HW #13

ALGEBRAIC NUMBER THEORY, GU4043; INSTRUCTOR: GYUJIN OH

Due Tuesday, April 23 by 11:59pm on Gradescope.

Question 1. In the notes, we provided the "analytic" proof of the cubic reciprocity law between two primary primes lying over the rational primes $\equiv 1 \pmod 3$. In this exercise, we supplement this with the proof of the remaining cases of the cubic reciprocity law.

Recall that a primary prime in $\mathbb{Z}[\zeta_3]$ is either $\pi \in \mathbb{Z}[\omega]$ with $N(\pi)$ a rational prime $\equiv 1 \pmod 3$ or a rational prime $p \equiv 2 \pmod 3$. For primary primes $\pi_1, \pi_2 \in \mathbb{Z}[\zeta_3]$, $\left(\frac{\pi_1}{\pi_2}\right) \in \{1, \zeta_3, \zeta_3^2\}$ is such that

$$\left(\frac{\pi_1}{\pi_2}\right) \equiv \pi_1^{\frac{N(\pi_2)-1}{3}} \pmod{\pi_2}.$$

(1) If $\pi_1 = q$ is a rational prime $\equiv 2 \pmod 3$, show that any integer coprime to q is a cube mod q. Deduce the cubic reciprocity law in the case when both π_1, π_2 are rational primes $\equiv 2 \pmod 3$.

(2) Suppose that $\pi_1 = q$ is a rational prime $\equiv 2 \pmod 3$ and $\pi_2 = \pi$ is such that $N(\pi) = p$ is a rational prime $\equiv 1 \pmod 3$. Let $\chi(n) := \left(\frac{n}{\pi}\right)$ be a Dirichlet character mod p. From $G(\chi)^3 = p\pi$, show that

$$G(\chi)^{q^2} \equiv \left(\frac{\pi}{q}\right) G(\chi) \pmod q.$$

(3) Show that

$$G(\chi)^{q^2} \equiv \sum_{a=1}^{p-1} \chi(a) e^{\frac{2\pi i a q^2}{p}} \pmod q.$$

(4) Deduce that

$$\chi(q) = \left(\frac{q}{\pi}\right) = \left(\frac{\pi}{q}\right).$$

Question 2. Let n be an even positive integer.

(1) Show that, for any $m \geq 1$.

$$B_n = m^{n-1} \sum_{a=1}^{m} B_n(a/m).$$

(2) Show that the denominator of B_n is a square-free integer.

Hint. You need to show that $v_p(pB_n) \geq 0$ for any prime number p. Use (1) with $m = p$ to get

$$pB_n = \sum_{a=1}^{p} \sum_{i=0}^{n} \binom{n}{i} p^i B_i a^{n-i}.$$

Now, use induction on n.

(3) Show that, for any prime p,

$$pB_n \equiv \begin{cases} -1 & \text{if } (p-1)|n \\ 0 & \text{otherwise} \end{cases} \pmod p.$$

This implies that $B_n + \sum_{p \text{ primes such that } (p-1)|n} \frac{1}{p}$ is an integer.[1]

Hint. From the identity used in the Hint of (2), one has

$$pB_n \equiv \sum_{a=1}^{p} \left(a^n + npB_1 a^{n-1}\right) \pmod p.$$

Then, show that $v_p(npB_1) \geq 1$.

Question 3. Using the analytic class number formula, compute the class number $h_{\mathbb{Q}(\sqrt{-21})}$ of $\mathbb{Q}(\sqrt{-21})$.

Question 4. Let $K = \mathbb{Q}(\sqrt{d}) \subset \mathbb{R}$ be a real quadratic field, where d is a square-free integer > 1 satisfying $d \equiv 2, 3 \pmod 4$.

(1) Show that

$$\epsilon_K > \sqrt{d},$$

where ϵ_K is the fundamental unit.

(2) Using the analytic class number formula, show that

$$h_K < -\frac{1}{\log \sqrt{d}} d \log\left(\sin\left(\frac{\pi}{4d}\right)\right).$$

(3) Show that, for $0 < x < 1$, $\sin\left(\frac{\pi}{2}x\right) > x$. Deduce that $h_K < 4d$.

[1] This result is often called the **von Staudt–Clausen theorem**. This in particular implies that 6 always divides the denominator of B_n.