MATEMATIK
Göteborgs universitet

LÖSNINGSFÖRSLAG TILL ANDRA INLÄMNINGSUPPGIFTEN I KURSEN ELEMENTÄR TALTEORI 2001

(**1**) (a) Funktionen $n \mapsto n^k$ är uppenbarligen multiplikativ för alla heltal k. Enligt sats 3.1 är därför

$$\sigma_k(n) = \sum_{d|n, d>0} d^k$$

en multiplikativ funktion.

(b) Antag att k är positivt och låt p vara ett primtal. Då är

$$\sigma_k(p^a) = \sum_{d|p^a, d>0} d^k = \sum_{i=0}^{a} (p^i)^k = \sum_{i=0}^{a} (p^k)^i = \frac{p^{(a+1)k} - 1}{p^k - 1},$$

för alla heltal $a > 0$. Den sista likheten följer från den välkända formeln

$$\sum_{i=0}^{n-1} x^i = \frac{x^n - 1}{x - 1}.$$

Antag nu att $n = p_1^{a_1} \cdots p_r^{a_r}$ där $p_1, \ldots, p_r$ är olika primtal och $a_1, \ldots, a_r$ är positiva tal. Eftersom σ_k är multiplikativ enligt (a) så är

$$\sigma_k(n) = \prod_{i=1}^{r} \sigma_k(p_i^{a_i}) = \prod_{i=1}^{r} \frac{p_i^{(a_i+1)k} - 1}{p_i^k - 1}.$$

(**2**) (a) Om p är ett primtal och k är ett positivt heltal så är $1, p, \ldots, p^{k-1}$ de enda positiva delarna i p^{k-1}. Antalet sådana delare är som synes $\nu(p^{k-1}) = k$. Antag nu att k är ett heltal större än 1. Då är $p^{k-1} \neq q^{k-1}$ om p och q är olika primtal. Det finns därför åtminstone lika många lösningar till ekvationen $\nu(n) = k$ som det primtal. Som vi vet så finns det oändligt många primtal.

(b) Låt n vara ett positivt heltal. Enligt definitionen är $\sigma(n)$ summan av de positiva delarna i n och eftersom n är en positiv delare i n så är $n \leq \sigma(n)$. En lösning till ekvationen $\sigma(n) = k$ där k är ett fixt positivt heltal måste därför uppfylla $n \leq k$. Ekvationen $\sigma(n) = k$ har således ingen eller ett ändligt antal lösningar (antalet lösningar är $\leq k$).

(**3**) Låt x vara ett heltal. Enligt definitionen av minsta gemensamma multipeln $[a, b]$ av två heltal a och b så gäller att $[a, b] \mid x$ om och endast om $a \mid x$ och $b \mid x$. I vårt fall betyder det att $n^{12} \equiv 1 \pmod{72}$ för något $n \in \mathbb{Z}$ om och endast om

$$\begin{cases} n^{12} \equiv 1 \pmod{8} \\ n^{12} \equiv 1 \pmod{9} \end{cases} \tag{i}$$

Det räcker därför att visa att (i) är uppfyllt för alla heltal n som är relativt prima med 72. Enligt Eulers sats är

$$n^{12} \equiv (n^4)^3 \equiv (n^{\phi(8)})^3 \equiv 1^3 \equiv 1 \pmod{8}$$

för alla $n \in \mathbb{Z}$ som är relativt prima med 8, och

$$n^{12} \equiv (n^6)^2 \equiv (n^{\phi(9)})^2 \equiv 1^2 \equiv 1 \pmod{9},$$

för alla $n \in \mathbb{Z}$ som är relativt prima med 9. Ett tal n som är relativt primt med 72 är naturligtvis relativt primt med både 8 och 9 och uppfyller därför (i).

(**4**) (a) Kongruensen $x^2 + 2 \equiv 0 \pmod{p}$ är lösbar om och endast om kongruensen $x^2 \equiv -2 \pmod{p}$ lösbar, vilket inträffar precis då -2 är en kvadratisk rest modulo p. Vi skall följaktligen visa att $\left(\frac{-2}{p}\right) = 1$ om och endast om $p \equiv 1, 3 \pmod{8}$. Observera att $\left(\frac{-2}{p}\right) = \left(\frac{-1}{p}\right)\left(\frac{2}{p}\right) = 1$ precis då $\left(\frac{-1}{p}\right) = \left(\frac{2}{p}\right)$. Genom att kombinera sats 4.6 och 4.8 följer det således att $\left(\frac{-2}{p}\right) = 1$ om och endast om

$$p \equiv 1 \pmod{4} \quad \text{och} \quad p \equiv 1, 7 \pmod{8},$$

eller

$$p \equiv 3 \pmod{4} \quad \text{och} \quad p \equiv 3, 5 \pmod{8}.$$

Eftersom $p \equiv 1 \pmod{4}$ precis då $p \equiv 1, 5 \pmod{8}$ och $p \equiv 3 \pmod{4}$ precis då $p \equiv 3, 7 \pmod{8}$, så har vi $\left(\frac{-2}{p}\right) = 1$ precis då $p \equiv 1, 3 \pmod{8}$, vilket fullbordar lösningen.

(b) Kongruensen $x^2 \equiv 3 \pmod{p}$ är lösbar om och endast om $\left(\frac{3}{p}\right) = 1$. Enligt kvadratiska reciprocitetssatsen gäller

$$\left(\frac{3}{p}\right)\left(\frac{p}{3}\right) = \begin{cases} 1 & \text{om } p \equiv 1 \pmod{4}, \\ -1 & \text{om } p \equiv 3 \pmod{4}. \end{cases} \tag{ii}$$

Eftersom 1 är den enda kvadratiska resten modulo 3 så har vi

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

Tillsammans ger (ii) och (iii) att $\left(\frac{3}{p}\right) = 1$ precis då

$$p \equiv 1 \pmod{4} \quad \text{och} \quad p \equiv 1 \pmod{3},$$

eller

$$p \equiv 3 \pmod{4} \quad \text{och} \quad p \equiv 2 \pmod{3}.$$

Eftersom $3 \equiv -1 \pmod{4}$, $2 \equiv -1 \pmod{3}$ och $(3, 4) = 1$ så följer det att $\left(\frac{3}{p}\right) = 1$ precis då $p \equiv \pm 1 \pmod{12}$, vilket fullbordar lösningen.

(**5**) Det finns inga lösningar till

$$2x^2 + x \equiv 5 \pmod{6}. \tag{iv}$$

Detta kan konstateras genom insättning av $x \in \{0, 1, 2, 3, 4, 5\}$. En alternativ lösning fås genom att, via definitionen av minsta gemensamma multipel, sluta sig till att kongruensen (iv) är lösbar om och endast om systemet

$$\begin{cases} 2x^2 + x \equiv 5 \pmod{3} \\ 2x^2 + x \equiv 5 \pmod{2} \end{cases}$$

är lösbart. Multiplicerar vi den första ekvationen med 2 så fås efter kvadratkomplettering att en lösning x till (iv) måste uppfylla

$$(x + 1)^2 \equiv 2 \pmod{3}.$$

Ett sådant x existerar inte, ty 1 är den enda kvadratiska resten modulo 3.