MATEMATIK
Göteborgs universitet

# LÖSNINGSFÖRSLAG TILL FÖRSTA OMTENTAMEN I ELEMENTÄR TALTEORI 2001

1. (a) Se boken, kapitel 1, Definition 5.
   (b) Genom insättning ser vi att
   $$x(x+2)(x+4) \equiv 0 \pmod 3,$$
   vilket implicerar att $3 \mid x$, $4 \mid x+2$ eller $3 \mid x+4$ för varje heltal $x$. Speciellt betyder detta att $3 = p$, $3 = p+2$ eller $3 = p+4$ om $p$, $p+2$ och $p+4$ är primtal. Enda möjligheten är i så fall $p = 3$.
2. Antag att $(a, m) = 1$. Då finns $x, y \in \mathbb{Z}$ sådana att $ax + my = 1$. Vidare ger $a \equiv b \pmod m$ existensen av ett heltal $z$ sådant att $a = b + zm$. Kombinerar vi dessa likheter får vi
   $$1 = ax + my = (b + zm)x + my = bx + (zx + y)m,$$
   vilket ger $(b, m) = 1$. På samma sätt visar vi att $(a, m) = 1$ om $(b, m) = 1$.
3. (a) Se boken, Sats 2.17.
   (b) Eulers sats kan användas eftersom $64 = 2^6$ är relativt primt med $915 = 3 \cdot 5 \cdot 61$. Vi räknar först ut $\phi(915)$:
   $$\phi(915) = \phi(3)\phi(5)\phi(61) = 2 \cdot 4 \cdot 60 = 480.$$
   Sedan är det bara att förenkla:
   $$64^{2001} \equiv 64^{4 \cdot 480 + 81} \equiv 64^{81} \equiv 2^{6 \cdot 81} \equiv 2^{480+6} \equiv 2^6 \equiv 64 \pmod{915}.$$
   Svar: 64.
4. (a) Eftersom $105 = 3 \cdot 5 \cdot 7$ så är $x \in \mathbb{Z}$ en lösning till $x^2 \equiv 1 \pmod{105}$ om och endast om $x$ är en lösning till
   $$\begin{cases} x^2 \equiv 1 \pmod 3, \\ x^2 \equiv 1 \pmod 5, \\ x^2 \equiv 1 \pmod 7, \end{cases} \quad \text{vilket är ekvivalent med} \quad \begin{cases} x \equiv \pm 1 \pmod 3, \\ x \equiv \pm 1 \pmod 5, \\ x \equiv \pm 1 \pmod 7. \end{cases}$$
   Vi kan nu använda kinesiska restsatsen för att hitta alla sådana $x$ modulo 105. Det minsta positiva lösningarna till
   $$\begin{cases} 5 \cdot 7 \cdot y_1 \equiv 1 \pmod 3, \\ 3 \cdot 7 \cdot y_2 \equiv 1 \pmod 5, \\ 3 \cdot 5 \cdot y_3 \equiv 1 \pmod 7 \end{cases}$$
   är $y_1 = 2$ och $y_2 = y_3 = 1$. Samtliga lösningar till $x^2 \equiv 1 \pmod{105}$ ges därför av
   $$x \equiv \pm 5 \cdot 7 \cdot 2 \pm 3 \cdot 7 \cdot 1 \pm 3 \cdot 5 \cdot 1 \equiv \pm 1, \pm 34, \pm 64, \pm 76 \pmod{105}$$
   Svar: $x \equiv \pm 1, \pm 34, \pm 64, \pm 76 \pmod{105}$.
   (b) Om $x^2 \equiv 11 \pmod{105}$ för något $x \in \mathbb{Z}$ så är även $x^2 \equiv 11 \pmod 3$. Genom prövning ser vi att $x^2 \equiv 11 \pmod 3$ saknar lösning. Alltså är $x^2 \equiv 11 \pmod{105}$ inte lösbar.
5. Vi börjar med att visa att $\phi(n)$ är jämnt då $n > 2$. Notera att $\phi(1) = \phi(2) = 1$ så villkoret $n > 2$ är nödvändigt. Låt $n = 2^a p_1^{a_1} \cdots p_n^{a_n}$, där $p_1, \ldots, p_n$ är olika udda primtal. Då är $\phi(n) = \phi(2^a)\phi(p_1^{a_1}) \cdots \phi(p_n^{a_n})$. Om $n > 2$ så är $a \geq 2$ eller $a_i \geq 1$ för något $i \in \{1, 2, \ldots, n\}$. I det första fallet har vi att $\phi(2^a) = 2^{a-1}$ är jämnt och i det andra fallet att $\phi(p_i^{a_i}) = p_i^{a_i - 1}(p_i - 1)$ är jämnt. Alltså är $\phi(n)$ jämnt då $n > 2$.

   Antag nu att $n = 2^k m$ där $k > 0$ och $m$ är udda. Då är
   $$\phi(n) = \phi(2^k m) = \phi(2^k)\phi(m) = 2^{k-1}\phi(m) \leq 2^{k-1} m = \frac{n}{2}.$$

Med andra ord är $\phi(n) \leq n/2$ om $n$ är jämnt. Kombinerar vi detta resultat med den triviala uppskattningen $\phi(n) \leq n-1$ för $n > 1$ så får vi

$$\phi(\phi(n)) \leq \frac{\phi(n)}{n} \leq \frac{n-1}{2}$$

för $n > 2$.

