Obligatoriske oppgave 3, MAT-1005

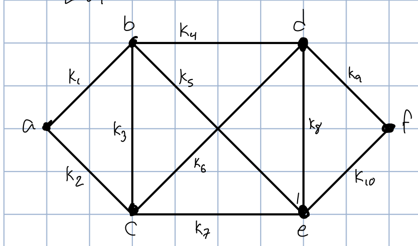
Eskil Bjørnbakk Heines

Oppgave 1.1)

En Eulerskrets til en graf G, er en krets som går gjennom alle kanter i grafen nøyaktig én gang. Kravet for en Eulerkrets er at alle grader er partall, og at start og slutt punkt er det samme ($v_0 = v_n$).

Oppgave 1.2)

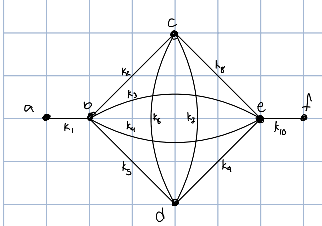
Eulerkrets:



a k_1 b k_3 c k_6 d k_4 b k_5 e k_8 d k_9 f k_{10} e k_7 c k_2 a

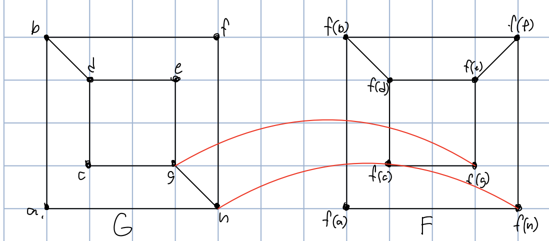
Vi ser at denne Eulerkretsen går gjennom alle kantene nøyaktig én gang, og slutter der den starter (i a).

Ikke Eulerkrets



Vi ser at grafen ikke er en Eulergraf siden vi ikke kan gå gjennom alle kantene nøyaktig én gang, og da gå gjennom alle. Vi har 4 noder med oddetall grader, og kan da ikke ha Eulerkrets eller Eulersti.

Oppgave 1.3)



g er nabo med h,
f(g) er ikke nabo med f(h)

Når vi jobber med isomorfi, jobber vi med en bijektiv funksjon. Altså en funksjon hvor alt i definisjonsmengden treffer noe i verdimengden. Begge grafene har 8 noder, altså hver node kan treffe en node i den andre grafen. Problemet med grafene er at naboene er forskjellig. Hvis G og F er isomorf vil naboene a og b i G, være naboene f(a) og f(b) i F. I vår graf G er g og h naboer, men i F er ikke f(g) og f(h) naboer. Derfor kan vi konkludere med at F og G ikke er isomorfe grafer.

Oppgave 2.1)

$n = 221 = 13 \cdot 17 \Rightarrow p = 13$ og $q = 17$

$e = 269$

$c = 76 \equiv m^e \mod n$

$76 \equiv m^{269} \mod 221 \Rightarrow 76 \equiv m^{269} \mod 13 \Rightarrow 11 \equiv m^{269} \mod 13$

$76 \equiv m^{269} \mod 17 \qquad 5 \equiv m^{269} \mod 17$

$e \cdot d \mod \phi(n) = 1$

$\phi = (p-1)\cdot(q-1) = 12 \cdot 16 = 192$

$269\, d \mod 192 = 1 \Rightarrow 77\, d \mod 192 = 1$

E.A.

