MATEMATIK
Göteborgs universitet

# LÖSNINGSFÖRSLAG TILL FÖRSTA INLÄMNINGSUPPGIFTEN I KURSEN ELEMENTÄR TALTEORI 2001

(**1**) Att hitta alla lösningar till $140x \equiv 133 \pmod{301}$ är det samma som att hitta alla lösningar till den diofantiska ekvationen

$$140x + 301y = 133. \tag{1}$$

En sådan linjär ekvation löser man enklast med hjälp av Euklides algoritm:

$$\begin{aligned} 301 &= 2 \cdot 140 + 21 \\ 140 &= 6 \cdot 21 + 14 \\ 21 &= 1 \cdot 14 + 7 \\ 14 &= 2 \cdot 7. \end{aligned}$$

Bakåtsubstitution ger 7 som en linjärkombination av 140 och 301:

$$\begin{aligned} 7 &= 21 - 1 \cdot 14 \\ &= 21 - 1 \cdot (140 - 6 \cdot 21) = 7 \cdot 21 - 140 \\ &= 7 \cdot (301 - 2 \cdot 140) - 140 = 140(-15) + 301 \cdot 7, \end{aligned}$$

Multiplicerar vi med 19 får vi

$$140(-285) + 301 \cdot 133 = 133.$$

Samtliga lösningar till (1) ges därför av

$$\begin{cases} x = -285 + \frac{301}{7}\, n \\ y = 133 - \frac{140}{7}\, n, \end{cases}$$

där $n \in \mathbb{Z}$. Genom att välja lämpliga $n$ ser vi att 16, 59, 102, 145, 188, 231 och 274 är de minsta positiva icke-kongruenta lösningarna till $140x \equiv 133 \pmod{301}$.
*Svar.* $x = 16 + 43\, n$ för $n \in \mathbb{Z}$

(**2**) Låt $d = (a+b, a-b)$ där $a$ och $b$ är två relativt prima heltal. Då måste $d \mid 2a$ och $d \mid 2b$ ty

$$\begin{aligned} 2a &= (a+b) + (a-b), \\ 2b &= (a+b) - (a-b). \end{aligned}$$

Men $(2a, 2b) = 2(a,b) = 2$ så $d \mid 2$. Alltså $d = 1$ eller $d = 2$.

(**3**) Låt $a$ vara ett udda tal, säg $a = 2b+1$ för något $b \in \mathbb{Z}$. Vi vill visa att

$$a^{2^n} \equiv 1 \pmod{2^{n+2}}, \tag{2}$$

for alla $n \geq 1$. Ett sätt att visa detta är genom induktion över $n$.

– Påstående (2) är sant för $n = 1$, ty

$$a^2 - 1 \equiv (2b+1)^2 - 1 \equiv 4b^2 + 4b \equiv 4b(b+1) \equiv 0 \pmod{8}.$$

Notera att precis ett av talen $b$ eller $b+1$ måste vara jämnt.

– Antag att (2) är sant för $n = m$ där $m \geq 1$ är något heltal (induktionsantagandet). Konjugatregeln säger att

$$a^{2^{m+1}} - 1 = (a^{2^m})^2 - 1 = (a^{2^m} - 1)(a^{2^m} + 1).$$

Enligt induktionsantagandet gäller att $2^{m+2} \mid a^{2^m} - 1$. Vi har också att $2 \mid a^{2^m} + 1$ eftersom $a$ är udda. Sammantaget betyder det att $2^{m+3} \mid (a^{2^m} - 1)(a^{2^m} + 1)$. Alltså (2) gäller även för $n = m + 1$.

(**4**) Om $n \geq 1$ har vi en faktorisering

$$8^n + 1 = 2^{3n} + 1 = (2^n + 1)(4^n - 2^n + 1).$$

Talen $2^n + 1$ och $4^n - 2^n + 1$ är båda större än 1 när $n \geq 1$. Det betyder att $8^n + 1$ är sammansatt då $n \geq 1$.

(**5**) Heltalet $x$ uppfyller

$$\begin{cases} x \equiv 2 \pmod 6 \\ x \equiv 8 \pmod 9 \end{cases}$$

precis då $x = 2 + 6a = 8 + 9b$ för några $a$, $b \in \mathbb{Z}$. Detta ger ett villkor på $a$ och $b$, nämligen att $6a - 9b = 6$. Dividerar vi bort 3 får vi den linjära ekvationen

$$2a - 3b = 2. \tag{3}$$

Denna ekvation löses enkelt genom påseende. En lösning är $a = 1$, $b = 0$, så samtliga lösningar till (3) är på formen $a = 1 + 3n$, $b = 2n$ för $n \in \mathbb{Z}$.

*Svar.* $x = 8 + 18n$ för $n \in \mathbb{Z}$