6. Eftersom $\left(\frac{22}{p}\right) = \left(\frac{2}{p}\right)\left(\frac{11}{p}\right)$ och $\left(\frac{8p}{11}\right) = \left(\frac{2}{11}\right)\left(\frac{p}{11}\right) = -\left(\frac{p}{11}\right)$ så är $\left(\frac{22}{p}\right) = \left(\frac{8p}{11}\right)$ om och endast om $\left(\frac{2}{p}\right)\left(\frac{11}{p}\right) = -\left(\frac{p}{11}\right)$. Från boken har vi

$$\left(\frac{2}{p}\right) = \begin{cases} 1 & \text{om } p \equiv 1,7 \pmod 8 \\ -1 & \text{om } p \equiv 3,5 \pmod 8 \end{cases}$$

och

$$\left(\frac{11}{p}\right) = \begin{cases} \left(\frac{p}{11}\right) & \text{om } p \equiv 1 \pmod 4 \\ -\left(\frac{p}{11}\right) & \text{om } p \equiv 3 \pmod 4 \end{cases} = \begin{cases} \left(\frac{p}{11}\right) & \text{om } p \equiv 1,5 \pmod 8 \\ -\left(\frac{p}{11}\right) & \text{om } p \equiv 3,7 \pmod 8 \end{cases}$$

Vi kan nu sammanställa räkningarna i en tabell:

| $p \pmod 8$ | $\left(\frac{2}{p}\right)\left(\frac{11}{p}\right)$ | $\left(\frac{22}{p}\right) = \left(\frac{8p}{11}\right)$ |
|---|---|---|
| 1 | $\left(\frac{p}{11}\right)$ | falskt |
| 3 | $\left(\frac{p}{11}\right)$ | falskt |
| 5 | $-\left(\frac{p}{11}\right)$ | sant |
| 7 | $-\left(\frac{p}{11}\right)$ | sant |

7. (a) Se boken, kapitel 5, Definition 1.
   (b) Enligt Proposition 5.3 uppfyller varje heltal $x$ mellan 1 och 112 kongruensen $x \equiv 3^k \pmod{113}$ för något heltal $k$ mellan 1 och 112. Enligt Proposition 5.4 är

$$\operatorname{ord}_{113}(3^k) = \frac{\operatorname{ord}_{113} 3}{(\operatorname{ord}_{113} 3, k)} = \frac{112}{(112, k)}.$$

   Alltså är $\operatorname{ord}_{113}(3^k) = 7$ precis då $(112, k) = 16$. De enda lösningarna mindre än 112 är $k = 16i$ där $i \in \{1,2,3,4,5,6\}$. Efter viss möda för man (modulo 113):

$$3^{16} \equiv 49, \quad 3^{2\cdot16} \equiv 28, \quad 3^{3\cdot16} \equiv 16, \quad 3^{4\cdot16} \equiv 106, \quad 3^{5\cdot16} \equiv 109, \quad 3^{6\cdot16} \equiv 30.$$

   <u>Svar</u>: 16, 28, 30, 49, 106, 109.

8. Om $x < -2$ så är även $x+1$ och $x+2$ negativa tal. Produkten är därför negativ och kan därför inte vara en heltalskvadrat.

   Antag att $y^2 = x(x+1)(x+2)$ för något $x \geq 1$. Vilka gemensamma primfaktorer kan $x$, $x+1$ och $x+2$ ha? Två på varandra följande tal kan inte ha några gemensamma primfaktorer ty $(x, x+1) \mid (x+1)-x$ d.v.s. $(x, x+1) \mid 1$. Talen $x$ och $x+2$ kan endast ha 2 som gemensam faktor, ty $(x, x+2) \mid (x+2)-x$ d.v.s. $(x, x+2) \mid 2$. Detta inträffar precis då $x$ är jämnt. Vi delar upp i två fall: $x$ udda, $x$ jämnt.

   <u>$x$ udda</u>: Eftersom $y^2 = x(x+1)(x+2)$ och $x$, $x+1$ och $x+2$ är parvis relativt prima så måste $x$, $x+1$ och $x+2$ vara kvadrater. Detta ser man genom att använda aritmetikens fundamentalsats. Om vi sätter $x = u^2$ och $x+1 = v^2$ så får vi ekvationen $v^2 = u^2 + 1$. Då denna ekvation endast har lösningarna $u = 0$, $v = \pm 1$ så måste $1 \leq x = u^2 = 0$. Detta är en motsägelse så $x$ kan inte var udda.

   <u>$x$ jämnt</u>: Sätt $x = 2^k a$, $x+1 = b$ och $x+2 = 2^\ell c$ där $a, b, c$ är udda och $k, \ell > 0$. Eftersom $a, b, c$ är relativt prima och $y^2 = 2^{k+\ell}abc$ så måste $k+\ell$ var jämnt och $a, b, c$ kvadrater. Vi har vidare att $(x, x+2) = 2$ så $k = 1$ eller $\ell = 1$. Det betyder att $k$ och $\ell$ båda är udda. Sätt $x = 2^k a = 2u^2$ och $x+2 = 2^\ell c = 2v^2$. Återigen får vi en ekvation $u^2 + 1 = v^2$ med lösningarna $u = 0$ och $v = \pm 1$. Detta ger en motsägelse, ty $1 \leq x = 2u^2 = 0$. Alltså är $x$ inte jämnt.

   Vi har visat att $x$ varken är jämnt eller udda och kan därför inte existera. Alltså är $(-2,0)$, $(-1,0)$ och $(0,0)$ de enda lösningarna till ekvationen $y^2 = x(x+1)(x+2)$.