Alderantzizko modularraren kalkulua

Euklidesen algoritmoa erabiliz
Izan bitez $a, n \in \mathbb{Z}$ lehen erlatiboak, $\text{zkh}(a,n) = 1$.
Dakigunez, $\exists x, y \in \mathbb{Z}$ non $xa + yn = \text{zkh}(a,n)$.
Hortaz,

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

a-ren alderantzizko modularra x dela ondoriozta daiteke horrela:

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

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

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

Euler-Fermat teoremak

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

Teorema ($\phi(n)$ren kalkulurako)
Izan bitez $p, q, n \in \mathbb{Z}$.

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

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

Euler-Fermat teoremak

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

Teorema (Fermat-en teorema txikia)
Izan bedi $n \in \mathbb{Z}^+$ lehena. $a \in \mathbb{Z}^+$ izanik, $\boxed{a^{n-1} \equiv 1 \bmod n}$
Oharrak:

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

Berreketa modularra

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

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

Aritmetika modularrean, $a^x \bmod n$ kalkulatzean:

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

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

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

Aritmetika Modularra

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

n *moduluko kongruentzia*

Definizioa (n moduluko kongruentzia)

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

Teorema (Zatiketa Euklidestarra)

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

$$\begin{array}{c|l} a & b \\ \cline{2-2} r & q \end{array} \qquad a = r + qb, \quad 0 \leq r < b.$$

n moduluko kongruentzian:

$$\begin{array}{c|l} a & n \\ \cline{2-2} r & q \end{array} \qquad a = r + qn, \quad 0 \leq r < n \quad \rightarrow \quad \boxed{a \equiv r \bmod n}$$

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

Batuketa eta Biderketa modularrak

Batuketa eta biderketa

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

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

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

Zatiketa

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

Alderantzizko modularra

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

Teorema (Alderantzizko modularraren existentzia)

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

$\mathbb{Z}_n$ multzoan alderantzikagarri diren elementuen multzoa $\mathbb{Z}_n^*$ da.

n moduluko hondarren multzo murriztua:

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

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

Berreketa modularra

Berreketa bitarraren metodoa

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

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

Berreketaren honako hiru propietateetan oinarritzen da:

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

Bibliografia

- Aritmética modular
  http://es.wikipedia.org/wiki/Aritmética_modular
- Modular Multiplicative Inverse edo alderantzizko modularra
  http://en.wikipedia.org/wiki/Modular_multiplicative_inverse
- Teorema de Euler, Pequeño teorema de Fermat
  http://es.wikipedia.org/wiki/Teorema_de_Euler
  http://es.wikipedia.org/wiki/Pequeño_teorema_de_Fermat
  RSA algorithm. Proofs of correctness
  http://en.wikipedia.org/wiki/RSA_(algorithm)
- Anexo: Números primos
  10000 baino txikiagoak diren zenbaki lehenak.
  http://es.wikipedia.org/wiki/Anexo:Números_primos
- Exponenciación binaria
  http://es.wikipedia.org/wiki/Exponenciación_binaria

Aritmetika Modularra. Ariketak

n moduluko kongruentzia. Batuketa. Biderketa

1. Esan honakoak egiazkoak ala faltsuak diren.
   - $2 \equiv 4 \bmod 2$
   - $13 \equiv -2 \bmod 5$
   - $15 \equiv 3 \bmod 3$
   - $20 \equiv 4 \bmod 7$

2. Izan bedi $\mathbb{Z}_5 = \{0,1,2,3,4\}$ multzoa. Kalkula itzazu elementuen arteko batuketak eta biderketak, eta osa itzazu beheko bi taulak. Egin ezazu gauza bera $\mathbb{Z}_6 = \{0,1,2,3,4,5\}$ multzorako.

+	0	1	2	3	4
0					
1					
2					
3					
4					

·	0	1	2	3	4
0					
1					
2					
3					
4					

   Ondoren erantzun itzazu honako galderak:
   - Zenbat da $2+3 \bmod 5$? Hau da, $2,3 \in \mathbb{Z}_5$ izanik, zenbat da $\mathbb{Z}_5$ multzoan $2+3$? Eta, $3+4 \bmod 5$? Eta, $2 \cdot 3 \bmod 5$? Eta, $4 \cdot 2 \bmod 5$?
   - Zenbat da $3+4 \bmod 6$? Hau da, $3,4 \in \mathbb{Z}_6$ izanik, zenbat da $\mathbb{Z}_6$ multzoan $3+4$? Eta, $5+1 \bmod 6$? Eta, $2 \cdot 3 \bmod 6$? Eta, $4 \cdot 4 \bmod 6$?

