Number Theory Homework #4 *Spring 2026*

Instructor: *Chan Ieong Kuan*

Solutions by: ***Haoyu Zhu***

Exercises

8 Gauss and Jacobi Sum

1. Exercise 8.21:

   Proof. Suppose that p is a prime and d is an integer. We want to show that

   $$\sum_x \zeta^{ax^d} = \sum_r N(x^d = r)\zeta^{ar}.$$

   To see this, compare the coefficients on both sides. Collect all solutions x with $x^d = r$; the number of such solutions is $N(x^d = r)$. Then the left-hand side can be rewritten as $\sum_r N(x^d = r)\zeta^{ar}$, where r runs over all elements of $\mathbb{Z}_p$. Hence the two sides are equal. □

2. Exercise 8.22:

   Proof. Use the fact that $N(x^d = a) = \sum_{\chi^d=\epsilon} \chi(a)$. $g_a(\chi) = \sum_t \chi(t)\zeta^{at}$. Therefore,

   $$\sum_x \zeta^{ax^d} = \sum_r N(x^d = r)\zeta^{ar} = \sum_r \sum_{\chi^d=\epsilon} \chi(a)\zeta^{ar} = \sum_{\chi^d=\epsilon} \sum_r \chi(a)\zeta^{ar} = \sum_{\chi^d=\epsilon} g_a(\chi).$$

   Moreover, when $\chi = \epsilon, g_a(\chi) = 0$. This completes the proof. □

9 Cubic and Biquadratic Reciprocity

3. Exercise 9.32:

Proof. Observe that $\chi_p(1+i) = \chi_\pi(1+i)\chi_{\overline{\pi}}(\overline{1-i})$, where $\chi_{\overline{\pi}}(\overline{a}) = \overline{\chi_\pi(a)}$. Hence

$$\chi_p(1+i) = \chi_\pi(1+i)\overline{\chi_\pi(1-i)}.$$

Now note that $(1-i)i = i - i^2 = i + 1 = 1 + i$. Thus $\chi_\pi(1+i) = \chi_\pi((1-i)i) = \chi_\pi(1-i)\chi_\pi(i)$. Substituting,

$$\chi_p(1+i) = \chi_\pi(1-i)\chi_\pi(i)\overline{\chi_\pi(1-i)} = \chi_\pi(i)\,|\chi_\pi(1-i)|^2 = \chi_\pi(i),$$

since the character takes values in the fourth roots of unity and thus $|\chi_\pi(1-i)|^2 = 1$. Finally, Proposition 9.8.6 gives $\chi_\pi(i) = i^{(p-1)/4}$. Therefore $\chi_p(1+i) = i^{(p-1)/4}$. □

4. Exercise 9.33:

Proof. We first accept $(1+i)^{q-1} \equiv -i \pmod q$, then

$$(1+i)^{(N(q)-1)/4} = (1+i)^{(q-1)(q+1)/4} \equiv (-i)^{(q+1)/4} \pmod q.$$

Now we prove $(1+i)^{q-1} \equiv -i \pmod q$. Write $q = 4k+3$, $k \in \mathbb{Z}$. Then

$$(1+i)^{q-1} \equiv (2i)^{(q-1)/2} = \left(\frac{2}{q}\right) i^{(q-1)/2} = (-1)^{(q^2-1)/8} i^{(q-1)/2} = (-1)^{k+1} i^{2k+1} = -i.$$

Hence the congruence holds, and therefore $\chi_q(1+i) = i^{(q+1)/4}$. □

5. Exercise 9.34:

Proof. We assume the result of Exercise 9.29: for a primary irreducible $\pi = a + bi$ with $(a,b) = 1$ and norm $p = a^2 + b^2$, we have

$$\chi_\pi\Big(a(-1)^{\frac{p-1}{4}}\Big) = (-1)^{\frac{a^2-1}{8}}.$$

(a) $\pi \equiv 1 \pmod 4$. Then $a \equiv 1 \pmod 4$ and $b \equiv 0 \pmod 4$. From Proposition 9.8.3(d) we have

$$\chi_\pi(-1) = (-1)^{\frac{a-1}{2}}.$$

Hence

$$\chi_\pi\Big((-1)^{\frac{p-1}{4}}\Big) = \big(\chi_\pi(-1)\big)^{\frac{p-1}{4}} = (-1)^{\frac{a-1}{2}\cdot\frac{p-1}{4}} = (-1)^{\frac{(a-1)(p-1)}{8}}.$$

