KTH Matematik
Examinator: Petter Brändén
Kursansvarig: Olof Sisask

Σ p	G/U	bonus

Efternamn	förnamn	pnr

Kontrollskrivning 1A till SF1610 Diskret Matematik, för CINTE, vt2018

Inga hjälpmedel tillåtna.
Minst 8 poäng ger godkänt.
Godkänd KS nr n medför godkänd 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 till tentamen.
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)!

	sant	**falskt**
a) Om både a och b är sammansatta tal, då är $\gcd(a, b) > 1$.		X
b) Mängden $A = \{x \in \mathbb{Z} : 2 \mid x \text{ och } 3 \mid x\}$ är uppräkneligt oändlig.	X	
c) Låt $n = 10! = 10 \cdot 9 \cdot \cdots \cdot 2 \cdot 1$. Inga tal x i $\mathbb{Z}_n$ är inverterbara.		X
d) För godtyckliga heltal med $a > b \geq 1$ gäller det att $\gcd(a + b, b) = \gcd(a, a - b)$.	X	
e) Det finns en surjektiv funktion från $\mathbb{R}$ till $\mathbb{N}$.	X	
f) För alla heltal $a, b \geq 1$ gäller det att åtminstone en av de diofantiska ekvationerna $ax + by = 1$ och $ax + by = 2$ har en lösning.		X

poäng uppg.1

Namn	poäng uppg.2

2a) (1p) Finn samtliga lösningar till ekvationen $3x = 3$ i $\mathbb{Z}_6$. (Det räcker att ange rätt svar.)

Svar: Lösningarna är $x = 1$, $x = 3$ och $x = 5$.

b) (1p) Om a och b är positiva heltal med $\gcd(a, b) = 2$, vilka värden kan $\gcd(a^2, b^4)$ anta? (Det räcker att ange rätt svar.)

Svar: 4 och 16.

c) (1p) Beskriv (t.ex. genom att ge en formel) en bijektion $f : \mathbb{Z} \to \mathbb{Z}$ sådan att $f(1) = 0$ och $f(0) = 1$. (Det räcker att ange rätt svar.)

Svar:

$$f(x) = 1 - x$$

Namn	poäng uppg.3

3) (3p) Vilket av talen $0, 1, 2, \ldots, 40$ är $9^{40 \cdot 2^{100}+2}$ kongruent med modulo 41?
OBS. En komplett lösning med fullständiga motiveringar skall ges.

Lösning: Eftersom 41 är ett primtal så är $a^{40} \equiv 1 \pmod{41}$ så länge $41 \nmid a$, enligt Fermats lilla sats. Alltså har vi

$$9^{40 \cdot 2^{100}+2} = (9^{40})^{2^{100}} \cdot 9^2 \equiv 1^{2^{100}} \cdot 9^2 = 81 \equiv 40 \pmod{41}.$$

Alternativt, eftersom $9^2 = 81 \equiv -1 \pmod{41}$:

$$9^{40 \cdot 2^{100}+2} = 81^{20 \cdot 2^{100}+1} \equiv (-1)^{20 \cdot 2^{100}+1} = -1 \equiv 40 \pmod{41}.$$

Svar: 40.

Namn	poäng uppg.4

4) (3p) Låt en talföljd a_0, a_1, a_2, ... definieras rekursivt genom

$$\begin{aligned} a_0 &= 0 \\ a_n &= a_{n-1} + 4n + 3 \quad \text{för } n \geq 1. \end{aligned}$$

Bevisa via induktion att

$$a_n = 2n^2 + 5n \quad \text{för alla } n \geq 0.$$

OBS. Kom ihåg att ett bevis ska vara en förklaring. Fullständiga motiveringar skall ges.

Lösning: Låt $b_n = 2n^2 + 5n$ för $n \geq 0$ — vi vill visa att påståendet

$$P(n): \quad \text{"} a_n = b_n \text{"}$$

är sant för alla $n \geq 0$, vilket vi gör via induktion.

Basfall: För $n = 0$ är $a_0 = 0$ och $b_0 = 0$. Alltså stämmer $P(0)$.

Induktionssteg: Vi visar nu att om $P(n-1)$ är sant (dvs $a_{n-1} = b_{n-1}$) för något $n \geq 1$, då är också $P(n)$ (dvs påståendet "$a_n = b_n$") sant. Vi har nämligen att

$$\begin{aligned} a_n &= a_{n-1} + 4n + 3 \\ &= b_{n-1} + 4n + 3 \\ &= 2(n-1)^2 + 5(n-1) + 4n + 3 \\ &= 2(n^2 - 2n + 1) + 5n + 4n - 2 \\ &= 2n^2 + 5n \\ &= b_n. \end{aligned}$$

Alltså är $P(n)$ sant.

Slutsats: Enligt induktionsprincipen gäller därför att $a_n = b_n$ för $n = 0, 1, 2, \ldots$.

Namn	poäng uppg.5

5) (3p) Lös, i $\mathbb{Z}_{19}$, ekvationssystemet

$$\begin{cases} 3x + 4y &= 1 \\ 2x - y &= 2. \end{cases}$$

OBS. En komplett lösning med fullständiga motiveringar skall ges.

Den första ekvationen plus 4 gånger den andra ger att för alla lösningar gäller

$$11x = 9.$$

Eftersom 19 är ett primtal (och $19 \nmid 11$) så är 11 inverterbart modulo 19, alltså finns det en unik lösning x till ekvationen (nämligen $x = 11^{-1} \cdot 9$). För att hitta denna lösning omvandlar vi till den motsvarande diofantiska ekvationen

$$11x + 19m = 9.$$

Om vi börjar använda Euklides algoritm på koefficienterna får vi:

$$\begin{aligned} 19 &= 1 \cdot 11 + 8 \\ 11 &= 1 \cdot 8 + 3, \end{aligned}$$

och här stannar vi, eftersom högerledet vi vill få fram är 9, som är delbart med 3. Vi använder nu dessa två rader för att skriva om 3 som en kombination av 11 och 19, för att sedan multiplicera igenom med $9/3 = 3$ för att få 9:

$$\begin{aligned} 3 &= 11 - 8 \\ &= 11 - (19 - 11) = 2 \cdot 11 - 19 \end{aligned}$$

Multiplicera igenom med 3:

$$9 = 6 \cdot 11 - 3 \cdot 19.$$

Alltså är

$$11 \cdot 6 \equiv 9 \pmod{19},$$

så det unika värdet på x vi sökte är

$$x = 6.$$

Med hjälp av den andra ekvationen löser vi sedan ut y (som vi på detta sätt också ser bara kan ta ett värde):

$$y = 2x - 2 = 10.$$

Svar: Den unika lösningen ges av $x = 6$ och $y = 10$.