3. Honako a eta b balioetarako, eta $n = 35$ izanik, kalkula itzazu batuketa eta biderketa modularrak, hau da, .
   - $a = 15, b = 5 \quad \to \quad a+b \bmod n =?, \quad ab \bmod n =?$
   - $a = 32, b = 3 \quad \to \quad a+b \bmod n =?, \quad ab \bmod n =?$
   - $a = 28, b = 10 \quad \to \quad a+b \bmod n =?, \quad ab \bmod n =?$
   - $a = 126, b = 3 \quad \to \quad a+b \bmod n =?, \quad ab \bmod n =?$

4. Gaur arratsaldeko 15:00etan autobusa hartuko dugu. Bidaia luzea da, 356 ordu beharko ditugu iristeko. Zein ordutan iritsiko gara? Erabil ezazu aritmetika modularra galderari erantzuteko.

Alderantzizko modularra

5. Izan bedi $\mathbb{Z}_5 = \{0,1,2,3,4\}$ multzoa. Kalkula ezazu $\mathbb{Z}_5^*$. Eulerren funtzioak zenbat balio du, $\phi(5) =$? Ondoren, egiazta itzazu honakoak: $1^{-1} \bmod 5 = 1, 2^{-1} \bmod 5 = 3, 3^{-1} \bmod 5 = 2, 4^{-1} \bmod 5 = 4$. Horretarako, Euklidesen algoritmoa erabil ezazu.

6. Izan bedi $\mathbb{Z}_6 = \{0,1,2,3,4,5\}$ multzoa. Kalkula ezazu $\mathbb{Z}_6^*$. Eulerren funtzioak zenbat balio du, $\phi(6) =$? Ondoren, egiazta itzazu honakoak: $1^{-1} \bmod 6 = 1, 5^{-1} \bmod 6 = 5$. Horretarako, Euklidesen algoritmoa erabil ezazu. Froga ezazu 2, 3 eta 4 elementuak ez direla alderantzikagarriak $\mathbb{Z}_6$ multzoan.

7. Egiazta ezazu honako alderantzizko modularrak existitzen direla, eta Euklidesen algoritmoa erabil ezazu kalkulatzeko.
   - 3aren alderantzizkoa $\mathbb{Z}_{10}$ multzoan, hau da, $3^{-1} \bmod 10 =$?
   - 5aren alderantzizkoa $\mathbb{Z}_{12}$ multzoan, hau da, $5^{-1} \bmod 12 =$?
   - 7aren alderantzizkoa $\mathbb{Z}_{16}$ multzoan, hau da, $7^{-1} \bmod 16 =$?
   - 6aren alderantzizkoa $\mathbb{Z}_{17}$ multzoan, hau da, $6^{-1} \bmod 17 =$?
   - 32aren alderantzizkoa $\mathbb{Z}_{81}$ multzoan, hau da, $32^{-1} \bmod 81 =$?
   - 777aren alderantzizkoa $\mathbb{Z}_{1009}$ multzoan, hau da, $777^{-1} \bmod 1009 =$?

Berreketa modularra

8. Kalkula itzazu honako berreketa modularrak. Euler-en teoremak berreketaren kalkuluan laguntzen al dizu?
   - $\mathbb{Z}_{21}$ multzoan, $5^{12} \bmod 21 =?, \quad 5^{47} \bmod 21 =?$
   - $\mathbb{Z}_9$ multzoan, $2^6 \bmod 9 =?, 4^6 \bmod 9 =?\ , 5^6 \bmod 9 =?\ , 7^6 \bmod 9 =?$

9. Kalkula itzazu honako berreketa modularrak. Fermat-en teorema txikiak berreketaren kalkuluan laguntzen al dizu?
   - $\mathbb{Z}_{11}$ multzoan, $4^{10} \bmod 11 =?, \quad 5^{10} \bmod 11 =?$
   - $\mathbb{Z}_{23}$ multzoan, $3^{90} \bmod 23 =?$
   - $\mathbb{Z}_{47}$ multzoan, $19^{200} \bmod 47 =?$
   - $\mathbb{Z}_{101}$ multzoan, $15^{1341402} \bmod 101 =?$

10. Honako berreketa modularrak kalkulatzeko, berreketa bitarrerako metodoa erabil ezazu. Horretarako, kalkula ezazu lehenik x berretzailearen adierazpen bitarra. Ondoren esan nola kalkulatuko den a^x berreketa. Zenbat biderketa egin behar izan dira berreketa kalkulatzeko? Kalkula ezazu berreketa modularra.
    - $x = 13$ izanik, a^{13}ren adierazpena? Zenbat da 2^{13}? Eta, $2^{13} \bmod 3$?
    - $x = 11$ izanik, a^{11}ren adierazpena? Zenbat da $49^{11} \bmod 85$?

