Tentamenskrivning i Algebraisk talteori 01-08-22

Lösningar

F.1 Resultatet är klart när $a < b$ så vi får antaga att $a \geq b$. Skriv

$$a = qb + r,$$

där $q \geq 1$ och $0 \leq r < b$. Notera då att

$$2^a + 1 = (2^{a-b} + 2^{a-2b} + \cdots + 2^{a-qb})(2^b - 1) + 2^r + 1$$

så att $2^b - 1 | 2^a + 1 \Leftrightarrow 2^b - 1 | 2^r + 1$. Men detta är omöjligt eftersom $b > 2$ och $r < b$, som medför att $2^r + 1 < 2^b - 1$.

F.2 (i) Om χ är icke-trivial, då är serien som definierar $L(s, \chi)$ redan holomorfisk i $\mathrm{Re}(s) > 0$ - se Sats 19(ii), s.28 i mina anteckningar. Om χ är den triviala karaktären modulo N, då gäller att, för $\mathrm{Re}(s) > 1$,

$$L(s, \chi) = \zeta(s) \cdot \prod_{p|N} \left(1 - \frac{1}{p^s}\right).$$

Den ändliga produkten över primtalen är redan holomorfisk i $\mathrm{Re}(s) > 0$. Zeta-funktionen har en meromorfisk fortsättning till $\mathrm{Re}(s) > 0$, med en enkel pol i $s = 1$ - se Sats 31, s.45 i mina anteckningar. Alltså, gäller detsamma för L-funktionen.

F.3 Den givna formen, som ska betecknas $f_1(x, y)$, är reducerad av diskriminant -15. Med hjälp av reduktionsteorin (Baker, s.36) beräknar man att det finns en reducerad form till av diskriminant -15, nämligen $f_2(x, y) = 2x^2 + xy + 2y^2$. Prop. 48 antyder att primtalet p representeras av en form av diskriminant -15 omm $\left(\frac{-15}{p}\right) = 1$. Nu har vi att

$$\left(\frac{-15}{p}\right) = \left(\frac{-1}{p}\right)\left(\frac{3}{p}\right)\left(\frac{5}{p}\right) = (-1)^{\frac{1}{2}(p-1)}\left[\left(\frac{p}{3}\right)(-1)^{\frac{1}{2}(p-1)}\right]\left(\frac{p}{5}\right) = \left(\frac{p}{3}\right)\left(\frac{p}{5}\right).$$

Och $\left(\frac{p}{3}\right)\left(\frac{p}{5}\right) = 1$ omm antingen

(i) $\left(\frac{p}{3}\right) = \left(\frac{p}{5}\right) = 1 \Leftrightarrow p \equiv 1 \bmod 3$ och $p \equiv \pm 1 \bmod 5 \Leftrightarrow p \equiv 1, 4 \bmod 15$,

eller

(ii) $\left(\frac{p}{3}\right) = \left(\frac{p}{5}\right) = -1 \Leftrightarrow p \equiv 2 \bmod 3$ och $p \equiv \pm 2 \bmod 5 \Leftrightarrow p \equiv 2, 8 \bmod 15$.

Till slut, notera att formen f_1 kan inte representera tal $\equiv 2 \bmod 3$ medan att f_2 kan inte representera tal $\equiv 1 \bmod 3$.

Alltså, representerar f_1 alla udda primtal $p \equiv 1$ eller $4 \bmod 15$, dvs $p \equiv 1$ eller $19 \bmod 30$.

F.4 Detta är Jacobis reciprocitetslag, en generalisering av Gauβ lag. Se Baker s.29-32 för beviset.

F.5 Se s.114 i mina anteckningar för definitionen av ramifikation. Låt den kubiska roten av 2 i K betecknas med x. Man ser direkt att primtalet 2 är totalt ramifierad i K eftersom

$$< 2 >= < x >^3 .$$

Detsamma gäller för primtalet 3, men det är kanske lite svårare att se. Vi har att

$$3 = x^3 + 1 = (x+1)(x^2 - x + 1) = (x+1)[(x+1)(x^2-1)] = (x+1)^3(x-1).$$

Notera att $x - 1$ är en enhet i O_K eftersom

$$1 = x^3 - 1 = (x-1)(x^2 + x + 1).$$

Därför har vi ideal faktoriseringen

$$< 3 >= < x + 1 >^3 .$$

Att inga fler primtal ramifierar kan bevisas med hjälp av Prop. 96. Enligt ekv. (173) på s.93, räcker det att ange bara EN integral bas till K vars diskriminant är delbar med bara 2 och 3. Det är helt naturligt att prova med basen $\{1, x, x^2\}$. Låt

$$\zeta = \frac{1 + \sqrt{-3}}{2}$$

vara en primitiv tredje enhetsrot, som då satisfierar ekvationen

$$\zeta^2 + \zeta + 1 = 0.$$

Nu har vi att

$$\begin{aligned} \Delta(1, x, x^2) &= \begin{vmatrix} 1 & x & x^2 \\ 1 & \zeta x & \zeta^2 x^2 \\ 1 & \zeta^2 x & \zeta x^2 \end{vmatrix}^2 \\ &= -2^2 3^3, \end{aligned}$$

efer en lätt beräkning.

