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					

$\cdot$	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, .

   - $a = 15$, $b = 5 \quad \rightarrow \quad a + b \bmod n =?, \quad ab \bmod n =?$
   - $a = 32$, $b = 3 \quad \rightarrow \quad a + b \bmod n =?, \quad ab \bmod n =?$
   - $a = 28$, $b = 10 \quad \rightarrow \quad a + b \bmod n =?, \quad ab \bmod n =?$
   - $a = 126$, $b = 3 \quad \rightarrow \quad a + b \bmod n =?, \quad ab \bmod n =?$

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. 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 $49^{11} \bmod 85$?
   - $x = 43$ izanik, a^{43}ren adierazpena? Zenbat da $65^{43} \bmod 85$?
   - $x = 235$ izanik, a^{235}ren adierazpena? Zenbat da $40^{235} \bmod 391$? (ikus emaitza "Kriptografia: RSA zifratze-algoritmoa" orritxo teorikoetan, "deszifratzea" atalean).

RSA zifratze-algoritmoa

9. Kalkula itzazu honako zenbaki lehen pare bakoitzetik abiatuz lortzen diren RSA gakoak. Aukera ezazu r gako publikoa ahalik eta txikiena.

   9.1 $p = 5$, $q = 17$

   9.2 $p = 17$, $q = 23$

   9.3 $p = 97$, $q = 101$

   9.4 $p = 307$, $q = 397$

10. $n = 209$ eta $r = 7$ gako publikoa duen zure lagunari "uau" mezua bidali nahi diozu, RSA algoritmoaren bidez zifratuta eta ASCII kodeketa erabiliz. Zifratuko duzu?

11. $n = 209$ eta $r = 7$ gako publikoa duen zure lagunari norbaitek $31, 62, 147, 22$ mezu zifratua bidali dio. Badakizu RSA algoritmoarekin zifratua izan dela eta ASCII kodeketa erabili dela. Kuxkuxero samarra zara eta, deszifratuko duzu?