

Efternamn, förnamn	personnummer	program	blad	uppg.
			1	1,4

Matematik, KTH

B.Ek

**Kontrollskrivning 4, må 24 april 2017, 8.00–10.00,
i SF1662, Diskret matematik**

Examinator: Bengt Ek, tel 790 6951.

Tillåtna hjälpmedel: Inga (utom penna och sudd), inte ens räknedosa.

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.

För in dina svar på uppgift 1 i rutorna nedan och lämna in detta blad tillsammans med övriga lösningsblad.

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)!

	sant	falskt
a) Om $(G, *)$ är en grupp och $a * (b * c) = (a * b) * c$ för alla $a, b, c \in G$, är G säkert en cyklisk grupp.		
b) Alla grupper av ordning 19 är isomorfa .		
c) Varje ring är också en kropp.		
d) Om S är en högersidoklass till en delgrupp H i en ändlig grupp G , finns säkert $n \in \mathbb{Z}_+$ med $ G = n S $.		
e) $f(x) = x^3 + x^2 + 2 \in \mathbb{Z}_3[x]$ är ett irreducibelt polynom.		
f) Ett carmichaeltal är ett primtal som för minst en bas inte klarar fermattestet.		

Vänd!

Lösningar på följande uppgifter skrivs på separata papper.

2a) (1p) Hur många element har rotationssymmetrigruppen för ett triangulärt prisma med fem sidoytor, två motstående liksidiga trianglar och tre kvadrater?

b) (1p) Faktorisera $17 - 7i$ i gaussiska primtal (dvs i irreducibla faktorer i $\mathbb{Z}[i]$).

c) (1p) Vad blir (minsta icke-negativa) resten då $24^{4^{2017}}$ (dvs $24^{(4^{2017})}$) divideras med 13?

Motivera kortfattat svaren i a) och c).

3) Låt G vara $U(\mathbb{Z}_{24})$, mängden av inverterbara (m.a.p. multiplikation, förstås) element i $\mathbb{Z}_{24}$. $(G, \cdot)$ är då en grupp (det behöver du inte visa).

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

b) (2p) Avgör (med motivering) om $(G, \cdot)$ är en **cyklisk** grupp.

4) (3p) I grupptabellen för gruppen $(G, *)$ finns två rader som här till höger.

Fyll i så många som möjligt av de tomma positionerna (markerade $-$).

Lämna motiveringar till det du fyllt i på ett separat blad.

$*$	a	b	c	d	f	g
a	b	$-$	$-$	c	$-$	$-$
b	$-$	b	$-$	$-$	$-$	$-$

5) (3p) I samband med ett livligt födelsedagsfirande råkade Donald och Vladimir blanda ihop (de offentliga) nycklarna till sina (små) RSA-system.

Donald har hemlig avkrypteringsparameter $d = 33$ och Vladimir har $d = 35$.

Deras offentliga "stora" tal n var (i storleksordning) 119 och 145, medan deras krypteringsparametrar (också i storleksordning) var $e = 11$ och $e = 17$.

Avgör (med motivering) vilket n och vilket e som hörde till var och en av dem.

Lösningar kommer att läggas ut på kurssidan efter skrivningen.