CHALMERS
EXAMINATION / TENTAMEN

Course code/kurskod	Course name/kursnamn			
DIT984	Diskret matematik för datavetare			
Anonymous code Anonym kod		Examination date Tentamensdatum	Number of pages Antal blad	Grade Betyg
DIT984-0006-FBC		03/01/2023	7+fusklapp	3

* I confirm that I've no mobile or other similar electronic equipment available during the examination.
Jag intygar att jag inte har mobiltelefon eller annan liknande elektronisk utrustning tillgänglig under eximinationen.

Solved task Behandlade uppgifter No/nr		Points per task Poäng på uppgiften	Observe: Areas with bold contour are to completed by the teacher. Anmärkning: Rutor inom bred kontur ifylles av lärare.
1	X	2	
2	X	2	+
3	X	1	−
4	X	0	+
5		−	
6	X	1	
7	X	2	
8			
9			
10			
11			
12			
13			
14			
15			
16			
17			
Bonus poäng			
Total examination points Summa poäng		8	

CHALMERS

Anonymous code / Anonym kod: DIT 984 - 0006 - FBC

Points for question (to be filled in by teacher) / Poäng på uppgiften (ifylles av lärare): 2

Consecutive page no. / Löpande sid nr: 1

Question no. / Uppgift nr: 1

1 a)

p	q	$(p \wedge q)$	$(\neg p \wedge \neg q)$	$[(p \wedge q) \vee (\neg p \wedge \neg q)]$
1	1	1	0	1
0	1	0	0	0
1	0	0	0	0
0	0	0	1	1

b)

p	q	$p \Rightarrow q$	$p \Leftarrow q$	$p \Leftrightarrow q$
1	1	1	1	1
0	1	1	0	0
1	0	0	1	0
0	0	1	1	1

CHALMERS	Anonymous code / Anonym kod	Points for question (to be filled in by teacher) / Poäng på uppgiften (ifylles av lärare)	Consecutive page no. / Löpande sid nr	Question no. / Uppgift nr
	DIT984-0006-FBC	2	2	2

2) Vi ska visa att $3 \mid 2^n+1$, $\begin{cases} n \text{ är udda} \\ n \in \mathbb{N} \end{cases}$

För att 3 ska kunna dela 2^n+1 måste 2^n+1 vara en multipel av 3.

Alltså: $2^n+1 \equiv 0 \pmod 3$

$$2^n+1 \equiv 0 \pmod 3$$

$$2^n \equiv -1 \pmod 3$$

$$2^n \equiv 2 \pmod 3$$

Fermats lilla sats säger att om p är prim och $p \nmid a$ gäller att: $a^{p-1} \equiv 1 \pmod p$.

I vårt fall gäller p är prim och $p \nmid a$, därmed får vi: $(2^n)^2 \equiv 1 \pmod 3$.

$$\boxed{\begin{aligned} (2^n)^2 &\equiv 1 \pmod 3 \\ 2^{2n} &\equiv 1 \pmod 3 \end{aligned}}$$

Exponenten 2n måste vara ett jämnt tal eftersom det är en multipel av två.

Alltså kan vi säga med säkerhet att exponenten inte får vara jämn. eftersom detta medför en rest.

Nu har vi kommit fram till att hela exponenten "n" i 2^n+1 inte kan vara jämn.

du är redan färdig!

Del två på nästa sida.

$$2^{2n} \equiv 1 \pmod 3 \Rightarrow 2 \cdot 2^{2n} \equiv 2 \cdot 1 \pmod 3$$

$$\Rightarrow 2^{2n+1} \equiv 2 \pmod 3$$

2) Eftersom vi vet att exponenten inte kan vara jämn ska vi nu kolla på vad som händer med udda exponenter.

Vi har en mängd U. Elementen i U är alla udda naturligen tal, $\{1, 3, 5, 7, 9 \dots\}$. Förenklat kan vi säga att alla element i U kan beskrivas

$2n+1, \quad n \in \mathbb{N}$.

Vi testar det enklaste fallet som är sant:

$$2^{2(0)+1}+1 = 2^1+1 = 3, \qquad 3 \mid 3$$

Vi antar nu att $3 \mid (2^{2k+1}+1)$ och därmed att $2^{2k+1}+1 \equiv 0 \pmod 3$.

Vi betraktar nu fallet $\left(2^{2(k+1)+1}+1\right)$:

$$2^{2(k+1)+1}+1 = 2^{2k+3}+1 = 2 \cdot 2 \cdot 2^{2k+1}+1$$

$$2 \cdot 2 \cdot 2^{2k+1}+1 \equiv 0 \pmod 3$$

$$2 \cdot 2^{2k+1}+1 \equiv 0 \pmod 3$$

$$2^{2k+1}+1 \equiv 0 \pmod 3$$

$$2^{2k+1}+1 \equiv 0 \pmod 3 \iff 2^{2(k+1)+1}+1 \equiv 0 \pmod 3$$

Q.E.D.

