Efternamn, förnamn	personnummer	program	blad	uppg.
			1	1

Matematik, KTH
B.Ek

Kontrollskrivning 4, må 25 april 2016, 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), $n = 1, \ldots, 5$.
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)	För alla grupper G och alla $x, y \in G$ sådana att $x^2 = y^2$ är också $x = y$.		
b)	Om A, B är högersidoklasser till samma delgrupp H till gruppen G, finns det säkert en bijektion $f : A \to B$.		
c)	$(\mathbb{R}, +, \cdot)$, de reella talen med operationerna addition och multiplikation, utgör en ring.		
d)	Ett (icke-konstant) polynom med rationella koefficienter är säkert irreducibelt om det saknar reella nollställen.		
e)	G (en ändlig grupp) verkar på X (en mängd). Om $x, y \in X$ har lika stora banor ($\lvert Gx\rvert = \lvert Gy\rvert$) är stabilisatorerna säkert lika stora ($\lvert G_x\rvert = \lvert G_y\rvert$).		
f)	Om $N \in \mathbb{N}$, $N \geq 2$, och för alla $b = 1, 2, \ldots, N-1$ gäller att $b^{N-1} \equiv 1 \pmod{N}$ är N säkert ett primtal.		

Vänd!

Lösningar på följande uppgifter skrivs på separata papper.

2a) (1p) Låt $\phi : \mathbb{Z}_3 \to \mathbb{Z}_3$ ges av $\phi(0) = 0$, $\phi(1) = 2$, $\phi(2) = 1$.
Är ϕ en isomorfi av gruppen $(\mathbb{Z}_3, +)$ på sig själv (en s.k. automorfi)?

b) (1p) Faktorisera $7 - 11i$ i gaussiska primtal (dvs i irreducibla faktorer i $\mathbb{Z}[i]$).

c) (1p) Vad blir (minsta icke-negativa) resten då 1071^{795} divideras med 13?
Motivera svaren i a) och c).

3) Låt $(G, *)$, där $G = \{u, v, x, y, z\}$, vara en grupp med 5 element och vidstående (delvis ifyllda) grupptabell.

$*$	u	v	x	y	z
u	x	_	y	z	_
v	_	_	_	_	_
x	_	_	_	_	_
y	_	_	_	_	_
z	_	_	_	_	_

a) (1p) Vad är $o(u)$, u:s ordning (order(u) i boken)?

b) (1p) Vilket är G:s identitetselement?

c) (1p) Ställ upp hela G:s grupptabell.

4) Låt $G = U_{22}$ vara gruppen av de inverterbara (under $\cdot$) elementen i ringen $(\mathbb{Z}_{22}, +, \cdot)$.

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

b) (2p) Avgör om G är en cyklisk grupp och ange i så fall en generator för G.

5) För ett (litet) RSA-system för kryptering har man valt den offentliga parametern $n = 299\,(= 13 \cdot 23)$.

a) (1p) Man tar den offentliga krypteringsexponenten e till det minsta möjliga värde som är ≥ 32. Vad blir e?

b) (2p) Finn en dekrypteringsexponent d med $1 < d < n$ för ovanstående RSA-system.

Lösningar kommer att läggas ut på kurssidan efter skrivningen.