Egin itzazu **gutxienez hiru ariketa** ondokoen artetik.
Laborategira eginda (paperean) eraman behar dira ariketa horien espezifikazioa, algoritmoa eta proba-kasuen diseinua.
Laborategi-saioan inplementatu eta probatuko dituzu.
Egindako lana eGela plataformaren bidez entregatuko da, aldez aurretik behar bezala dokumentatuta.

Espezifikatu, kodetu eta probatu honako enuntziatuak ebatziko dituzten programak:

1. 9 digitu dituen N zenbaki oso positiboa irakurrita, erabaki ea zenbaki hori telefono finko batena (9 digituarekin hasten da), telefono mugikor batena (6 digituarekin hasten da) edo bestelakoa den. Idatzi mezu bat adierazteko hiru aukera horietatik zein dagokion N zenbakiari.
   Adibidez:
   N = 943202030 datua irakurrita, "Telefono finkoa" mezua idatziko litzateke pantailan.

2. N zenbaki oso positiboa irakurrita, idatz ezazu 3ren multiplo diren lehen N zenbakien batura.
   Adibidez:
   4 zenbakia irakurrita, 30 idatzi beharko luke (30 = 3 + 6 + 9 + 12).

3. N zenbaki oso positiboa irakurrita, idatzi zenbat digitu dituen.
   Adibidez:
   12345678 irakurrita, 8 idatzi beharko luke.

4. Puntu karaktereaz amaitzen den karaktere-sekuentzia bat irakurrita, idatzi karaktere guztiak zuriuneak kenduta.
   Oharra: Sekuentzian dagoen puntu bakarra azkena da.
   Adibidez

Sarrera:	*Komando honek lehen sortutako direktoriora eramaten gaitu.*
Irteeera:	*Komandohoneklehensortutakodirektorioraeramatengaitu.*
Sarrera:	.
Irteera:	.
Sarrera:	.
Irteera:	.

5. Zero zenbakiarekin bukatzen den oso-sekuentzia bat irakurrita, idatzi zenbat zenbaki negatibo dauden eta zein den zenbaki positiboen batura.
   Adibidez:

Sekuentzia: <6, -6, -8, -3, 4, 7, 0>	Emaitzak: 3 eta 17
Sekuentzia: <-6, -8, -3, 0>	Emaitzak: 3 eta 0
Sekuentzia: <6, 4, 7, 0>	Emaitzak: 0 eta 17
Sekuentzia: <0>	Emaitzak: 0 eta 0

Egin itzazu **gutxienez hiru ariketa** ondokoen artetik.
Laborategira eginda (paperean) eraman behar dira ariketa horien espezifikazioa, algoritmoa eta proba-kasuen diseinua.
Laborategi-saioan inplementatu eta probatuko dituzu.
Egindako lana eGela plataformaren bidez entregatuko da, aldez aurretik behar bezala dokumentatuta.

Espezifikatu, kodetu eta probatu honako enuntziatuak ebatziko dituzten programak:

1. 9 digitu dituen N zenbaki oso positiboa irakurrita, erabaki ea zenbaki hori telefono finko batena (9 digituarekin hasten da), telefono mugikor batena (6 digituarekin hasten da) edo bestelakoa den. Idatzi mezu bat adierazteko hiru aukera horietatik zein dagokion N zenbakiari.
   Adibidez:
   N = 943202030 datua irakurrita, "Telefono finkoa" mezua idatziko litzateke pantailan.

2. N zenbaki oso positiboa irakurrita, idatz ezazu 3ren multiplo diren lehen N zenbakien batura.
   Adibidez:
   4 zenbakia irakurrita, 30 idatzi beharko luke (30 = 3 + 6 + 9 + 12).