F.6 Prop. 78, s.99 i mina anteckningar.

F.7 Låt $K = \mathbf{Q}(\sqrt{-11})$.

Steg 1 : Notera att $-11 \equiv 1 \pmod 4$ så att $\mathbf{Z}\left[1, \frac{1+\sqrt{-11}}{2}\right] = O_K$ och

$$d_K = -11.$$

Steg 2 : Notera näst att

$$n(4 + 3\sqrt{-11}) = (4 + 3\sqrt{-11})(4 - 3\sqrt{-11}) = 115 = 5 \cdot 23.$$

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

Steg 3 : $5 \dagger d_K$ och $\left(\frac{-11}{5}\right) = \left(\frac{-1}{5}\right) = 1$, och $2^2 \equiv -11 \pmod 5$, så att 5 splittrar i K och

$$< 5 > = \mathbf{p}_1 \mathbf{p}_2,$$

där

$$\mathbf{p}_1 = < 5, 2 + \sqrt{-11} >$$

och

$$\mathbf{p}_2 = \mathbf{p}_1' = < 5, 2 - \sqrt{-11} > .$$

Steg 4 : $23 \dagger d_K$ och $\left(\frac{-11}{23}\right) = \left(\frac{-1}{23}\right)\left(\frac{11}{23}\right) = -\left(\frac{11}{23}\right) = +\left(\frac{23}{11}\right) = +\left(\frac{1}{11}\right) = 1$, och $9^2 \equiv -11 \pmod{23}$, så att 23 också splittrar i K och

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

där

$$\mathbf{q}_1 = < 23, 9 + \sqrt{-11} >$$

och

$$\mathbf{q}_2 = \mathbf{q}_1' = < 23, 9 - \sqrt{-11} > .$$

Steg 5 : Nu har vi att

$$< 4 + 3\sqrt{-11} >< 4 - 3\sqrt{-11} > = \mathbf{p}_1\mathbf{p}_2\mathbf{q}_1\mathbf{q}_2,$$

så att

$$< 4 + 3\sqrt{-11} > = \mathbf{p}_1\mathbf{q}_1 \ \text{ eller } \ \mathbf{p}_1\mathbf{q}_2 \ \text{ eller } \ \mathbf{p}_2\mathbf{q}_1 \ \text{ eller } \ \mathbf{p}_2\mathbf{q}_2.$$

Mer explicit, måste vi nu betrakta ekvationerna

$$5\left(a + b\frac{1+\sqrt{-11}}{2}\right) + (2 \pm \sqrt{-11})\left(c + d\frac{1+\sqrt{-11}}{2}\right) = 4 + 3\sqrt{-11}, \quad (1)$$

$$23\left(a + b\frac{1+\sqrt{-11}}{2}\right) + (9 \pm \sqrt{-11})\left(c + d\frac{1+\sqrt{-11}}{2}\right) = 5 + 2\sqrt{-13}, \quad (2)$$

där $a, b, c, d \in \mathbf{Z}$, och både (1) och (2) har en lösning för antingen + eller − tecken, men inte båda. En direkt beräkning visar att (1) och (2) har lösningar för − och + tecken respektivt (man får osatisfierbara kongruensvillkor i de andra fallen), som antyder äntligen att

$$< 4 + 3\sqrt{-11} > = \mathbf{p}_2\mathbf{q}_1.$$

F.8 (i) Det finns oändligt många lösningar. $x = 10$, $y = 3$ är en fundamental lösning, och alla lösningarna ges av

$$x + y\sqrt{11} = \pm(10 + 3\sqrt{11})^m, \quad m \in \mathbf{Z}$$

enligt Sats 104, s.131 i mina anteckningar (mer precis, enligt BEVISET av denna sats).

(ii) Den enda saken som kunde stoppa $10 + 3\sqrt{11}$ från att vara en fundamental enhet är om det fanns en lösning till $x^2 - 11y^2 = -1$. Men detta skulle betyda att kongruensen $x^2 \equiv -1 \bmod 11$ hade en lösning, som inte finns eftersom $11 \equiv 3 \bmod 4$.