ondorioz, aurreko $p-1$ zenbakiekin $1, 2, \ldots p-1$ hondarrak lortzen ditugu. Eta orduan, $a, 2a, \ldots (p-1)a$ zenbakiak, ordenen batetan, kongruenteak dira p moduluarekiko, $1, 2, \ldots p-1$ zenbakiekin. Orain, kongruentzia guzti hauek biderkatuz, ondokoa lortzen dugu:*

$$a \cdot 2a \cdot 3a \ldots (p-1)a \equiv 1 \cdot 2 \cdot 3 \ldots (p-1) (mod\ p),$$

hau da,

$$1 \cdot 2 \cdot 3 \ldots (p-1)a^{p-1} \equiv 1 \cdot 2 \cdot 3 \ldots (p-1) (mod\ p),$$

eta $1 \cdot 2 \cdot 3 \ldots (p-1)$ kantzelatu ondoren, $a^{p-1} \equiv 1 (mod\ p)$ dugu.

Ariketa. *Kalkulatu 614^{6943} zenbakia 17 zenbakiagatik zatitzerakoan lortzen den hondarra. Nola $614 \equiv 2 (mod\ 17)$ den, ($614 = 36 \cdot 17 + 2$), orduan $614^{6943} \equiv 2^{6943} (mod\ 17)$ dugu. Nola $17 \nmid 2$, Fermat-en Teorema txikiagatik, $2^{16} \equiv 1 (mod\ 17)$ dugu. Orain, $6943 = 433 \cdot 16 + 15$ denez,*

$$2^{6943} \equiv 2^{433 \cdot 16 + 15} \equiv (2^{16})^{433} 2^{15} \equiv 1^{433} 2^{15} \equiv 2^{15} (mod\ 17).$$

Azkenik, $2^4 \equiv 16 \equiv -1 (mod\ 17)$ denez, orduan

$$2^{15} \equiv 2^{4 \cdot 3 + 3} \equiv (2^4)^3 2^3 \equiv (-1)^3 2^3 \equiv -8 \equiv 9 (mod\ 17).$$

Beraz, bilatzen genuen hondarra 9 da.

Proposizioa. *Baldin eta p eta q bi zenbaki lehen desberdinak eta a zenbaki osoa non $p \nmid a$ eta $q \nmid a$ badira, orduan $a^{(p-1)(q-1)} \equiv 1 (mod\ pq)$ dugu.*

Froga 2.2. *Fermat-en Teorema txikiagatik, badakigu $a^{p-1} \equiv 1 (mod\ p)$ dela. Aurreko propietate bat aplikatuz, $a^{(p-1)(q-1)} \equiv 1 (mod\ p)$ dugu. Antzeko moduan, $a^{q-1} \equiv 1 (mod\ q)$ dugu, eta ondorioz $a^{(p-1)(q-1)} \equiv 1 (mod\ q)$. Orain, nola $p \mid a^{(p-1)(q-1)} - 1$ eta $q \mid a^{(p-1)(q-1)} - 1$, eta p eta q zenbaki lehen desberdinak diren, $pq \mid a^{(p-1)(q-1)} - 1$ ondorioztatzen dugu, edo baliokideki, $a^{(p-1)(q-1)} \equiv 1 (mod\ pq)$.*

3 Kongruentzia linealak

Definizioa. *Baldin eta m zenbaki osoa eta positiboa, eta $a, b \in \mathbb{Z}$ badira, $ax \equiv b(\text{mod } m)$ ekuazioa, non $x \in \mathbb{Z}$ aldagaia den, kongruentzia lineala deitzen da.*

Ariketa. *Ebatzi $4x \equiv 2(\text{mod } 28)$ kongruentzia lineala. Baldin eta $x \in \mathbb{Z}$ kongruentziaren emaitza bat bada, orduan $4x = 2 + 28q$ da, $q \in \mathbb{Z}$ batentzako, eta nabaria da hau ezinezkoa dela, berdintzaren ezker aldea 4-gatik zatigarria delako, baina eskuma partekoa ez ordea.*

Ariketa. *Ebatzi $13x \equiv 2(\text{mod } 31)$ kongruentzia lineala. Baldin eta $x \in \mathbb{Z}$ kongruentziaren emaitza bat bada, orduan $13x = 2 + 31q$, $q \in \mathbb{Z}$ batentzako. Ohartu zkh$(13, 31) = 1$ dela, eta orduan Bezout-en identitateagatik, existitzen dira s, t zenbaki osoak, zeinentzat $1 = 13s + 31t$ den. Beraz, $13s \equiv 1(\text{mod } 31)$, eta kongruentzia 2-gatik biderkatuz, $13(2s) \equiv 2(\text{mod } 31)$ dugu. Hau da, $x = 2s$ ($s \in \mathbb{Z}$) hasierako kongruentziaren emaitza bat da.*

Aurreko adibideak aipatzen digu zein den giltza kongruentzia linealen emaitzen existentzia frogatzeko eta emaitza horiek topatzeko.