3. N zenbaki oso positiboa irakurrita, idatzi zenbat digitu dituen.
   Adibidez:
   12345678 irakurrita, 8 idatzi beharko luke

4. Puntu karaktereaz amaitzen den karaktere-sekuentzia bat irakurrita, idatzi karaktere guztiak zuriuneak kenduta.
   Oharra: Sekuentzian dagoen puntu bakarra azkena da.
   Adibidez
   Sarrera: *Komando honek lehen sortutako direktoriora eramaten gaitu.*
   Irteera: *Komandohonleklehensortutakodirektorioraeramatengaitu.*
   Sarrera: .
   Irteera: .
   Sarrera: .
   Irteera: .

5. Zero zenbakiarekin bukatzen den oso-sekuentzia bat irakurrita, idatzi zenbat zenbaki negatibo dauden eta zein den zenbaki positiboen batura.
   Adibidez:
   Sekuentzia: <6, -6, -8, -3, 4, 7, 0> Emaitzak: 3 eta 17
   Sekuentzia: <-6, -8, -3, 0> Emaitzak: 3 eta 0
   Sekuentzia: <6, 4, 7, 0> Emaitzak: 0 eta 17
   Sekuentzia: <0> Emaitzak: 0 eta 0

$65^{43} \bmod 85 = 10$

$65^{43} = 9'0214o823 \cdot 10^{77}$

RSA galdeak

$p=5,\ q=17 \rightarrow$ Gako publikoak? $n=\ ;\ r=$
Pribatua? $s=$

$n = p \cdot q = \boxed{85}$

$m = (p-1)(q-1) = 4 \cdot 16 = 64$

$ZKH(m, r) = 1 \qquad r = ?$
Handia izan beharko luke
Gure kasuan $\boxed{r=3}$

$s = r^{-1} \bmod m = 3^{-1} \bmod 64 = 43$

Hortaz, $m = 85$, $r = 3 \rightarrow$ publikoa
Pribatuan gorde $\boxed{s=43}$

$\cancel{65}^{43}$ mod 85

$3 \in \mathbb{Z}_{64}$, $3^{-1} \bmod 64 = ?$

$\exists\, 3^{-1} \bmod 64$?

lnko$(3, 64) = 1$

$3 \;\lfloor 64$
$3 \quad 0 \rightarrow 3 = 64 \cdot 0 \, 3 - 64 \cdot 0$

$64 \;\lfloor 3$
$\boxed{1} \quad 21 \rightarrow 64 = 3 \cdot 21 + 1 \rightarrow 1 = 64 - 3 \cdot 21$

lnko$(3, 64) = -3 \cdot 21 + 1 \cdot 64$

-21 Neg!

$-21 + 64 = 43$

$3^{-1} \bmod 64 = 43$

b)
$3^{-1} \bmod 352 = ?$

$\exists\, 3^{-1} \bmod 352$, lnko$(3, 352) = 1$

$3 \;\lfloor 352$
$3 \quad 0$

$352 \;\lfloor 3$
$\boxed{1} \quad 117 \rightarrow 1 = -117 \cdot 3 + 352$

$352 - 117 = \cancel{235}\ 235$

(2) Borrellata modulerre $\boxed{65^{43} \bmod 85}$

$a^{43} \rightarrow$ adiersapan biteren

$43 \rightarrow 1\,0\,1\,0\,1\,1$

$2^5 \quad 2^3 \quad 2^1\, 2^0 = 32 + 8 + 2 + 1 = 43$ 8 eoagillela

$a^{43} = a^{32} \cdot a^8 \cdot a^2 \cdot a =$

$= (a^{16})^2 \cdot (a^4)^2 \cdot a^2 \cdot a =$

$= (a^{16} \cdot a^4)^2 \cdot a^2 \cdot a =$

$= ((a^8 \cdot a^2)^2)^2 \cdot a^2 \cdot a = (((a^4)^2 \cdot a^2)^2)^2 \cdot a^2 \cdot a =$

$= (((a^4)^2 a^2)^2 a)^2 \cdot a =$

$= (((a^2)^2 \cdot a)^2)^2 \cdot a)^2$

```
            Bitartean S /= 0 egin
                  Baldin S<0 egin
                        Kont:= Kont + 1
                        Irakurri_osoa(F,S)
                  Bestela S>0
                        Barura:= Batura + S
                        Irakurri_osoa(F,S)
                  ambaldin
            ambitartean
            Idatzi_osoa(Kont eta Batura)
      Amaia
```

Proba-kasu esanguratsuak eta emaitzak

Zer kasu hartu behar dugu kontuan programa probatzeko eta zergatik? Jarraian eman lortutako emaitzak.

