Tentamenskrivning i Algebraisk talteori 01-01-27

Lösningar

F.1 SVAR : Oändligt många.

BEVIS : Enligt CRT finns det $a \in \mathbf{N}$ som löser alla 4 kongruenser. Sätt $q = 3 \cdot 5 \cdot 7 \cdot 11$. Då löser varje term i den aritmetiska följden $\{a + nq : n \in \mathbf{N}\}$ alla 4 kongruenser. Eftersom $(a, q) = 1$, innehåller denna följd oändligt många primtal, enligt Dirichlets sats.

F.2 (i) Sats 31, s.45 i mina anteckningar.

(ii) Från Sats 16, s.33 i mina anteckningar får vi att

$$\prod_p \left(1 - \frac{1}{p^2}\right) = \frac{1}{\zeta(2)} = \frac{6}{\pi^2},$$

där värdet av $\zeta(2)$ är ett välkänt faktum.

F.3 (i) f är reducerad om antingen $-|a| < b \leq |a| \leq |c|$ eller $0 \leq b \leq |a| = |c|$.

(ii) Enligt Prop. 48(i), s.68 finns det en form av diskriminant 265 som representerar p omm $\left(\frac{265}{p}\right) = 1$. Man kontrollerar, m.h.a. Sats, s.38, att $\left(\frac{265}{31}\right) = -1$ medan att $\left(\frac{265}{23}\right) = 1$. Nu beräknar man direkt att

$$9^2 = 265 - 2 \cdot (4 \cdot 23)\,,$$

som antyder (se Sats 47, s.63 och dess bevis) att formen $23x^2 + 9xy - 2y^2$ har diskriminant 265 och representerar 23 vid $(x\ y) = (1\ 0)$. Det kvarstår att reducera formen. Dess matris är

$$A = \begin{pmatrix} 23 & 9/2 \\ 9/2 & -2 \end{pmatrix}.$$

Om man tar

$$M_1 = \begin{pmatrix} 0 & -1 \\ 1 & 0 \end{pmatrix}, \quad M_2 = \begin{pmatrix} 1 & -2 \\ 0 & 1 \end{pmatrix},$$

då kontrollerar man att

$$(M_1 M_2)^T A (M_1 M_2) = \begin{pmatrix} -2 & -1/2 \\ -1/2 & 33 \end{pmatrix},$$

som är matrisen av den reducerad formen $-2x^2 - xy + 33y^2$. Denna form representerar 23 i

$$\begin{pmatrix} x \\ y \end{pmatrix} = (M_1 M_2)^{-1} \begin{pmatrix} 1 \\ 0 \end{pmatrix} = \begin{pmatrix} -2 \\ -1 \end{pmatrix}.$$

F.4 s.33 i mina anteckningar.

F.5 **(i)** Låt $L = \mathbf{Q}(\sqrt[3]{2})$ och $M = \mathbf{Q}(\sqrt[4]{3})$. Notera att $[L : \mathbf{Q}] = 3$ och $[M : \mathbf{Q}] = 4$. Eftersom $K = LM$ så har vi (se ekv. (155), s.84) å ena sidan att

$$[K : \mathbf{Q}] = [LM : \mathbf{Q}] = [LM : L][L : \mathbf{Q}] = 3[LM : L], \tag{1}$$

och å andra sidan att

$$[K : \mathbf{Q}] = [LM : \mathbf{Q}] = [LM : M][M : \mathbf{Q}] = 4[LM : M]. \tag{2}$$

Från (1) och (2) ser vi att $[K : \mathbf{Q}]$ är delbar med både 3 och 4, och det följer att $[K : \mathbf{Q}] = 12$.

(ii) Enligt beviset av Sats 67, s.88, om $a \in \mathbf{Q}$ inte uppfyller villkoret, då måste det finnas $\zeta, \eta \in \mathbf{C}$ så att $\eta \neq 1$, $\zeta^3 = 1$, $\eta^4 = 1$ och

$$\zeta \sqrt[3]{2} + a\eta \sqrt[4]{3} = \sqrt[3]{2} + a\sqrt[4]{3} \quad \Rightarrow \quad a = \frac{\sqrt[3]{2}}{\sqrt[4]{3}} \left(\frac{1-\zeta}{\eta - 1} \right).$$

Det finns bara ändligt många sådana a och, t.ex.,

$$|a| = \frac{\sqrt[3]{2}}{\sqrt[4]{3}} \frac{|1-\zeta|}{|\eta - 1|} \leq \frac{2}{1} \cdot \frac{2}{\sqrt{2}} < 3,$$

eftersom $|1-\zeta| \leq 1+|\zeta| = 2$ och $\eta = i, -i$ eller -1 så att $|\eta - 1| \geq \sqrt{2}$.
Alltså, tag $a = 3$ säg.