$192 = 77 \cdot 2 + 38$

$77 = 38 \cdot 2 + 1$

$1 = 77 - 38 \cdot 2$

$= 77 - (192 - 77 \cdot 2) \cdot 2$

$= 77 - 192 \cdot 2 + 77 \cdot 4$

$= 77 \cdot 5 - 192 \cdot 2$ — jobber i mod 192 så kan stryke $192 \cdot 2$

$77 \cdot 5 \mod 192 = 1 \Rightarrow d = 5$

$m = c^d \mod n = 76^5 \mod 221$

$= (76)^4 \cdot (76)^1 \mod 221$

$76^1 \equiv 76 \mod 221$

$76^2 = 5776 \equiv 30 \mod 221$

$76^4 = (76^2)^2 = 30^2 = 900 \equiv 16 \mod 221$

$76^4 \cdot 76^1 = 16 \cdot 76 = 1216 \equiv 111 \mod 221$

$\underline{\underline{m = 111}}$

Oppgave 2.2)

Vi løser systemet av kongruensene:

$4x \equiv 5 \mod 9 \Rightarrow 4x \equiv 5 \mod 9$

$2x \equiv -1 \mod 7 \qquad 2x \equiv 6 \mod 7$

For å løse systemet må vi gjøre $4x$ og $2x$ om til bare x og x. Da må vi finne den inverse ved hjelp av E.A.:

$9 = 2 \cdot 4 + 1 \qquad 7 = 2 \cdot 3 + 1$

$1 = 9 - 2 \cdot 4 \qquad 1 = 7 - 2 \cdot 3$

-2 er invers til $4x \qquad -2$ er invers til $2x$

Da får vi kongruensene:

$-2\cdot 4x \equiv -2\cdot 5 \mod 9$
$-8 \equiv 10 \mod 9$
$-10 \equiv 8 \mod 9$

$-2\cdot 2x \equiv (-1)\cdot(-2) \mod 7$
$-4 \equiv 3 \mod 7$
$2 \equiv 9 \mod 7$

$x \equiv -10 = 8 \mod 9$

$x \equiv -4 = 3 \mod 7$

Vi jobber nå med systemet

$x \equiv a \mod m$ $\quad$ $x \equiv b \mod n$
$x \equiv 8 \mod 9$ $\quad$ $x \equiv 3 \mod 7$

$GCD(m,n) = GCD(7,9) = 1$

Det finnes $u, v \in \mathbb{Z}$, slik at

$mu \equiv 0 \mod m$ $\quad$ $nv \equiv 1 \mod m$
$mu \equiv 1 \mod n$ $\quad$ $nv \equiv 0 \mod n$

Vi finner c ved:

$c = a\cdot n\cdot v + b\cdot m\cdot u$

Finner v og u v.h.a. E.A. på 7 og 9

$7\cdot v + 9\cdot u = 1$
$7\cdot 4 + 9\cdot(-3) = 1 \Rightarrow v = 4$ og $u = -3$

$c = 8\cdot 7\cdot 4 + 3\cdot 9\cdot(-3)$
$= 224 + (-81$
$= 143$

Vi vet fra formel at $x \equiv c \pmod{mn}$

$x \equiv 143 \mod_{7\cdot 9}$
$x \equiv 143 \mod_{63}$
$x \equiv 17 \mod_{63}$

Sjekker 17 med originale kongruenser

$4\cdot 17 = 68 \equiv 5 \mod 9$
$9\cdot 7 + 5 \equiv 5 \mod 9$

$2\cdot 17 = 34 \equiv -1 \mod 7$
$7\cdot 5 - 1 \equiv -1 \mod 7$

Ser at $x = 17$ løser begge kongruensene og er da det minste positive heltallet som tilfredsstiller systemet.

$17 + 63k$, $k \in \mathbb{Z}$ er formel for alle løsninger til systemet.

Oppgave 3.1)

$n = \{x \in \mathbb{Z} : 1 \leq x \leq n\}$

$f : [2022] \to [1011]$ ved $f(x) = y$ h.b.h. $x \equiv y \mod_{1011}$

Løser $f(x) = y$ for de sitte verdiene til x:

$f(1) = 1$ siden $1 \equiv 1 \mod 1011$

$f(2) = 2$ siden $2 \equiv 2 \mod 1011$

$f(1011) = 0$ siden $1011 \equiv 0 \mod 1011$

$f(2022) = 0$ siden $2022 \equiv 0 \mod 1011$

Oppgave 3.2)

Er funksjonen f injektiv?