Sekuentzia:<6,-6,-8,-3,4,7,0>	Emaitzak: 3 eta 17
Sekuentzia:<-6,-8,-3>	Emaitzak: 3 eta 0
Sekuentzia:<6,4,7,0>	Emaitzak: 0 eta 17
sekuentzia:<0>	Emaitzak: 0 eta 0

Balorazioa eta hobekuntzak

Idatzi hemen, nahi duzun luzera hartuta, zure balorazioa ariketa honi buruz: aurkitu dituzun arazo nagusiak, zenbat denbora behar izan duzun eta egin dituzun edo egin zitezkeen hobekuntzak.

Berreketa modularra

(10) $a^{13} \rightarrow$ Berreketa bitarreko adierazpena

B-ren adierazpen Bitarra kalkulatuko dugu.

$$\begin{array}{lllll} 13 & \lfloor 2 & & & \\ 1 & 6 & \lfloor 2 & & \\ & 0 & 3 & \lfloor 2 & \\ & & 1 & 1 & \lfloor 2 \\ & & & 1 & 0 \end{array} \qquad 13_{10} = 1101_2$$

a^{13} berreketa horrek adierazi dezakegu

$$\boxed{a^{13} = a^8 \cdot a^4 \cdot a^1}$$

$a^{13} = a^8 \cdot a^4 \cdot a^1 = (a^4)^2 \cdot (a^2)^2 \cdot a^1 = \cancel{(a^2)^6}\,(a^4 \cdot a^2)^2 \cdot a^1 = ((a^2)^2 \cdot (a^2))^2 \cdot a =$

$= ((a^2 \cdot a)^2)^2 \cdot a$

Zenbat da 2^{13}?

$2^{13} = 2 \cdot 2 \cdot \ldots \cdot 2 = \boxed{8192}$

$2^{13} = ((2^2 \cdot 2)^2)^2 \cdot 2$.

Zenbat da $2^{13} \bmod 3 = ?$

Bi modutara egin daiteke: $2^{13} = 8192$

$8192 \bmod 3 = 2$

Hain zenbaki handietara joaten arazoa izaten da. Aplikatu erregela

$$2^{13} \bmod 3 = \underbrace{((\underbrace{\underbrace{(\underbrace{2^2 \bmod 3}_{1}) \cdot 2 \bmod 3}_{2}{}^2}_{4} \bmod 3)^2 \bmod 3}_{1}) \cdot 2 \bmod 3$$

$$= 2$$

Egin itzazu **gutxienez hiru ariketa** ondokoen artetik.
Laborategira eginda (paperean) eraman behar dira ariketa horien espezifikazioa, algoritmoa eta proba-kasuen diseinua.
Laborategi-saioan inplementatu eta probatuko dituzu.
Egindako lana eGela plataformaren bidez entregatuko da, aldez aurretik behar bezala dokumentatuta.

Espezifikatu, kodetu eta probatu honako enuntziatuak ebatziko dituzten programak:

1. 9 digitu dituen N zenbaki oso positiboa irakurrita, erabaki ea zenbaki hori telefono finko batena (9 digituarekin hasten da), telefono mugikor batena (6 digituarekin hasten da) edo bestelakoa den. Idatzi mezu bat adierazteko hiru aukera horietatik zein dagokion N zenbakiari.
   Adibidez:
   N = 943202030 datua irakurrita, "Telefono finkoa" mezua idatziko litzateke pantailan.

2. N zenbaki oso positiboa irakurrita, idatz ezazu 3ren multiplo diren lehen N zenbakien batura.
   Adibidez:
   4 zenbakia irakurrita, 30 idatzi beharko luke (30 = 3 + 6 + 9 + 12).

3. N zenbaki oso positiboa irakurrita, idatzi zenbat digitu dituen.
   Adibidez:
   12345678 irakurrita, 8 idatzi beharko luke.

4. Puntu karaktereaz amaitzen den karaktere-sekuentzia bat irakurrita, idatzi karaktere guztiak zuriuneak kenduta.
   Oharra: Sekuentzian dagoen puntu bakarra azkena da.
   Adibidez

Sarrera:	*Komando honek lehen sortutako direktoriora eramaten gaitu.*
Irteeera:	*Komandohoneklehensortutakodirektorioraeramatengaitu.*
Sarrera:	.
Irteera:	.
Sarrera:	.
Irteera:	.