3) $5x + 12y = 3$

Vi måste först hitta gcd(12, 5):

$12 = 5(2) + 2$

$5 = 2(2) + \boxed{1}$ — gcd, bekräftas av att 5 är ett primtal, gcd(12,5) måste alltså vara 1.

$2 = 1(2) + 0$

gcd | 3, därmed finns det lösningar.

Vi kommer nu att lösa ut resten av våra ekvationer:

$$2 = 12(1) + 5(-2)$$
$$1 = 5(1) + 2(-2)$$

Nu kommer vi att använda substitution för att förhoppningsvis få fram svaret:

Vi substituerar 2.

$$1 = 5(1) + 2(-2)$$
$$= 5(1) + [12(1) + 5(-2)](-2)$$
$$= 5(1) + 12(-2) + 5(4)$$
$$= 5(5) + 12(-2)$$

$$\underbrace{5(5)}_{u} + \underbrace{12(-2)}_{v} = 1 \leftarrow (au + bv = 1)$$

hur ?

I detta fall kan vi enkelt se att $x = 3, y = -1$ är ett svar till originalekvationen. Samtliga svar kan beskrivas:

$$x_k = 3 + \cancel{5k}$$
$$y_k = (-1) - \cancel{12k}$$

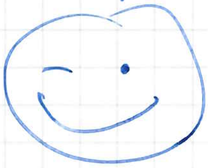
2

CHALMERS	Anonymous code	Points for question (to be filled in by teacher)	Consecutive page no. Löpande sid nr 5
	Anonym kod DIT984-0006-FBC	Poäng på uppgiften (ifylles av lärare) 0	Question no. Uppgift nr 4

4 a) Falskt

b) Sant

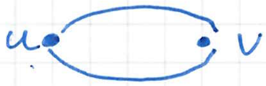
Jag har ett mycket elegant bevis men tyvärr får det inte plats här.



2

CHALMERS	Anonymous code / Anonym kod	Points for question (to be filled in by teacher) / Poäng på uppgiften (ifylles av lärare)	Consecutive page no. / Löpande sid nr	6
	DIT984-0006-FBC	1	Question no. / Uppgift nr	6

6) Vi har en enkel och oriktad graf G.
Det är alltså inte tillåtet att en nod har en kant till sig själv eller att två godtyckligen noder u & v har kanter enligt:



Samtidigt måste varje nod åtminstonne ha två kanter, ty gradtal enligt uppgiften är > 1.

Om vi tillåt två av noderna att ha gradtal 1 hade vi garanterat haft två ändar, en början och ett slut.

Om vi tänker oss att vi ritar en nod, a, måste vi rita en till nod, a+1, för att skapa en kant (ty gradtal minst 2). Vi ritar godtyckligt många noder med gradtal ≥2.
När vi har ritat alla noder måste vi fortfarande dra en kant mellan a och en annan nod. Vi får inte dra en kant till a+1 eftersom denna redan finns.
Vi har inget val än att skapa en kant mellan a och en nod som redan nås indirekt genom nod (a+1).

Vi måste alltså skapa en cykel för att kunna upprätthålla gradtalet.

CHALMERS	Anonymous code / Anonym kod	Points for question (to be filled in by teacher) / Poäng på uppgiften (ifylles av lärare)	Consecutive page no. / Löpande sid nr
	DIT984-0006-FBC	2	7
			Question no. / Uppgift nr: 7

7) Vi letar efter permutationer av talen 0, 1, 2, 3, 4 som ger oss summan 4.
Möjliga sätt att göra detta är:

I) fyra st. 1, sex st. 0
II) två st. 2, åtta st. 0
III) en st. 1, en st. 3, åtta st. 0
IV) en st. 2, två st 1, sju st. 0
V) en st. 4, nio st. 0

Om man vill räkna ut antalet permutationer av bokstäver i ett ord kan man dela antalet bokstäver i fakultet med de bokstäver som repeteras i fakultet. Vi kan betrakta våra olika fall som ord.

I) $\frac{10!}{6!\,4!} = \frac{10\cdot 9\cdot \cancel{8}\cdot 7\cdot \cancel{6\cdot 5\cdot 4\cdot 3\cdot 2\cdot 1}}{\cancel{6\cdot 5\cdot 4}\cdot 3\cdot \cancel{2\cdot 1}\cdot \cancel{4\cdot 3\cdot 2\cdot 1}} = \frac{10\cdot 9\cdot 7}{3} = \boxed{10\cdot 7\cdot 3}$

II) $\frac{10!}{8!\,2!} = \frac{10\cdot 9\cdot 8!}{8!\,2!} = \frac{10\cdot 9}{2!} = \boxed{9\cdot 5}$

III) $\frac{10!}{1!\,1!\,8!} = \frac{10!}{8!} = \boxed{10\cdot 9}$

IV) $\frac{10!}{1!\,2!\,7!} = \frac{10!}{2!\,7!} = \frac{10\cdot 9\cdot 8}{2} = \boxed{10\cdot 9\cdot 4}$

V) $\frac{10!}{1!\,9!} = \boxed{10}$

Svar: $(10\cdot 7\cdot 3) + (9\cdot 5) + (10\cdot 9) + (10\cdot 9\cdot 4) + 10$

Induktion

1. Visa att hypotes stämmer för basfall
2. Anta att det stämmer för $n = k$
3. Förenkla om möjligt med hjälp av $n=k$
4. Visa $n = k+1$

Fermats lilla sats

Om p är prim och $p \nmid a$ gäller: $a^{p-1} \equiv 1 \pmod{p}$.
Kan användas för att räkna ut resten av stora kongruenser.

