Algebraic Number Theory
MATH 512

Solutions to Assignment 4

1. We observe that the cubes mod 9 are -1, 0 and 1. Therefore if $3 \nmid x, y$, then $z^3 = x^3 + y^3 \equiv -2, 0, 2 \bmod 9$, so we must have $z \equiv 0 \bmod 9$, i.e. $3|z$.

2. (a) A prime that divides any two of x, y, z must necessarily divide the third, and therefore may be factored out. Thus we may assume that x, y, z are pairwise coprime. In particular, 3 can divide no more than one of x, y, z. Therefore, by exercise **1.**, 3 must divide *exactly* one of x, y, z. By relabelling x, y, z if necessary, and introducing signs as appropriate, we may assume that $3|z$. Write $z = 3^m \tilde{z}$ with $\tilde{z}$ a non-zero integer not divisible by 3. Then $x^3 + y^3 = 3^m \tilde{z}^3$, and we are done.

(b) 3 divides $\alpha\beta\gamma$ in $\mathbb{Z}[\zeta]$, so π also divides $\alpha\beta\gamma$ since $(1-\zeta)(1-\zeta^2) = 3$. Since π is prime, it divides at least one of α, β, γ. However, π is associate to $1 - \zeta^2$, and so

$$x + y \equiv x + y\zeta \equiv x + y\zeta^2 \bmod \pi.$$

Thus π divides all three of α, β, γ.

(c) If π divides β', then $\pi^2|\beta$, but $\pi^2 = -3\zeta$ and so 3 divides β in that case. But then 3 divides both x and y, a contradiction. Similarly, π does not divide γ' in $\mathbb{Z}[\zeta]$.

$$\begin{aligned} 3^{3m} z^3 &= \alpha\beta\gamma \\ &= (1-\zeta)(1-\zeta^2)\alpha\beta'\gamma' \\ &= 3\alpha\beta'\gamma', \end{aligned}$$

so $3^{3m-1}z^3 = \alpha\beta'\gamma'$. By the above, 3^{3m-1} is coprime to each of β', γ', and so 3^{3m-1} divides α in $\mathbb{Z}[\zeta]$, i.e. there is $\alpha' \in \mathbb{Z}[\zeta]$ such that $\alpha = 3^{3m-1}\alpha'$.

Now, any prime dividing at least two of α', β', γ' must divide at least two of α, β, γ. The proof of Lemma 46 shows in that case that the prime in question must be associate to π, and so π divides β' or γ'. However, we have just seen that this cannot happen. Thus α', β', γ' are pairwise coprime.

(d) The units in $\mathbb{Z}[\zeta]$ are $\pm\zeta^k$, $k = 0, 1, 2$. By replacing δ_i by $-\delta_i$ if necessary, we may assume that u_i is a power of ζ. Write $u_i = \zeta^{k_i}$ with $k_i \in \{0, 1, 2\}$.

We first deal with k_1. Let σ be the non-trivial element of $\mathrm{Gal}(\mathbb{Q}(\zeta)/\mathbb{Q})$, i.e. $\sigma(\zeta) = \zeta^{-1}$. Then

$$\begin{aligned} \zeta^{2k_1} &= u_1/\sigma(u_1) \\ &= \frac{\alpha'\sigma(\delta_1)^3}{\alpha'\delta_1^3} \\ &= \left(\frac{\sigma(\delta_1)}{\delta_1}\right)^3. \end{aligned}$$

Therefore ζ^{2k_1} is both a square and a cube in the cyclic group $\langle -\zeta \rangle$ of order 6, and is therefore trivial. Thus ζ^{k_1} is trivial also, so $k_1 = 0$.

Now to deal with k_2. Write $\delta_2 = d_1 + d_2\zeta$ with $d_1, d_2 \in \mathbb{Z}$. Since $\beta' = \zeta^{k_2}\delta_2^3$, we have

$$\beta' = \begin{cases} 3d_1d_2^2 - 3d_1^2d_2 + (d_1^3 + d_2^3 - 3d_1^2d_2)\zeta & \text{if } k_2 = 1 \\ 3d_1^2d_2 - d_1^3 - d_2^3 + (3d_1d_2^2 - d_1^3 - d_2^3)\zeta & \text{if } k_2 = 2. \end{cases} \tag{1}$$

