Matematik, KTH
B.Ek

Efternamn	förnamn	pnr	program

Kontrollskrivning 4, må 14 maj 2012, 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), $n = 1, \ldots, 5$.
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.
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 finns säkert för varje $g \in G$ (minst) ett $h \in G$ så att $h * h = g$.		
b)	Alla grupper av ordning 23 är **isomorfa**.		
c)	Varje ring är också en kropp.		
d)	Om gruppen G verkar på mängden X (båda ändliga) är **antalet banor** $\frac{1}{\lvert G\rvert}\sum_{x\in X}\lvert G_x\rvert$ (där $G_x = \{g \in G \mid gx = x\}$).		
e)	$13^{242} \equiv 26 \pmod{143}$ [$143 = 11 \cdot 13$].		
f)	Ett **carmichaeltal** är ett primtal som för minst en bas inte klarar fermattestet.		

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 14.5-12

Namn	poäng uppg.2

2a) (1p) Vi vet att gruppen $(G, *)$ med $G = \{a, b, c, d, e, f, g\}$ (där a, b, c, d, e, f, g alla är olika) uppfyller att

$$a * a = b \text{ och } b * b = c.$$

Vad är $c * c$?
Motivera kortfattat ditt svar.

b) (1p) Låt H vara en delgrupp till gruppen G. G verkar på

$$X = \{gH \mid g \in G\},$$

mängden av H:s vänstersidoklasser, enligt $g(hH) = (gh)H$ (du behäver inte visa att detta är en gruppverkan på X).
Vad är **stabilisatorn** för H (som element i X) under denna verkan?

c) (1p) Formulera **Fermats lilla sats**.
Var noga med att inte missa någon förutsättning.

Namn	poäng uppg.3

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 (vilket du inte behöver visa).

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

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

Namn	poäng uppg.4

4) (3p) Låt $m \in \mathbb{Z}_+$ och (som vanligt) $\mathbb{Z}_m = \{0, 1, \ldots, m-1\}$.
Visa att funktionen $\phi : \mathbb{Z}_m \to \mathbb{Z}_m$, som ges av

$$\phi(x) = \begin{cases} 0 & \text{om } x = 0 \\ m - x & \text{om } x \in \mathbb{Z}_m \setminus \{0\}, \end{cases}$$

(så $\phi(x) = -x$ med vanliga beteckningar) är en **isomorfi** mellan $(\mathbb{Z}_m, +)$ och $(\mathbb{Z}_m, +)$ själv (en s.k. automorfi).

Namn	poäng uppg.5

5) I samband med ett livligt födelsedagsfirande råkade Fred och George blanda ihop (de offentliga) nycklarna till sina (pytte-)RSA-system.
Fred har den hemliga avkrypteringsparametern $d = 33$ och George 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.