Fermats sista sats

$x^n + y^n = z^n$, $n > 2$ har inga lösningar

Diofantiska ekvationer

$ax + by = c$

1. Om $\gcd(a,b) \nmid c$ finns ej lösningar
2. Skriv det största av talen a, b på formen: $\boxed{a = bq + r}$ (Alltså dela det största i det minsta.)
3. Dela "r" med ditt nya "a".
4. Repetera tills vi når gcd.
5. Lös ut "r" ur alla ekvationerna.
6. Börja med ekvationen för gcd och substituera bakåt tills vi når den första resten.
7. Multiplicera endast koeff. i parenteserna. Dessa kommer bli x o y.
8. Kontrollera svaret mot originalet.

Alla lösningar

Måste ha formen $\boxed{au + bv = 1}$, för att få detta kan man dela med gcd.

$$\boxed{\begin{aligned} X_k &= X + k \cdot a \\ Y_k &= Y - k \cdot a \end{aligned}}$$

Additionsprincipen:

Addera de kombinationer som finns

Subtraktionsprincipen

Subtrahera alla otillåtna kombinationer

Multiplikationsprincipen

Multiplicera alla fristående val man kan göra.

Divisionsprincipen

Delar bort otillåtna permutationer

Permutationer

Ordningen av element spelar roll.
Formel: $nP_k = \frac{n!}{(n-k)!}$

Kombinationer

Ordningen av element spelar ingen roll.
Formel: $nC_k = \frac{n!}{(n-k)!\,k!}$

$\binom{n}{k} = \frac{n!}{(n-k)!\,k!}$

Om du ska räkna ut permutationer av bokstäver i ett ord, dela antalet bokstäver i fakultet med antalet repeterande bokstäver i fakultet.

Kongruenser

$a \equiv b \pmod{n}$
Samma sak som:

1. a och b har samma rest när de delas med n.
2. $a = k \cdot n + b$
3. $n \mid (a-b)$ ($a-b$ är en multipel av n)

Att lösa kongruenser

1. Division får endast ske när $\gcd(a,n) = 1$: $\boxed{ax \equiv b \pmod{n}}$
2. Tänk på att vi kan lägga till och ta bort mod för att förenkla.
3. Vi vill inte ha bråktal. ex: $x \equiv \frac{1}{2} \pmod{5}$
4. Negativa tal är ok.

System av kongruenser

Om modulona i systemet är parvis relativt prim kan vi använda kinesiska restsatsen.
Vi kan fortfarande ha lösningar om satsen inte är applicerbar men med satsen är det garanterat.

Gör såhär:

1. Skriv om första kongruensen som en ekvation: $a = k \cdot n + b$
2. Substituera detta "a" in i kongruens två.
3. Lös ut "n" ur kongruensen.
4. Skriv om "n" som en ekvation likt steg 1.
5. Substituera denna ekv. in för "n" i ekv. ett.
6. Förenkla och stoppa in som "a" i den sista kongruensen (om det bara är tre)
7. Du har nu en kongruens som du kan lösa som vanligt.
8. Stoppa in det du får ut här in i sista kongruensens ekv. för att slutligen få ut svaret.

(Om modulon är relativt koprim borde svaret innehålla deras produkt)

Grafteori

Noder är punkter i en graf. Kanter kopplar samman noder. Maximalt antal kanter i en enkel graf med n noder är $\frac{n(n-1)}{2}$. Antalet kanter en nod har kallas gradtal.
Sammanhängande grafer är grafer där alla noder är direkt eller indirekt sammanlänkade. För alla enkla grafer gäller att $\sum_{u \in V} \deg(u) = |E| \cdot 2$. En väg i en graf är en sekvens av noder där det finns en kant mellan intilliggande noder. En tom väg har bara en nod. I en enkel väg repeteras inga noder. I en sluten väg är början och slutet samma nod. I en cykel upprepas inga noder förutom början/slutet, en sluten väg. En "Eulercykel" är en sluten väg där alla kanter i en graf används exakt en gång. Euler $\Rightarrow$ Sammanhängande
Euler $\Rightarrow$ Alla noder jämnt gradtal
I en enkel graf finns max en kant mellan noder. Ingen kant från u till u. I en riktad graf är $(u \to v) \neq (v \to u)$. Loopar $(u \to u)$ får förekomma.
Topologisk ordning förekommer i riktade grafer med en sekvens där alla noder i V förekommer en gång så att alla pilar går V till H.
Om cykel ingen top. ordning.