

Var god markera på tentaomslaget ifall du läser kursen inom lärarprogrammet eller ej. Uppgift fem ger fyra poäng, de andra ger tre poäng. För G krävs 12 poäng, för VG 18 poäng.

1. Vilka är de två sista siffrorna i decimalframställningen av 91^{243} ?
2. Vad är antalet positiva heltal mindre än eller lika med 500, som
 - (a) delas av både 2 och 3,
 - (b) inte delas av vare sig 2 eller 3?
3. En student får till uppgift att fylla ett tomt kärl med 12 dl vatten. Till sitt förfogande har han två spänner som rymmer 78 respektive 102 dl, obegränsad tillgång på vatten och ett stort kar att hälla i och ösa ur. Kan han överhuvudtaget lösa sin uppgift och i så fall hur?
4. Följande uppgift syftar till att förklara hur dekrypteringen går till i RSA-krypto.
Låt p och q vara två (stora) primtal och låt m vara deras produkt. Låt x och e vara positiva heltal sådana att $x < m$ och $\text{SGD}(x, m) = \text{SGD}(e, \phi(m)) = 1$. Visa att om $a \equiv x^e \pmod{m}$ och r uppfyller $er \equiv 1 \pmod{\phi(m)}$ så är $a^r \equiv x \pmod{m}$ och förklara varför vetskap om vad a^r är modulo m entydigt definierar talet x .
5. Vilka av funktionerna $f_1(n) = 1$, $f_2(n) = 2$, $f_3(n) = \sum_{d|n} d^3$ och $f_4(n) = \sum_{d|n} \mu\left(\frac{n}{d}\right)\phi(d)$ är multiplikativa? Visa dina påståenden.
6. (a) Visa att om $m > 2$ så är $\phi(m)$ jämnt.
(b) Visa att om $m > 2$ och $n > 2$ är relativt prima heltal och a är ett heltal relativt prima med produkten mn så är $a^{\frac{\phi(m)\phi(n)}{2}} \equiv 1 \pmod{mn}$. Förklara varför detta visar att mn saknar primitiva rötter.
7. Hur många inkongruenta lösningar modulo 2201 finns det till ekvationen

$$x^2 \equiv 671 \pmod{2201}?$$

8. Låt n vara ett positivt heltal och $a_r a_{r-1} \cdots a_0$ dess decimalframställning. Visa att 7 delar n om och endast om 7 delar talet man får från n genom att stryka entalsciffran a_0 från decimalframställningen av n och subtrahera $2a_0$ från detta.

(Detta är ett delbarhetstest för 7. Tex säger det att $7 \mid 5215$ omm $7 \mid 521 - 2 \cdot 5 = 511$, vilket sen i sin tur gäller omm $7 \mid 51 - 2 \cdot 1 = 49$.)

Tentan beräknas vara färdiggrättad 2003-09-29. Rättade skrivningar kan hämtas i mottagningsrummet kl. 12.20-13.00 varje vardag. Resultatet kan fås per telefon på nummer 772 3509 efter kl. 14.00 varje vardag.

Lycka till!
Fredrik och Håkan.