5. Zero zenbakiarekin bukatzen den oso-sekuentzia bat irakurrita, idatzi zenbat zenbaki negatibo dauden eta zein den zenbaki positiboen batura.
   Adibidez:

Sekuentzia: <6, -6, -8, -3, 4, 7, 0>	Emaitzak: 3 eta 17
Sekuentzia: <-6, -8, -3, 0>	Emaitzak: 3 eta 0
Sekuentzia: <6, 4, 7, 0>	Emaitzak: 0 eta 17
Sekuentzia: <0>	Emaitzak: 0 eta 0

Aritmetika modularra

(2)

Alderantzizko modularraren kalkulua Euklidesen algoritma

6 ren alderantzizkoa $\mathbb{Z}_{12}$ multzoan?

$\exists\, 6^{-1} \bmod 12$?

Existitzeko Bete behar da $ZKH(6, 12) = 1$

Bai!

$$\begin{array}{l|l} 6 & 12 \\ \hline 6 & 0 \end{array} \rightarrow 6 = 12\cdot 0 + 6 \rightarrow 6 = 6 - 12\cdot 0$$

$$\begin{array}{l|l} 12 & 6 \\ \hline 5 & 2 \end{array} \rightarrow 12 = 6\cdot 2 + 5 \rightarrow 5 = 12 - 6\cdot 2$$

$$\begin{array}{l|l} 6 & 5 \\ \hline 1 & 1 \end{array} \rightarrow 6 = 5\cdot 1 + 1 \rightarrow 1 = 6 - 5\cdot 1$$

$$\begin{array}{l|l} 5 & 1 \\ \hline 0 & 5 \end{array}$$

$\rightarrow ZKH(6, 12)$

$$1 = 6 - 5\cdot 1 \rightarrow 6 - (12 - 6\cdot 2)\cdot 1 = 6 - 12 + 6\cdot 2 = 6\cdot 3 - 12$$

$$1 = 6\cdot 3 - 12$$

Koefiziente hau da bilatzen ari garena

$ZKH(6,12) = x\cdot 6 + y\cdot 12$

Hortaz, $6^{-1} \bmod 12 = 3$, Alderantzizkoa izanik $6\cdot 6^{-1} \bmod 12 = 1$

Egiaztatu dezagun,

$(6\cdot 3) \bmod 12$

$18 \bmod 12 \rightarrow \begin{array}{l|l} 18 & 12 \\ \hline 1 & 1 \end{array}$

3

```
WITH Ada.Integer_text_IO USE Ada.Integer_text_IO
PROCEDURE Telefono_mota IS

        N:= Integer;

  Bestelakoa, Telefono mugikorra eta Telefono finkoa:= Character;

BEGIN

                Get(N)

                IF N /= 9 AND N /= 6 THEN

                Put(Bestelako telefonoa);

                ELSE

                        IF S= 9 orduan

                        Put(Telefono Fijoa);

                        ELSE

                        Put(Telefono Mugikorra);

                END IF;

                END IF;

        END
```

3aren alderantzizkoa $\mathbb{Z}_{10}$ multzoan

$\exists\, 3^{-1} \bmod 10\,?$

$ZKH(3,10)=1$

$$3 \,\underline{\lfloor 10}\quad 3 \quad 0 \rightarrow 3 = 10\cdot 0 + 3 \rightarrow 3 = 3 - 10\cdot 0$$

$$10 \,\underline{\lfloor 3}\quad 1 \quad 3 \rightarrow 1 = -3\cdot 3 + 10$$

1 → Bai betetzen da, $ZKH(3,10)=1$

$$\boxed{1 = 10 - 3\cdot 3}$$

$3^{-1} \bmod 10 = -3$

$-3 \cdot 3^{-1} \bmod 10 = 1$

$\mathbb{Z}_{10}$ multzoan ari gara lanean honderren multzoan

$\mathbb{Z}_{10} = \{0,1,2\ldots 9\}$

$-3+10=7$

Hortaz, $3^{-1} \bmod 10 = 7$

<u>Egiaztatu</u>

$(3\cdot 3^{-1}) \bmod 10 = 1$

$3\cdot 7 \bmod 10$

$21 \bmod 10$

1

$$21 \,\underline{\lfloor 10}\quad 1 \quad 2$$

Oinarrizko Programazioa
Lab01

Egilea: Aitzol Elu Etxano

Enuntziatua:

