Tentamen i **MAN060 Elementär talteori, 5p** Göteborgs universitet
Telefonvakt: 0762–721861 Matematik
Inga hjälpmedel 2005–09–24 kl 8:30–13:30

Varje uppgift är värd tre poäng. För godkänt krävs 12 poäng, för väl godkänt 18 poäng.

Tentamen kommer vara färdigrättad den 13 oktober. Därefter kan skrivningarna hämtas ut i mottagningsrummet (rum 1202D) vardagar kl. 12:30–13:00. Resultat kan också erhållas från expeditionen på telefon 031–7723509.

Lycka till!

---

1. Bestäm den största gemensamma delaren till talen 11270, 4048 och 3864.

2. (a) Skriv 2660 som en summa av fyra kvadrater, eller visa att detta är omöjligt.
   (b) Skriv 2660 som en summa av två kvadrater, eller visa att detta är omöjligt.

3. Finn alla lösningar till kongruensen $10x^5 \equiv -4 \pmod{59}$. (Ledning: Talet 2 är en primitiv rot modulo 59.)

4. En talföljd definieras rekursivt genom

$$\begin{cases} a_0 = 0, \\ a_1 = 1, \\ a_n = 2a_{n-2} + 1 \quad \text{för } n \geq 2. \end{cases}$$

   Visa att $a_{2n} = 2^n - 1$ för alla $n \geq 0$.

5. (a) Bevisa Wilsons sats: Om p är ett primtal så är

$$(p-1)! \equiv -1 \pmod{p}.$$

   (b) Visa omvändningen: Om $n > 1$ och $(n-1)! \equiv -1 \pmod{n}$ så är n ett primtal.

6. Låt a, b och c vara heltal sådana att $abc \neq 0$. Visa att $\text{sgd}(a, b, c) = \text{sgd}(a, \text{sgd}(b, c))$.

7. (a) Visa att 3 är en primitiv rot modulo 17.
   (b) Finn alla primitiva rötter r modulo 17 som ligger i intervallet $1 \leq r \leq 16$.

8. Matematikläraren använder ett RSA-system med modulen $m = 301337$ för att kryptera lösningarna till en tenta i kursen Elementär talteori. Lösningarna till de två första uppgifterna (klartexter) är

$$M_1 = 253 \quad \text{och} \quad M_2 = 1358,$$

   och motsvarande kryptotexter är

$$C_1 = 242752 \quad \text{och} \quad C_2 = 210324.$$

   Några studenter har lyckats snappa upp kryptotexten till den tredje uppgiften $C_3 = 139727$. De upptäcker då att $139727 \equiv 242752 \cdot 210324 \pmod{301337}$. Vad är motsvarande klartext M_3?