

Matematik, KTH

B.Ek

Efternamn	förnamn	personnr

**Kontrollskrivning 4, må 14 april 2014, 10.30–12.00,
i SF1662 Diskret matematik för CLGYM1, TSVDK2**

Inga hjälpmedel tillåtna.

Minst 8 poäng ger godkänt.

Godkänd ks n medför godkänd (3p) uppgift n vid tentor till (men inte med) nästa ordinarie tenta (högst ett år), $n = 1, \dots, 5$.

13–15 poäng ger ett ytterligare bonuspoäng vid samma tentor.

Uppgifterna 3)–5) kräver väl motiverade lösningar för full poäng.

Uppgifterna står inte säkert i svårighetsordning.

Spara alltid återlämnade skrivningar till slutet av kursen!

Skriv dina lösningar och svar på samma blad som uppgifterna, använd baksidan om det behövs.

1) (För varje delfråga ger rätt svar $\frac{1}{2}$ p, inget svar 0p, fel svar $-\frac{1}{2}$ p. Totalpoängen på uppgiften rundas av uppåt till närmaste icke-negativa heltal.)

Kryssa för om påståendena **a)–f)** är sanna eller falska (eller avstå!)

poäng uppg.1

	sant	falskt
a) Om $a, b, c \in G$, en grupp, och $ab = bc$ gäller säkert $a^{-1}bc = abc^{-1}$.		
b) Om H är en delgrupp till G och $g \in G$ finns säkert $g' \in G$ med $gH = Hg'$.		
c) Varje ring är också en kropp.		
d) Om $z \in \mathbb{Z}[i]$ och $ z ^2$ är ett (reellt) primtal, är z säkert ett gaussiskt primtal.		
e) Antalet rotationssymmetrier för en kub är 18.		
f) Ett RSA-system med offentlig nyckel $(n, e) = (187, 7)$ kan ha dekrypteringsparameter $d = 13$. $[187 = 11 \cdot 17]$		

Resultat på skrivningen:

Fylls i av rättaren

p 1	p 2	p 3	p 4	p 5	Σ p	G/U	bonus

SF1662 CLGYM1, TSVDK2, ks4 14.4-14

Namn	poäng uppg.2

2a) (1p) Vad innebär det (dvs hur definieras) att en grupp $(G, *)$ är **abelsk**?

b) (1p) Faktorisera $7 + 9i$ i gaussiska primtal.

c) (1p) Finn alla $a \in \mathbb{Z}_3$ sådana att $f(x) = x^3 + 2x + a$ är irreducibelt i $\mathbb{Z}_3[x]$.
Motivera.

Namn	poäng uppg.3

3) Låt $(G, *)$, där $G = \{a, b, c, d, f\}$, vara en grupp med 5 element. Grupptabellens två första rader syns nedan, delvis ifyllda.

$*$	a	b	c	d	f
a	f	d	–	–	–
b	–	a	–	–	–

a) (1p) Vad är $o(b)$, ordningen för elementet b ?
Glöm inte att motivera varför andra värden är uteslutna.

b) (1p) Vilken av a , b , c , d och f är 1, identitetselementet i G ? Motivera.

c) (1p) Fyll i de sju tomma positionerna i grupptabellens två första rader ovan. Motivera här:

Namn	poäng uppg.4

4a) (2p) Vad blir den minsta icke-negativa resten då 24^{100} divideras med 17?

b) (1p) Vad blir den minsta icke-negativa resten då 24^{100} divideras med 21?

Namn	poäng uppg.5

5) Låt $G = U(\mathbb{Z}_{12})$ (som vanligt) vara gruppen av de inverterbara (under $\cdot$) elementen i ringen $(\mathbb{Z}_{12}, +, \cdot)$.

a) (1p) Ange alla element i G .

b) (1p) Vi låter gruppen G verka på mängden $X = \mathbb{Z}_{12}$ med multiplikationen i $(\mathbb{Z}_{12}, +, \cdot)$.

Finn stabilisatorn G_2 och banan $G2$ för elementet $2 \in X$.

c) (1p) Ange alla banor för G 's verkan på X (med verkan beskriven i b)).