Proposizioa. *$ax \equiv b(\text{mod } m)$ kongruentzia linealak emaitza du, $x \in \mathbb{Z}$ izanik, baldin eta soilik baldin $d =$ zkh(a, m)-k, b zatitzen badu. Gainera, kasu honetan existitzen dira zehatz-mehatz d emaitza ez kongruenteak m moduluarekiko.*

Froga 3.1. *Lehenengo eta behin, demagu $x_0 \in \mathbb{Z}$ kongruentzia linealaren emaitza bat dela. Orduan, $ax_0 = b + qm$, $q \in \mathbb{Z}$ batentzako. Nola $d \mid a$ eta $d \mid m$ diren, $d \mid b$ dela ondorioztatzen da. Alderantziz, demagun orain $d \mid b$ eta idatzi $b = kd$, $k \in \mathbb{Z}$ batentzako. Bezout-en identitateagatik, existitzen dira s, t zenbaki osoak, zeinentzat $d = sa + tm$ den. Aurreko berdintza k-gatik biderkatuz, $b = kd = ksa + ktm$ dugu eta orduan, $aks = b - ktm \equiv b(\text{mod } m)$. Hau da, ks emandako kongruentziaren emaitza bat da. Bestalde, baldin eta x_0 eta x_1, $ax \equiv b(\text{mod } m)$ kongruentziaren bi emaitza desberdinak badira, orduan $ax_1 \equiv ax_0(\text{mod } m)$, eta a-gatik kantzelatuz $x_1 \equiv x_0(\text{mod } \frac{m}{d})$ lortzen da. Beraz, kongruentziaren d emaitza desberdinak, eta elkarrekin m moduluarekiko ez kongruenteak direnak ondokoak dira:*

$$\{x_0, x_0 + \frac{m}{d}, x_0 + 2\frac{m}{d}, \ldots, x_0 + (d-1)\frac{m}{d}\}.$$

Ariketa. *Frogatu **Wilson-en Teorema***

Baldin eta p zenbaki lehena bada, orduan $(p-1)! + 1 \equiv 0(\text{mod } p)$ dugu. Fermat-en Teorema txikiagatik $x^{p-1} \equiv 1(\text{mod } p)$ kongruentziak, edo baliokideki $x^{p-1} - 1 \equiv 0(\text{mod } p)$ kongruentziak, $p-1$ emaitza desberdinak ditu, hain zuzen ere, $1, 2, \ldots, p-1$. Beraz,

$$x^{p-1} - 1 \equiv (x-1)(x-2)\ldots(x-(p-1))(\text{mod } p).$$

Nola x-ren edozein baliok kongruentzia hau betetzen duen, $x = 0$ hartuta ondokoa dugu:

$$-1 \equiv (-1)(-2)\dots(-(p-1))(mod\ p) \equiv (-1)^{p-1}1 \cdot 2 \dots (p-1)(mod\ p),$$

hau da, $(-1)^{p-1} \cdot (p-1)! + 1 \equiv 0(mod\ p)$. Baldin $p = 2$ bada, $-1 + 1 \equiv 0(mod\ 2)$ dugu, eta baldin eta p zenbaki bakoitia bada, $(p-1)! + 1 \equiv 0(mod\ p)$ dugu.