F.6 Sats 65(ii) och Prop. 66, s.86 i mina anteckningar. Alltså räcker det t.ex. att bevisa Props. 63,64,66.

F.7 Låt $K = \mathbf{Q}(\sqrt{-13})$.

Steg 1 : Notera att $-13 \equiv 3 \pmod 4$ så att $\mathbf{Z}[\sqrt{-13}] = O_K$ och

$$d_K = 4(-13) = -52.$$

Steg 2 : Notera näst att

$$n(5+2\sqrt{-13}) = (5+2\sqrt{-13})(5-2\sqrt{-13}) = 77 = 7 \cdot 11.$$

I följande två steg, använder vi Sats 101, s.125 och dess bevis.

Steg 3 : $7 \dagger d_K$ och $\left(\frac{-13}{7}\right) = \left(\frac{1}{7}\right) = 1$, och $1^2 \equiv -13 \pmod 7$, så att 7 splittrar i K och

$$< 7 > = \mathbf{p}_1 \mathbf{p}_2,$$

där

$$\mathbf{p}_1 = < 7, 1+\sqrt{-13} >$$

och

$$\mathbf{p}_2 = \mathbf{p}_1' = < 7, 1-\sqrt{-13} > .$$

Steg 4 : $11 \dagger d_K$ och $\left(\frac{-13}{11}\right) = \left(\frac{9}{11}\right) = 1$, och $3^2 \equiv -13 \pmod{11}$, så att 11 också splittrar i K och

$$< 11 > = \mathbf{q}_1 \mathbf{q}_2,$$

där
$$\mathbf{q}_1 = < 11, 3 + \sqrt{-13} >$$
och
$$\mathbf{q}_2 = \mathbf{q}_1' = < 11, 3 - \sqrt{-13} > .$$

Steg 5 : Nu har vi att
$$< 5 + 2\sqrt{-13} >< 5 - 2\sqrt{-13} > = \mathbf{p}_1\mathbf{p}_2\mathbf{q}_1\mathbf{q}_2,$$
så att
$$< 5 + 2\sqrt{-13} > = \mathbf{p}_1\mathbf{q}_1 \text{ eller } \mathbf{p}_1\mathbf{q}_2 \text{ eller } \mathbf{p}_2\mathbf{q}_1 \text{ eller } \mathbf{p}_2\mathbf{q}_2.$$
Mer explicit, måste vi nu betrakta ekvationerna
$$7(a + b\sqrt{-13}) + (1 \pm \sqrt{-13})(c + d\sqrt{-13}) = 5 + 2\sqrt{-13}, \tag{3}$$
$$11(a + b\sqrt{-13}) + (3 \pm \sqrt{-13})(c + d\sqrt{-13}) = 5 + 2\sqrt{-13}, \tag{4}$$
där $a, b, c, d \in \mathbf{Z}$, och både (3) och (4) har en lösning för antingen $+$ eller $-$ tecken, men inte båda. En direkt beräkning visar att både (3) och (4) har lösningar för $-$ tecken, som antyder äntligen att
$$< 5 + 2\sqrt{-13} > = \mathbf{p}_2\mathbf{q}_2.$$

F.8 (i) Oändligt många. Notera att $x = 2, y = 1$ är en lösning, och att alla lösningarna ges av
$$x + y\sqrt{2001} = (2 + \sqrt{2001})(z + w\sqrt{2001}),$$
där $(z, w) \in \mathbf{Z}^2$ satisfierar
$$z^2 - 2001w^2 = 1. \tag{5}$$
Enligt Sats 103, s.129 har (5) oändligt många lösningar.

(ii) Samma idé, men använd Sats 104 (och dess bevis) i stället för Sats 103. Man ser lätt att $1 + \sqrt{2}$ är en fundamental enhet i $\mathbf{Q}(\sqrt{2})$. Den har norm -1 och dess kvadrat, $3 + 2\sqrt{2}$, är en fundamental enhet av norm $+1$. Då antyder Sats 104 att alla lösningarna ges av
$$\begin{aligned} x + y\sqrt{2} &= \pm(1 + \sqrt{2})(3 + 2\sqrt{2})^m, \quad \text{där } m \in \mathbf{Z}, \\ &= \pm(1 + \sqrt{2})^{2m+1}, \quad \text{där } m \in \mathbf{Z}. \end{aligned}$$