

Matematik, KTH

B.Ek

Efternamn	förnamn	personnr

**Kontrollskrivning 4, må 6 maj 2013, 9.00–10.00,
i SF1662 Diskret matematik för CL1**

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 $(G, *)$ är en grupp och $g * h^{-1} = g^{-1} * h$, $g, h \in G$, måste $g = h$.		
b) Om G och H är grupper är de direkta produkterna $G \times H$ och $H \times G$ säkert isomorfa.		
c) Om p, q är två olika primtal, är $(\mathbb{Z}_{pq}, +, \cdot)$ en kropp.		
d) Om gruppen G verkar på mängden X är för varje $x \in X$ säkert $\{g \in G \mid gx = x\}$ en delgrupp till G .		
e) Om $a, b \in \mathbb{Z}$ är sådana att $a + bi$ är ett gaussiskt primtal, måste $a^2 + b^2$ vara ett (reellt) primtal.		
f) Om n är ett udda heltal, $n \geq 3$ och $2^n \equiv 2 \pmod{n}$ är n säkert ett primtal.		

Resultat på skrivningen:

Fylls i av rättaren

p 1	p 2	p 3	p 4	p 5	Σ p	G/U	bonus

SF1662 CL1, ks4 6.5-13

Namn	poäng uppg.2

2a) (1p) Ett element g i en grupp $(G, *)$ uppfyller $g^{75} = 1$ (dvs $\underbrace{g * g * \dots * g}_{75 \text{ st}} = 1$), där 1 är G :s identitetselement.

Ange alla möjliga värden för $o(g)$, g :s ordning.

b) (1p) Faktorisera $21 + 9i$ i gaussiska primtal.

c) (1p) Är $f(x) = 2x^3 + 3x^2 + x + 3$ reducibelt i $\mathbb{Z}_5[x]$?

Svaret skall motiveras, men faktorisering krävs inte även om svaret är ”ja”.

Namn	poäng uppg.3

3) (3p) Låt $G = \{e, a, b, c, d\}$ vara en grupp med 5 element. Fyll i de sju namn som fattas i grupptabellens två första rader nedan. Motivera kortfattat varför just dessa namn skall stå där.

	e	a	b	c	d
e	–	a	–	–	–
a	–	c	–	–	e

Namn	poäng uppg.4

4) (3p) Avgör (med motivering) om gruppen $(\mathbb{Z}_{61} \setminus \{0\}, \cdot)$ genereras av elementet $8(= 2^3)$.

Namn	poäng uppg.5

5) (3p) I ett RSA-system för kryptering används parametern $e = 15$ i krypteringsfunktionen.

Visa att precis ett av värdena 75, 85, 95 är möjligt för "det stora talet n " och ange det värdet.

Kan man för det n -värdet ta dekrypteringsparametern $d = 7$? Motivera.

Lösningar kommer att läggas ut på kurssidan efter skrivningen.