4 Eulerren ρ funtzioa

Definizioa. *Baldin eta $n \in \mathbb{N}$ bada, $\rho(n)$ deitzen diogu n baino txikiagoak edo berdinak diren, eta aldi berean, n-rekin elkarrekiko lehenak diren, zenbaki positibo osoen kopuruari. Definizioz, $\rho(1) = 1$ da, eta honi Euler-ren ρ funtzioa deitzen zaio.*

Proposizioa. *Baldin eta p zenbaki lehena bada, orduan $\rho(p) = p - 1$.*

Proposizioa. *Baldin eta p zenbaki lehena eta $n \in \mathbb{N}$ badira, orduan $\rho(p^n) = p^n - p^{n-1}$.*

Froga 4.1. *p^n baino txikiagoak edo berdinak diren, eta aldi berean p^n-rekin elkarrekiko lehenak ez diren zenbaki positibo osoak ondokoak dira:*

$$p, 2p, 3p, \dots, p(p-1), p^2, (p+1)p, (p+2)p, \dots, 2p^2, 3p^2, \dots,$$

$$(p-1)p^2, p^3, \dots, p^{n-2}, 2p^{n-2}, 3p^{n-2}, \dots p^{n-1}p,$$

eta hauek kontatuta, horietariko p^{n-1} zenbaki positibo oso daude.

Beraz, $\rho(p^n) = p^n - p^{n-1} = p^{n-1}(p-1) = p^n(p - \frac{1}{p})$.

Korolarioa. *Baldin eta p zenbaki lehena eta $n \in \mathbb{N}$ badira, orduan $\sum_{i=0}^{n} \rho(p^i) = p^n$.*

Froga 4.2. *Aurreko proposizioa erabiliz,*

$$\sum_{i=0}^{n} \rho(p^i) = \rho(p^0) + \sum_{i=1}^{n} \left(p^i - p^{i-1}\right) = 1 + (p-1)\sum_{i=1}^{n} p^{i-1} =$$

$$= \rho(1) + (p-1)\frac{p^n - 1}{p-1} = 1 + p^n - 1 = p^n.$$

Teorema. *Baldin eta $n = p_1^{k_1} p_2^{k_2} \dots p_r^{k_r}$, $n \in \mathbb{N}$ zenbakiaren faktorizazio kanonikoa bada orduan,*

$$\rho(n) = \prod_{i=1}^{r} \rho(p_i^{k_i}) = \prod_{i=1}^{r} (p_i^{k_i} - p_i^{k_i - 1}) = n \prod_{i=1}^{r} (1 - \frac{1}{p_i}).$$

Froga 4.3. *Froga indukzioz egin daiteke. Lehenengo eta behin, p_1 zenbakiagatik zatigarriak ez diren, eta aldi berean n baino txikiagoak edo berdinak diren zenbaki positibo osoen kopurua, $n - \frac{n}{p_1}$ bidez emanda dago. Demagun n baino txikiagoak edo berdinak, eta aldi berean $p_1, p_2, \ldots, p_s$ ($s < r$ izanik) zenbaki lehenegatik zatigarriak ez diren zenbaki positibo osoen kopurua, ondoko formularen bidez emanda dagoela,*

$$n(1 - \frac{1}{p_1})(1 - \frac{1}{p_2}) \ldots (1 - \frac{1}{p_s}).$$

Orain, n baino txikiagoak edo berdinak diren, eta aldi berean, p_{s+1}-ren multiploak diren zenbaki positibo osoak ondokoak dira: p_{s+1}, $2p_{s+1}, \ldots, \frac{n}{p_{s+1}}p_{s+1}$. Horietatik, $p_1, p_2, \ldots, p_s$ zenbakien multiploak ez diren zenbakiak, p^{s+1}-ri dagozkion koefizienteak (hau da, $1, 2, 3, \ldots, \frac{n}{p_{s+1}}$), $p_1, p_2, \ldots, p_s$ zenbakiegatik zatigarriak ere ez diren, zenbakiak dira. Indukzio hipotesiagatik, zenbaki positibo oso hauen kopurua, ondoko adierazpenaren bidez emanda dago,

$$\frac{n}{p_{s+1}}(1 - \frac{1}{p_1})(1 - \frac{1}{p_2}) \ldots (1 - \frac{1}{p_s}).$$

Beraz, n baino txikiagoak edo berdinak diren, eta aldi berean $p_1, p_2, \ldots p_{s+1}$ zenbakiegatik zatigarriak ez diren zenbaki positibo osoen kopurua, ondoko formularen bidez emanda dago,

$$n(1 - \frac{1}{p_1})(1 - \frac{1}{p_2}) \ldots (1 - \frac{1}{p_s}) - \frac{n}{p_{s+1}}(1 - \frac{1}{p_1})(1 - \frac{1}{p_2}) \ldots (1 - \frac{1}{p_s}) =$$