Hvis f er injektiv, sier da definisjonen at for $x, y \in A$ og $x \neq y$ impliser det at $f(x) \neq f(y)$.

I vår funksjon kan vi teste med 1 og 1012.

$1 \neq 1012$, men $f(1) = f(1012)$

siden $1 \equiv 1 \mod 1011$

og $1012 \equiv 1 \mod 1011$.

Vi ser da at f ikke er injektiv.

Oppgave 3.3)

Er funksjonen f surjektiv?

Etter definisjon er en funksjon $f : A \to B$ surjektiv hvis det for alle $y \in B$, finnes en $x \in A$ slik at $f(x) = y$.

I vår funksjon vil da for alle $y \in [1011]$, finnes en $x \in [2022]$ slik at $f(x) = y$.

Hvis $y = 1011$, finnes $x = 0$ og $x = 1011$ siden $f(0) = 1011$ og $f(1011) = 1011$

fordi $f(x) = y$ h.b.h $x \equiv y \mod 1011$ og

$0 \equiv 1011 \mod 1011$ og

$1011 \equiv 1011 \mod 1011$.

Vi ser at definisjonsområdet $[2022]$ er dobbelt så stort som verdiområdet $[1011]$.

Siden $x \in [2022]$ og $y \in [1011]$ og $f(x) = y$ h.b.h $x \equiv y \mod 1011$

Så for hver y finnes det 2 x som løser funksjonen. f.eks.

$f(1) = f(1012) = 1$

$f(10) = f(1021) = 10$

$f(1011) = f(2022) = 0$

Vi konkluderer med at f er surjektiv.

Oppgave 3.4)

Definerer en relasjon $R : [1011] \to [2022]$ ved $(x,y) \in R$
h.b.h. $x \equiv y \mod 2022$
Er relasjonen R en funksjon?

$(x,y) \in R$ betyr at $x \in [1011]$ og $y \in [2022]$, som vi kan skrive som xRy.
Kravet er at $x \equiv y \mod 2022$.
Altså vil feks.:
$(1,1) \in R$ siden $1 \equiv 1 \mod 2022$
$(1,2) \notin R$ siden $1 \not\equiv 2 \mod 2022$

Vi vet fra definisjon av funksjoner at grafen til $f: A \to B$
er "settet av ordnet parr (a,b) slik at $b = f(a)$. Siden f er et "subset"
av $A \times B$, er det en relasjon fra A til B. Dette tilsier også at
hvert element i A er startelementet i nøyaktig ett parr.

Vi kan oversette dette til vår funksjon f.
Vi har $f: [2022] \to [1011]$ ved $f(x) = y$ h.b.h $x \equiv y \mod 1011$.
Relasjonen $R : [1011] \to [2022]$ ved $(x,y) \in R$ h.b.h. $x \equiv y \mod 2022$
er en funksjon siden hvert element i $[1011]$ er ikke et start punkt i
nøyaktig ett parr. Vi sjekker:

$x = 1$, $1 \equiv 1 \mod 2022$
$(1,1)$ er et parr
$x = 1011$, $1011 \equiv 1011 \mod 2022$
$(1011, 1011)$ er et parr.

Konkluderer med at relasjonen R er en funksjon.

Oppgave 4.1)

La A være en mengde og la $\preccurlyeq$ være en partiell ordning på A.
Sier at $\preccurlyeq$ er rettet hvis for alle a og b i A, det finnes et
medlem c i A slik at $a \preccurlyeq c$ og $b \preccurlyeq c$.

