2. Partzialaren Laburpena :)

Grafoak

Kontzeptuak:

Katea:

Ertz errepikaturik ez duen ibilbide irekia.

Kate Eulertarra:

Ertz guztietatik behin eta bakarrik behin igarotzen den Kate irekia da.

Zirkuitua:

Ertz errepikaturik ez duen ibilbide itxia.

Zirkuitu Eulertarra:

Ertz guztietatik behin eta bakarrik behin igarotzen den zirkuitua da.

Zikloa:

Erpin errepikatuak ez duen ibilbide itxia. $\forall x \in V \delta(x) \geq 2$

Ziklo Hamiltondarra:

Erpin guztiak duen zikloa

Grafo Hamiltondarra:

Ziklo Hamiltondarra duen grafoa. $\forall x \in V \delta(x) \geq \frac{n}{2}$

Grafo osagarria:

Grafo osagarria grafo batek falta dituen ertzak grafo osotua lortzeko daukan grafoa da. Ertzak $= \frac{V(V-1)}{2} - e$

Bidea:

Erpin errepikatuak ez duen ibilbide irekia.

Bide Hamiltondarra

Erpin guztiak duen bidea. $\forall x \in V, \delta(x) \geq \frac{n-2}{2}$

K-Grafo:

K erpineko grafo osotua

K-erregularra:

Erpin guztiak K gradua dute. $\forall x \in V, \delta(x) = K$

Azpigrafo sortzailea:

Azpigrafoa eta grafoa erpin berdinak dituztenean.

Sortzaile $\Leftrightarrow V_1 = V$

2^m azpigrafo sortzaile daude, $m = N(V)$

Aritmetika modularra:

RSA:

Gakoen sormena

1. Aukeratu bi zenbaki lehen (p,q)
2. $n = p \cdot q$
3. $m = (p-1)(q-1)$
4. $r \Rightarrow zkh(m,r) = 1$
5. $s = r^{-1} \bmod m$

Zifratzea:

$R_i = M_i^s \bmod n$

Deszifratzea:

$M_i = R_i^r \bmod n$

Berreketa modularra

Adb: $a^{15} \bmod 5$

1. Forma generala atera

$a^{15} = a^{14} \cdot a = (a^7)^2 \cdot a = (a^6 \cdot a)^2 \cdot a =$

$= ((a^3)^2 \cdot a)^2 \cdot a = \boxed{((a^2 \cdot a)^2 \cdot a)^2 \cdot a}$

2. modulua aplikatu

$((a^2 \bmod 5 \cdot a \bmod 5)^2 \bmod 5 \cdot a \bmod 5)^2 \bmod 5 \cdot a \bmod 5$

Alderantzizko modularra

Adb: $a^{-1} \bmod b$

$b \,\underline{|\, a}$ $\quad b = c \cdot a + 1$

$1 \quad c \quad\quad 1 = b \boxed{-c} \cdot a$

Alderantzizko modularra

Eulerren funtzioa $\phi(n)$

n Lehena bada: $\phi(n) = n-1$

$n = p \cdot q$: $\phi(n) = (p-1)(q-1)$

Zenbaki teoria

Zatigarritasun prop.

1. $\forall a \neq 0,\ 1|a;\ a|a;\ a|0$
2. $\forall a,b \neq 0,\ (a|b) \wedge (b|a) \Rightarrow a=b \vee a=-b$
3. $\forall a,b \neq 0,\ (a|b) \wedge (b|c) \Rightarrow a|c$
4. $\forall a \neq 0,\ a|b \Rightarrow (\forall x \in \mathbb{Z})\ a|xb$
5. $\forall a \neq 0,\ a|b \wedge a|c \Rightarrow \forall x,y \in \mathbb{Z}\ a|xb+yc$

Zkh-ren propietateak

1. $zkh(a,b) = zkh(b,a)$
2. $zkh(0,0)$ ez dago definiturik.
3. $\forall a \in \mathbb{Z} \wedge a \neq 0,\ zkh(a,0) = |a|$
4. $a,b \in \mathbb{Z}$ emanik beti existituko da $zkh(a,b)$ $a=b=0$ izan ezik. $zkh(a,b) = zkh(|a|,|b|)$
5. Bezouten identitatea

$\forall a,b \in \mathbb{Z} \wedge a,b \neq 0\ \exists x,y \Rightarrow zkh(a,b) = xa + yb$

$zkh(a,b)$ da a eta b ren Konbinazio lineal moduan adieraz daitekeen zenbaki oso positiborik txikiena.

6. Aurreko Konbinazio linealen Koefizienteak ez dira bakarrak

$zkh(a,b) = xa + yb$

$\wedge$

$zkh(a,b) = (x+pb)a + (y-pa)b,\ p \in \mathbb{Z}$

Multiplo Komun txikiena

1. m zenbakia a eta b ren multiplo komuna da $a|m \wedge b|m$
2. a eta b zenbakien edozein multiplo komun m baino handiago edo berdina da.

$\forall c \in \mathbb{Z}^+\ a|c, b|c \Rightarrow m \leq c$

Aritmetikaren oinarrizko teorema

$\forall n \in \mathbb{N}$ n lehena da edo n zenbaki lehenen biderketa gisa idatz daiteke era bakarrean.

Lema:

$p|ab \Rightarrow (p|a) \vee (p|b)$

Lema:

$p|a_1 a_2 \cdots a_n \Rightarrow p|a_j;\ j \in \{1, \ldots, n\}$ bateratko