$$n(1 - \frac{1}{p_1})(1 - \frac{1}{p_2}) \ldots (1 - \frac{1}{p_{s+1}}).$$

Oharra. *Beste modu bat, aurreko baldintzetan, $\rho(n) = \prod_{i=1}^{r} \rho(p_i^{k_i})$ dela ikusteko ondokoa litzateke. Ohartu $\mathbb{Z}/n\mathbb{Z}$ eraztunean nortzuk diren alderantzizkoa duten elementuak biderketarekiko, hau da, nor den $\mathcal{U}(\mathbb{Z}/n\mathbb{Z})$ taldea, eta ondoren ohartu aplikazio bijektiboa eta aldi berean homomorfismoa den aplikazio bat existitzen dela $\mathcal{U}(\mathbb{Z}/n\mathbb{Z})$ eta $\mathcal{U}(\mathbb{Z}/{p_1}^{k_1}\mathbb{Z}) \times \mathcal{U}(\mathbb{Z}/{p_2}^{k_2}\mathbb{Z}) \times \ldots \times \mathcal{U}(\mathbb{Z}/{p_r}^{k_r}\mathbb{Z})$ biderkadura kartesiarraren artean. Ondorioz, horietariko talde batetan lortzen diren elementu alderanzgarriak biderketarekiko eta bestean lortzen direnak, elkar erlazionatuta daude, eta hauen kopurua ere bi modutan konta daiteke.*

Proposizioa. *Baldin eta $n > 1$ bada, n baino txikiagoak edo berdinak diren, eta aldi berean n-rekin elkarrekiko lehenak diren zenbaki positibo osoen batura, $\frac{1}{2}n\rho(n)$ da.*

Froga 4.4. *Izan bitez $m_1, m_2, \ldots, m_{\rho(n)}$, n baino txikiagoak edo berdinak, eta aldi berean n-rekin elkarrekiko lehenak diren zenbaki positibo oso guztiak. Zenbaki oso horien batura ondokoa da,*

$$S = m_1 + m_2 + \cdots + m_{\rho(n)}.$$

Edozein $i \in \{1, \ldots, \rho(n)\}$ indizerako, $n - m_i$ eta n zenbakiak elkarrekiko lehenak direnez gero, orduan n baino txikiagoak edo berdinak, eta aldi berean n-rekin elkarrekiko lehenak diren zenbaki positibo osoak ondoko eran ere adieraz daitezke,

$$(n - m_1), (n - m_2), \ldots, (n - m_{\rho(n)}),$$

beraz,

$$S = (n - m_1) + (n - m_2) + \cdots + (n - m_{\rho(n)}).$$

S-rentzako adierazpen biak batuz, ondokoa dugu,

$$2S = n + \overbrace{\ldots}^{\rho(n)} + n = n\rho(n).$$

Proposizioa. *Euler-ren ρ funtzioa, numeriko biderkakorra da, hau da, baldin eta m eta n zenbakiak elkarrekiko lehenak badira, orduan $\rho(mn) = \rho(m)\rho(n)$ betetzen da.*

Froga 4.5. *Izan bitez $m = p_1^{\alpha_1} p_2^{\alpha_2} \ldots p_r^{\alpha_r}$ eta $n = q_1^{\beta_1} q_2^{\beta_2} \ldots q_s^{\beta_s}$ zenbaki oso horien faktorizazio kanonikoak, non $p_i \neq q_j$ diren, indizetako balio guztietarako. Orduan,*

$$mn = p_1^{\alpha_1} p_2^{\alpha_2} \ldots p_r^{\alpha_r} q_1^{\beta_1} q_2^{\beta_2} \ldots q_s^{\beta_s},$$

eta aurreko teoremagatik,

$$\rho(mn) = mn(1 - \frac{1}{p_1})(1 - \frac{1}{p_2}) \ldots (1 - \frac{1}{p_r})(1 - \frac{1}{q_1})(1 - \frac{1}{q_2}) \ldots (1 - \frac{1}{q_s}) =$$

$$\left(m(1 - \frac{1}{p_1}) \ldots (1 - \frac{1}{p_r})\right) \left(n(1 - \frac{1}{q_1}) \ldots (1 - \frac{1}{q_s})\right) = \rho(m)\rho(n).$$

Oharra. *Ohartu $\rho(3) = 2$ eta $\rho(6) = 6(1 - \frac{1}{2})(1 - \frac{1}{3}) = 2$ dela, baina $\rho(3 \cdot 6) = \rho(18) = 18(1 - \frac{1}{2})(1 - \frac{1}{3}) = 6 \neq \rho(3)\rho(6)$ dela.*

5 Hondarren txinatar teorema

Proposizioa. *Ondoko kongruentzia linealetako sistemak*

$$x \equiv a_1 (\textit{mod}\ m_1)$$

$$x \equiv a_2 (\textit{mod}\ m_2)$$

emaitza du baldin eta soilik baldin $zkh(m_1, m_2) \mid (a_2 - a_1)$. Baldin eta x_1 sistemaren emaitza bat bada, edozein beste emaitzaren bat, $x \equiv x_1 (\textit{mod mkt}(m_1, m_2))$ motatakoa da.