$(\preccurlyeq \text{ er rettet}) \to (\forall a, b \in A)(\exists c \in A)(a \preccurlyeq c \wedge b \preccurlyeq c)$

Oppgave 5.1)

$n \in \mathbb{Z}^+$

$(\forall n \in \mathbb{Z}^+)\left(1\cdot(1!)+2\cdot(2!)+\ldots+n\cdot(n!)=(n+1)!-1\right)$

$P(n)=1\cdot(1!)+2(2!)+\ldots+n\cdot(n!)=(n+1)!-1$

Basissteg: $P(1)=1\cdot(1!)=(1+1)!-1 \quad =0$ ✓

$P(3)=1\cdot(1!)+2\cdot(2!)+3(3!)=(3+1)!-1$

$=1+4+18=24-1$

$=23=23$ ✓

Induksjons steg: Antar at $P(k)=1\cdot(1!)+2\cdot(2!)+\ldots+k\cdot(k!)=(k+1)!-1$ er sant for en vilkårlig k.

$1\cdot(1!)+2(2!)+\ldots+k(k!)+(k+1)((k+1)!)=((k+1)+1)!-1$

$1\cdot(1!)+2\cdot(2!)+\ldots+k(k!)+(k+1)((k+1)!)=(k+2)!-1$

$(k+1)!-1+(k+1)((k+1)!)=(k+2)!-1$

$(k+1)!+(k+1)((k+1)!)-1=(k+2)!-1$

$(1+(k+1))\cdot((k+1)!)-1=(k+2)!-1$

$(k+2)\cdot((k+1)!)-1=(k+2)!-1$

$(k+2)\cdot((k+1)!)-1=(k+2)\cdot(k+1)!-1$

Vi ser at begge sidene er lik for $P(k+1)$, og konkluderer med at påstanden er sann.

Oppgave 5.2)

Hvor mange 5-tupler av positive heltall (x_1,x_2,x_3,x_4,x_5) oppfyller $x_1+x_2+x_3+x_4+x_5=10$?
Siden det er tupler vet vi at rekkefølgen på tallene er viktig, og at samme tall kan forekomme i tupelen flere ganger.
Vi ser på muligheter, og legger til antall muligheter å ordne den:

$10 = (10,0,0,0,0) - 5 = 5$

$9 = (9,1,0,0,0) - 5\cdot4 = 20$

$8 = (8,1,1,0,0) - 5\cdot6 = 30$
$(8,2,0,0,0) - 5\cdot4 = 20$

$7 = (7,1,1,1,0) - 5\cdot4 = 20$
$(7,2,1,0,0) - 5\cdot12 = 60$
$(7,3,0,0,0) - 5\cdot4 = 20$

$6 = (6,1,1,1,1) - 5 = 5$
$(6,2,1,1,0) - 5\cdot12 = 60$
$(6,3,1,0,0) - 5\cdot12 = 60$
$(6,4,0,0,0) - 5\cdot4 = 20$

$5 = (5,2,1,1,1) - 5\cdot4 = 20$
$(5,2,2,1,0) - 5\cdot12 = 60$
$(5,3,1,1,0) - 5\cdot12 = 60$
$(5,3,2,0,0) - 5\cdot12 = 60$
$(5,4,1,0,0) - 5\cdot12 = 60$
$(5,5,0,0,0) - 5\cdot2 = 10$

$4 = (4,2,2,1,1) - 5\cdot6 = 30$
$(4,2,2,2,0) - 5\cdot4 = 20$
$(4,3,2,1,0) - 5! = 120$
$(4,3,3,0,0) - 5\cdot6 = 30$
$(4,3,1,1,1) - 5\cdot4 = 20$
$(4,4,1,1,0) - 5\cdot6 = 30$
$(4,4,2,0,0) - 5\cdot6 = 30$

$3 = (3,3,2,1,1) - 5\cdot6 = 30$
$(3,2,2,2,1) - 5\cdot4 = 20$
$(3,3,3,1,0) - 5\cdot4 = 20$

$2 = (2,2,2,2,2) - 1 = 1$

Sum = $\underline{\underline{941}}$

Så adderer vi alle de forskjellige mulighetene og får da at det er 941 mulige 5-tupler som fyller kravet om sum=10.