# HW #14

ALGEBRAIC NUMBER THEORY, GU4043; INSTRUCTOR: GYUJIN OH

Due Tuesday, April 30 by 11:59pm on Gradescope.

**Question 1.**

(1) Show that the Bernoulli polynomials $B_n(X)$ can be defined by the equation

$$\frac{Ze^{XZ}}{e^Z-1}=\sum_{n=0}^{\infty}\frac{B_n(X)}{n!}Z^n.$$

(2) Show that $B_{n+1}(X+1)-B_{n+1}(X)=(n+1)X^n$.

(3) Let $n,m\in\mathbb{N}$. Show that

$$\sum_{a=1}^{m}a^n=\frac{B_{n+1}(m)-B_{n+1}(0)}{n+1}=\frac{1}{n+1}\sum_{j=0}^{n}(-1)^j\binom{n+1}{j}B_jm^{n+1-j}.$$

This is called the **Faulhaber's formula**.

(4) Let $p$ be an odd prime and $n>0$ be even integer not divisible by $p-1$. Using (3), show that

$$\sum_{a=1}^{p}a^n\equiv pB_n\ (\mathrm{mod}\,p^2).$$

(5) Let $b\in\mathbb{N}$, $(b,p)=1$. Show that, for $1\leq a\leq p$, if $ab=px_a+r_a$ for $x_a,r_a\in\mathbb{Z}$, $0\leq r_a<p$,

$$(ab)^n\equiv r_a^n+pn(ab)^{n-1}\left\lfloor\frac{ab}{p}\right\rfloor\ (\mathrm{mod}\,p^2).$$

By adding the above equation over $1\leq a\leq p$, show

$$(b^n-1)\sum_{a=1}^{p}a^n\equiv pnb^{n-1}\sum_{a=1}^{p-1}a^{n-1}\left\lfloor\frac{ab}{p}\right\rfloor\ (\mathrm{mod}\,p^2).$$

(6) Let $p$ be an odd prime and $a,b$ be positive even integers such that $a\equiv b\not\equiv 0\ (\mathrm{mod}\,p-1)$ and $a,b$ are coprime to $p$. Using (4), (5), show that

$$\frac{B_a}{a}\equiv\frac{B_b}{b}\ (\mathrm{mod}\,p).$$

This is called the **Kummer's congruences**.

**Question 2.**

(1) Let $p$ be an odd prime. Recall that the Teichmüller character $\omega:\mathbb{F}_p^\times\to\mathbb{Z}_p^\times$ takes $a$ to the $(p-1)$-st root of unity congruent to $a$ mod $p$. Show that, for $1\leq a\leq p-1$,

$$\omega(a)\equiv a+\frac{a^{p-1}-1}{a^{p-2}}\ (\mathrm{mod}\,p^2).$$

(2) Let $p$ be an odd prime, and let $3 \leq i \leq p-2$ be an odd integer. Using Question 1, show that

$$B_{1,\omega^{-i}} \equiv \frac{B_{p-i}}{p-i} \pmod{p}.$$

This implies that one may replace $B_{1,\omega^{-i}}$ with $B_{p-i}$ in the statement of Herbrand's theorem.

**Question 3.** Let $p$ be a prime, and let $1 \leq a \leq b$. Show that the norm map

$$N_{\mathbb{Q}(\zeta_{p^b})/\mathbb{Q}(\zeta_{p^a})} : \mathrm{Cl}(\mathbb{Q}(\zeta_{p^b})) \to \mathrm{Cl}(\mathbb{Q}(\zeta_{p^a})),$$

is surjective. Deduce that $h_{\mathbb{Q}(\zeta_{p^a})}$ divides $h_{\mathbb{Q}(\zeta_{p^b})}$.

**Hint.** Show that, for any subextension $\mathbb{Q}(\zeta_{p^b})/K/\mathbb{Q}(\zeta_{p^a})$, the unique prime $\mathfrak{p}$ of $\mathbb{Q}(\zeta_{p^a})$ over $p$ is ramified in $K/\mathbb{Q}(\zeta_{p^a})$. Deduce that $H_{\mathbb{Q}(\zeta_{p^a})} \cap \mathbb{Q}(\zeta_{p^b}) = \mathbb{Q}(\zeta_{p^a})$.

**Question 4.** Let $p \equiv 3 \pmod{4}$ be a prime. Let $K = \mathbb{Q}(\sqrt{-p})$, and let $\chi_p$ be the quadratic Dirichlet character of modulus $p$ (cf. Definition 19.14).

(1) Show that Theorem 19.17(1) reads

$$h_K = -\frac{1}{p}\sum_{a=1}^{p} \chi_p(a)a = \frac{1}{p}\left(-2\sum_{a=1}^{\frac{p-1}{2}} \chi_p(a)a + p\sum_{a=1}^{\frac{p-1}{2}} \chi_p(a)\right).$$

**Hint.** We know exactly what the value of $G(\chi_p)$ is.

(2) Show that (1) can be massaged into

$$h_K = \frac{1}{p}\left(-4\sum_{a=1}^{\frac{p-1}{2}} \chi_p(2a)a + p\sum_{a=1}^{\frac{p-1}{2}} \chi_p(2a)\right).$$

**Hint.** $\chi(2a) = -\chi(p-2a)$.

(3) Show that (1) and (2) together gives

$$h_K = \frac{1}{2-\chi_p(2)}\sum_{a=1}^{\frac{p-1}{2}} \chi_p(a).$$

Deduce that there are more quadratic residues than non-residues in the interval $(0, \frac{p}{2})$.

(4) If $p \equiv 1 \pmod{4}$ is a prime, show that the number of quadratic residues in the interval $(0, \frac{p}{2})$ is the same as the number of quadratic non-residues.