

Matematik, KTH

B.Ek

Efternamn	förnamn	personnr

**Kontrollskrivning 4, må 27 april 2015, 8.30–10.00,
i SF1662 Diskret matematik**

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 det i en grupptabell står 1 (identitets-elementet) i rad i , kolumn j , står det också 1 i rad j , kolumn i .		
b) Om antalet element i en grupp är ett primtal är gruppen säkert abelsk.		
c) Om G är en grupp, $ G = n$ ($\in \mathbb{N}$) och $g \in G$ uppfyller $g^s = 1$ (G :s identitets-element), så är säkert $g^{\text{sgd}(s,n)} = 1$.		
d) Om $z \in \mathbb{Z}[i]$ och 61 är en delare till $ z ^2$ (dvs $61 \mid z ^2$), måste $\frac{z}{6+5i} \in \mathbb{Z}[i]$.		
e) Om polynomet $f(x) \in F[x]$ (F en kropp) är reducibelt så är säkert $f(a) = 0$ för något $a \in F$.		
f) Om en grupp G verkar på en mängd X gäller för alla $x \in X$ att $ Gx \mid G $ (där Gx är banan för x).		

Resultat på skrivningen:

Fylls i av rättaren

p 1	p 2	p 3	p 4	p 5	Σ p	G/U	bonus

SF1662, ks4 27.4-15

Namn	poäng uppg.2

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

b) (1p) Finn positiva heltal x och y sådana att $(18\,241 = 17 \cdot 29 \cdot 37)$

$$x^2 + y^2 = 18\,241.$$

c) (1p) Vad innebär **fermattestet med bas b** för att testa primalitet för ett tal N och hur tolkas resultatet?

Namn	poäng uppg.3

3) Låt $(G, *)$, där $G = \{p, q, r, s, t, u\}$, vara en grupp med 6 element och nedanstående grupptabell.

$*$	p	q	r	s	t	u
p	t	r	u	p	s	q
q	u	s	t	q	r	p
r	q	p	s	r	u	t
s	p	q	r	s	t	u
t	s	u	q	t	p	r
u	r	t	p	u	q	s

a) (1p) Vilket av p, q, r, s, t, u är G :s identitetsselement?

b) (1p) Ange en delgrupp H till G med precis två element.

c) (1p) Finn alla H :s vänster- och högersidoklasser i G .
Vänstersidoklasserna är:

Högersidoklasserna är:

Namn	poäng uppg.4

4) Man vill skapa ett (pytte-)RSA-system för kryptering med den offentliga nyckeln (n, e) , där e skall vara 21.

a) (1p) Välj bland de udda talen 81, 83, $\dots$, 97, 99 ett möjligt värde för n .

b) (1p) Finn en dekrypteringsparameter d för n -värdet från uppgift a. och $e = 21$.

c) (1p) Finn 10^{8823} i $\mathbb{Z}_{473}$ (dvs finn $x \in \mathbb{Z}$ med $0 \leq x < 473$ och $x \equiv 10^{8823} \pmod{473}$).
Motivera ordentligt. $[473 = 11 \cdot 43]$

Namn	poäng uppg.5

5) Låt $G = U(\mathbb{Z}_{34})$ (som vanligt) vara gruppen av de inverterbara (under $\cdot$) elementen i ringen $(\mathbb{Z}_{34}, +, \cdot)$.

a) (1p) Ange G :s ordning, dvs dess storlek $|G|$.

b) (1p) Finn ordningen $o(3)$ för elementet 3 i G (i boken betecknad $\text{order}(3)$).

c) (1p) Finn ordningen $o(13)$ för elementet $13 \in G$.

Lösningar kommer att läggas ut på kurssidan efter skrivningen.