Zero zenbakiarekin bukatzen den oso-sekuentzia bat irakurrita, idatzi zenbat zenbaki negatibo eta zein den zenbaki positiboen batura

Zehaztapena (aurrebaldintza eta postbaldintza)

Aurrebaldintza: F=<S>

S:= < s_1, s_2,..., s_n>

S:= integer

S_n:= 0

S /=0 azkena izan ezik

Postbaldintza: G<n eta p>

n:= zenbaki negatiboen kopurua, 0 edo handiagoa izan daiteke.
p=zenbaki positiboen batura, 0 edo handiagoa izan daiteke.

Algoritmoa

Algoritmoa: Sekuentzia_Ebazpena

S, Kont, Batura:= integer

Hasiera:

Irakurri_osoa(F,S)
Batura:=0
Kont:=0

Aritmetiko modularra

①

$2 \equiv 4 \mod 2$

$2 \mid 2-4$

$\exists k \in \mathbb{Z}$ non $2-4 = 2k$

$-2 = 2k$

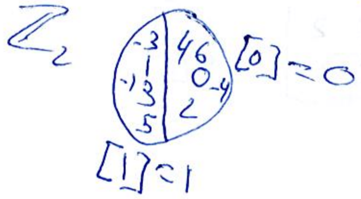
$\exists k = -1 \in \mathbb{Z}$

kongruenteak dira

$2 \,\underline{\lfloor 2}$
$\boxed{0}$ 1

$4 \,\underline{\lfloor 2}$
$\boxed{0}$ 2

Biek hondar bera usten dutenez kongruenteak dira



$20 \equiv 4 \mod 7$

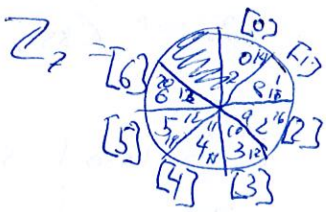
Ez!

$7 \mid 20-4$

$\exists k \in \mathbb{Z}$ non $20-4 = 7k$

$16 = 7k$

$\exists k \notin \mathbb{Z}$ $k = \frac{16}{7}$



$20 \,\underline{\lfloor 7}$
$\boxed{6}$ 2

$4 \,\underline{\lfloor 7}$
$\boxed{4}$ 0

r_1 r_2

$r_1 \neq r_2$ beraz ez dira kongruenteak.

(2)

$\mathbb{Z} = \{0,1,2,3,4\} \Rightarrow$ 5 moduluko kongruentziek sortutako hondarren multzoa.

$5 \,\lfloor 5$; $\boxed{0}$ 1 → hondarra

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

$\to 2+4 \bmod 5$; $6 \,\lfloor 5$; $1 \quad 1$

·	0	1	2	3	4
0	0	0	0	0	0
1	0	1	2	3	4
2	0	2	4	1	3
3	0	3	1	4	2
4	0	4	3	2	1

$2 \cdot 3 \bmod 5$

$6 \,\lfloor 5$; $\boxed{1}$ 1

$8 \,\lfloor 5$; 3 1

$9 \,\lfloor 5$

IR-n $2^{-1} = \frac{1}{2}$

$2 \cdot 2^{-1} = \frac{2}{2} = \boxed{1}$

(3) $m = 35 \Rightarrow \mathbb{Z}_{35}$, 35 Moduluko kongruentzia

$a = 15$

$b = 5$

$a + b \bmod 35$

$20 \bmod 35$

20

$20 \,\lfloor 35$; $\boxed{20}$ 0

~~15·5~~ $a \cdot b \bmod 35$

$75 \bmod 35$

$\boxed{5}$

$75 \,\lfloor 35$; $\boxed{5}$ 2

$a = 126$

$b = 3$

$a + b \bmod 35$

$126 + 3 \bmod 35$

$((126 \bmod 35) + (3 \bmod 35)) \bmod 35$

$\boxed{a \cdot b \bmod 35}$

$126 \bmod 35 \qquad 3 \bmod 35$

$126 \,\lfloor 35$; $\boxed{21}$ 3

~~3 mod 35~~

$3 \,\lfloor 35$; $\boxed{3}$ 0

$24 \bmod 35$

$24 \,\lfloor 35$; $\boxed{24}$ 0 $\boxed{24}$