Froga 5.1. *Baldin eta $x \equiv a_1 (mod\ m_1)$ bada, orduan $x = a_1 + km_1$ da, non k zenbaki osoa den. Bigarren kongruentzia linealean ordezkatuz, $a_1 + km_1 \equiv a_2 (mod\ m_2)$ dugu, eta beraz $m_1 k \equiv (a_2 - a_1) (mod\ m_2)$ dugu. Aurreko proposizio bategatik, badakigu kongruentzia honek emaitza duela baldin eta soilik baldin $zkh(m_1, m_2) \mid (a_2 - a_1)$. Demagun x_0 bigarren kongruentzia lineal berriaren emaitza bat existitzen dela. Orain deitu $x_1 = a_1 + x_0 m_1$. Edozein bigarren kongruentzia berriaren beste emaitzaren bat, $x_0 + \frac{m_2}{d} t$ motatakoa da, non $d = zkh(m_1, m_2)$ eta $t \in \{1, 2, \ldots, d-1\}$ diren. Orduan, hasierako sistemaren beste emaitzen bat ondoko erakoa da,*

$$x = a_1 + (x_0 + \frac{m_2}{d} t) m_1 = a_1 + x_0 m_1 + \frac{m_1 m_2}{d} t.$$

Nola $x_1 = a_1 + x_0 m_1$ den, eta $zkh(m_1, m_2) \cdot mkt(m_1, m_2) = m_1 m_2$ edo beste modu batetan esanda, $\frac{m_1 m_2}{zkh(m_1, m_2)} = mkt(m_1, m_2)$ diren, orduan $x \equiv x_1 (mod\ mkt(m_1, m_2))$ dugu.

Teorema. *(Hondarren txinatar teorema.) Baldin eta $zkh(m_i, m_j) = 1$ bada, edozein $i \neq j$ balioetarako, orduan ondoko kongruentzia linealetako sistemak*

$$x \equiv a_1 (mod\ m_1)$$

$$x \equiv a_2 (mod\ m_2)$$

$$\ldots\ldots$$

$$x \equiv a_n (mod\ m_n)$$

emaitza bakarra du $m = m_1 \ldots m_n$ moduluarekiko.

Froga 5.2. *Deitu $M_i = \frac{m}{m_i}$ edozein $i \in \{1, \ldots, n\}$ baliotarako. Orduan, $zkh(M_i, m_i) = 1$. Aurreko proposizio bategatik, emaitza bakarrak existitzen dira ondoko kongruentzia linealetarako, hurrenez hurren:*

$$M_1 x_1 \equiv 1 (mod\ m_1), M_2 x_2 \equiv 1 (mod\ m_2), \ldots, M_n x_n \equiv 1 (mod\ m_n).$$

Kongruentzia bakoitza dagokion faktoreagatik biderkatuz ondokoa dugu,

$$M_1 x_1 a_1 \equiv a_1 (mod\ m_1), M_2 x_2 a_2 \equiv a_2 (mod\ m_2), \ldots, M_n x_n a_n \equiv a_n (mod\ m_n).$$

Orain enuntziatuko kongruentzia lineal bakoitza betetzen da baldin eta

$$x_0 = M_1 x_1 a_1 + M_2 x_2 a_2 + \cdots + M_n x_n a_n$$

bada, M_j-k, m_i faktorea barne duelako, baldin eta $i \neq j$ bada. Beraz, hasierako kongruentzia linealetako sistemak emaitza bat du behintzat. Baldin eta x' sistemaren beste edozein emaitzaren bat bada, $x' \equiv a_i (mod\ m_i)$ dugu, i balio bakoitzarentzat. Baita ere, $x' \equiv x_0 (mod\ m_i)$, eta nola $zkh(m_i, m_j) = 1$ den, $i \neq j$ den kasuetarako, behin eta berriro aurreko proposizioa aplikatuz, $x' \equiv x_0 (mod\ m)$ adierazpenera heltzen gara.