

*Skrivtid:* 14-19. *Inga hjälpmödel.* Alla svar ska **MOTIVERAS**.

Varje uppgift är värd 5 poäng. Minst 18 poäng krävs för betyget 3, 25 för betyget 4 och 32 för betyget 5.

*Vänligen påbörja varje uppgift på en ny sida och skriv enbart på papperets ena sida.*

**LYCKA TILL!**

- 1.** Bestäm det minsta positiva heltal som är kongruent med uttrycket modulo 7:

$$5^{2010} + (2010)^5$$

- 2. a)** Lös ekvationen  $x^2 + x = 0$  i  $(\mathbf{Z}_6[x], +_6, \times_6)$ .

**b)** Avgör om det går att skriva polynomet  $f(x) = x^2 + x$  i  $\mathbf{Z}_6[x]$  entydigt som en produkt av polynom av grad 1.

- 3.** Låt  $H$  vara den  $3 \times 6$ -matris som har som kolonner binära representationer av talen 1, 2, 3, 4, 5, 6.

**a)** Hur många kodord innehåller den kodmängd som genereras av  $H$ ? Ange dessa.

**b)** Hur stort fel kan säkert rättas med denna kodmängd?

**c)** Visa att 111100 inte är ett kodord och ange en procedur för att rätta det utsända meddelandet 111100 så att man får ett kodord i  $H$ .

- 4.** Låt  $G = (V, E)$  vara en graf. Komplementet  $H = (V, F)$  har samma hörn som  $G$  och en kant är med i  $F$  om den inte är med i  $E$ . Visa att en cykel med  $n$  hörn är isomorf med sitt komplement om och endast om  $n = 5$ .

- 5.** I RSA-algoritmen låt  $p$  och  $q$  vara primtal, så att  $p > q$  och låt  $n = p \cdot q$ . Låt vidare  $r = \Phi(n)$ , där  $\Phi$  är Eulers  $\Phi$ -funktion. Vi vill visa att om  $n$  och  $r$  är kända, så kan vi bestämma  $p$  och  $q$ .

**a)** Visa att  $p + q = n - r + 1$ .

**b)** Visa att  $(p - q)^2 = (n - r + 1)^2 - 4n$ .

**c)** Ange  $p$  respektive  $q$  som uttryck i  $n$  och  $r$ .

- 6. a)** Låt  $R$  bestå av alla tvåställiga relationer på mängden  $\mathbf{Z}_n$ .

Sammansättningsoperationen på  $R$  definieras genom:

$$R \circ S = \{(a,b) \mid \text{det finns något } c \text{ i } \mathbf{Z}_n \text{ så att } (a,c) \in R \text{ och } (c,b) \in S\},$$

där  $R$  och  $S$  är två tvåställiga relationer på mängden  $\mathbf{Z}_n$ .

Visa att det finns en enhet i  $R$  med avseende på o. Ange också vilka relationer i  $R$  som har inverser. Visa genom motexempel att  $\circ$  inte är kommutativ.

- b)** Ange i ett Hassediagram hur alla tvåställiga relationer på mängden  $\mathbf{Z}_2$  är ordnade medelst inklusion.

7. a) Definiera vad som menas med en grupp, en ring respektive en kropp.  
b) Ge ett exempel vardera på en grupp, en ring respektive en kropp.  
c) Ge ett exempel på en ring som inte är en kropp.
8. a) Låt  $p$  vara ett primtal. Visa att polynomet  $x^2 + 1$  är reducibelt i  $\mathbf{Z}_p[x]$ , dvs kan skrivas som en produkt på formen  $(x + a)(x + b)$  om och endast om  
 $n \cdot p - 1$  är en jämn kvadrat för något  $n$  sådant att  $0 < n \leq p$ .  
b) Visa att  $x^2 + 1$  är reducibelt i  $\mathbf{Z}_p[x]$ , för  $p = 2, 5$  och  $13$ .  
c) Visa att  $x^2 + 1$  är irreducibelt i  $\mathbf{Z}_p[x]$ , för  $p = 3, 7$  och  $11$ .