Tentamen i **MAN060 Elementär talteori, 5p** Göteborgs universitet
Telefonvakt: 0762–721861 Matematik
Inga hjälpmedel 2006–01–09 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 januari. Därefter kan skrivningarna hämtas ut på studieexpeditionen vardagar kl 8^{30}–13^{00}, telefon 031–772 35 00.

Lycka till!

---

1. Lös kongruensen $748x \equiv 12 \pmod{1992}$.

2. Finn det minsta positiva heltal x som löser systemet

$$\begin{cases} x \equiv 1 \pmod 4 \\ 2x \equiv 3 \pmod 5 \\ 4x \equiv 5 \pmod 7). \end{cases}$$

3. (a) Lös den diofantiska ekvationen $2x^2 + 7y^2 = 30$.
   (b) Lös den diofantiska ekvationen $2x^2 - 7y^2 = 30$.

4. Avgör om kongruensen $x^2 \equiv 2006 \pmod{2741}$ har någon lösning. Talet 2741 är ett primtal.

5. (a) Definiera Eulers ϕ-funktion.
   (b) Bevisa Eulers sats: Om a och m är heltal med $m > 0$ och $\text{sgd}(a, m) = 1$, så är
   $$a^{\phi(m)} \equiv 1 \pmod m).$$

6. Låt (x, y, z) vara en *primitiv* pythagoreisk trippel med $x^2 + y^2 = z^2$. Visa att precis ett av talen x och y är jämnt, och ett är udda. (Om du använder satsen om klassifikation av pythagoreiska tripplar måste du bevisa den, men du kan också lösa uppgiften direkt.)

7. Låt m vara ett heltal större än 1, och låt a vara ett heltal med $\text{sgd}(a, m) = 1$ och $\text{ord}_m(a) = m - 1$. Visa att m är ett primtal.

8. Jultomten använder Elgamals signatursystem för att signera barnens önskelistor innan de skickas iväg till lagret på julaftonens morgon. Tyvärr råkar den tomtenisse som har till uppgift att slumpa k-värden använda samma k till två olika meddelanden. Om dessa meddelanden m_1 och m_2 och deras signaturer (r_1, s_1) och (r_2, s_2) är kända, hur kan man beräkna tomtens hemliga nyckel x? (Talet k som användes är inte känt.)

   För Elgamal-signaturer gäller

   $$\begin{aligned} r &\equiv g^k \pmod p \\ s &\equiv (m - xr)k^{-1} \pmod{p-1}, \end{aligned}$$

   där g är en primitiv rot modulo p, x är den hemliga nyckeln, m är meddelandet och k väljs slumpmässigt så att $\text{sgd}(k, p - 1) = 1$.