However, $\beta' = \beta/\pi = \frac{1}{3}(2x - y) + \frac{1}{3}(x + y)\zeta$. Also, $9|\alpha = x + y$, i.e. $y \equiv -x \bmod 9$, so $3|\frac{1}{3}(x + y)$ and $2x - y \equiv 3x \bmod 9$. This last congruence says $\frac{1}{3}(2x - y) \equiv x \not\equiv 0 \bmod 3$. In summary,

$$\begin{aligned} \frac{1}{3}(2x - y) &\not\equiv 0 \bmod 3 \\ \frac{1}{3}(x + y) &\equiv 0 \bmod 3. \end{aligned}$$

This contradicts the descriptions of β', in the cases $k_2 = 1, 2$, given in (1). Hence $k_2 = 0$. That $\gamma' = \delta_3^3$ for some $\delta_3 \in \mathbb{Z}[\zeta]$ now follows just by applying σ to the equation $\beta' = \delta_2^3$.

(e) Write $\delta_1 = s + t\zeta$ with $s, t \in \mathbb{Z}$. Then

$$\begin{aligned} \alpha' &= (s + t\zeta)^3 \\ &= s^3 + t^3 - 3st^2 + 3st(s - t)\zeta, \end{aligned}$$

so one of $s, t, s - t$ is zero. Since $\zeta^3 = 1$ and $(1 + \zeta)^3 = -1$, we may assume $\delta_1 \in \mathbb{Z}$.

(f) Any rational prime dividing both a and b would divide both $\tilde{\beta}$ and $\tilde{\gamma}$, which is impossible.

(g)

$$\begin{aligned} x + y\zeta &= \beta'\pi \\ &= (a + b\zeta)^3(1 - \zeta) \\ &= (a^3 + b^3 + 3a^2b - 6ab^2) + (6a^2b - 3ab^2 - a^3 - b^3)\zeta, \end{aligned}$$

so

$$\begin{aligned} x + y &= 9a^2b - 9ab^2 \\ &= 9ab(a - b). \end{aligned}$$

Then

$$\begin{aligned} 9ab(a - b) &= x + y \\ &= \alpha \\ &= 3^{3m-1}\alpha' \\ &= 3^{3m-1}\delta_1^3, \end{aligned}$$

i.e. $ab(a-b) = 3^{3m-3}\delta_1^3$.

(h) Since 3^{3m-3} divides $ab(a-b)$ and $a, b, a-b$ are pairwise coprime, 3^{3m-3} divides exactly one of them. Dividing that integer by 3^{3m-3}, the product is then equal to δ_1^3, and so each of the integers is a cube in $\mathbb{Z}$, say r^3, s^3, t^3.

(i) If, for example, $a = r^3$, $b = s^3$ and $a - b = 3^{3m-3}t^3$, then

$$r^3 + (-s)^3 = 3^{3m-3}t^3,$$

so we take $r_1 = r$, $s_1 = -s$ and $t_1 = t$. All the other possibilities involve simply reordering terms and changing signs as necessary.

(j) It remains to show that 3 divides none of r_1, s_1, t_1. For this, suppose that $3|\alpha'$ in $\mathbb{Z}$, say $\alpha' = 3\alpha''$ with $\alpha'' \in \mathbb{Z}$. Then

$$\begin{aligned} 3^{3m}z^3 &= 3\alpha\beta'\gamma' \\ &= 3^{3m}\alpha'\beta'\gamma' \\ &= 3^{3m+1}\alpha''\beta'\gamma', \end{aligned}$$

so $z^3 = 3\alpha''\beta'\gamma'$, implying that $3|z$, a contradiction. Therefore $3 \nmid \alpha'$ and so $3 \nmid \delta_1$. This means that 3 divides none of r, s, t, and so also 3 divides none of r_1, s_1, t_1 as required. By induction on $m \geq 0$, we are done (the case $m = 0$ being exercise **1.**, the first case of Fermat with $p = 3$).

3. Suppose $\alpha \in \mathcal{O}_K$, so that $f(\alpha) = 0$ for some $f(x) = x^n + a_{n-1}x^{n-1} + \cdots + a_1x + a_0 \in \mathbb{Z}[x]$ with $n \geq 1$. If $|\alpha| > 1$, then for $0 \leq k < n$ we have

$$\begin{aligned} |\alpha^n| &= |\alpha|^n \\ &> |\alpha|^k \\ &= |\alpha^k| \\ &\geq |a_k||\alpha^k| \\ &= |a_k\alpha^k|. \end{aligned}$$

This means that the first term in $f(\alpha)$ has absolute value strictly greater than that of every other term, and so $|f(\alpha)| = |\alpha^n| > 1$. However, $f(\alpha) = 0$, so that we have a contradiction. Thus $|\alpha| \leq 1$, as required.