Now apply Exercise 9.29:

$$\chi_\pi(a)\cdot\chi_\pi\Big((-1)^{\frac{p-1}{4}}\Big)=\chi_\pi\Big(a(-1)^{\frac{p-1}{4}}\Big)=(-1)^{\frac{a^2-1}{8}}.$$

Thus

$$\chi_\pi(a)=(-1)^{\frac{a^2-1}{8}-\frac{(a-1)(p-1)}{8}}.$$

We must show that the exponent on the right equals $\frac{a-1}{4}$ modulo 2. Since $p=a^2+b^2$ and $b\equiv 0 \pmod 4$, write $a=4k+1$, $b=4m$. Then

$$p=(4k+1)^2+(4m)^2=16k^2+8k+1+16m^2=8k+1 \pmod{16},$$

so

$$\frac{a^2-1}{8}-\frac{(a-1)(p-1)}{8}\equiv k-4k(k)\equiv k(2)$$

while $\frac{a-1}{4}\equiv k(2)$. Therefore

$$\chi_\pi(a)=(-1)^{\frac{a-1}{4}}=i^{\frac{a-1}{2}}.$$

(b) $\pi\equiv 3+2i \pmod 4$. Then $a\equiv 3 \pmod 4$ and $b\equiv 2 \pmod 4$. Again $\chi_\pi(-1)=(-1)^{\frac{a-1}{2}}$. As before,

$$\chi_\pi\Big((-1)^{\frac{p-1}{4}}\Big)=(-1)^{\frac{(a-1)(p-1)}{8}}.$$

Using Exercise 9.29 we obtain

$$\chi_\pi(a)=(-1)^{\frac{a^2-1}{8}-\frac{(a-1)(p-1)}{8}}.$$

Now set $a=4k+3$, $b=4m+2$. Then $a-1=4k+2$, $a+1=4k+4$, and

$$p=(4k+3)^2+(4m+2)^2=16k^2+24k+9+16m^2+16m+4=16(k^2+m^2)+24k+16m+13.$$

Hence $p-1=16(k^2+m^2+m)+24k+12$, so

$$(a-1)(p-1)/8=(4k+2)\big(16(k^2+m^2+m)+24k+12\big)/8\equiv 1(2).$$

Compute the exponent difference modulo 2:

$$\frac{a^2-1}{8}-\frac{(a-1)(p-1)}{8}\equiv k+1-1\equiv k(2).$$

Moreover, $-i^{(-a-1)/2}=(-1)^{(-a-1)/4+1}$, and $(-a-1)/4+1\equiv -k\equiv k(2)$, giving $\chi_\pi(a)=(-1)^k=-i^{(-a-1)/2}$. □

6. Exercise 9.35:

Proof. We first generalize Exercises 9.32 and 9.33: if $n \equiv 1 \pmod 4$, $n \neq 1$, then $\chi_n(1+i) = i^{(n-1)/4}$.

By Exercises 9.32 and 9.33, if $p \equiv 1 \pmod 4$ is a rational prime, then $\chi_p(1+i) = i^{(p-1)/4}$, and if $q \equiv 3 \pmod 4$ (so $-q \equiv 1 \pmod 4$) is a rational prime, then $\chi_{-q}(1+i) = i^{(-q-1)/4}$.

Let $n \in \mathbb{Z}$, $n \equiv 1 \pmod 4$, $n \neq 1$. We can decompose n in this way:

$$n = (-q_1)(-q_2)\cdots(-q_k)p_1\cdots p_\ell = s_1 s_2 \cdots s_N,$$

where $s_i = -q_i$ for $1 \leq i \leq k$, $s_i = p_{i-k}$ for $k+1 \leq i \leq N$, and each $s_i \equiv 1 \pmod 4$. If $n > 0$, then k is even. If $n < 0$, then k is odd. Hence

$$\chi_n(1+i) = \chi_{-q_1}(1+i)\cdots\chi_{-q_k}(1+i)\chi_{p_1}(1+i)\cdots\chi_{p_\ell}(1+i) = i^{(-q_1-1)/4}\cdots i^{(-q_k-1)/4}\cdots i^{(p_\ell-1)/4} = i^{(n-1)/4},$$

where the last equality follows from Exercise 9.44.

Now let $\pi = a + bi$ be primary and irreducible with $(a,b) = 1$. Since $a(1+i) = a + b + i(a+bi)$, we have $a(1+i) \equiv a + b \pmod \pi$, so

$$\chi_\pi(a)\chi_\pi(1+i) = \chi_\pi(a+b).$$

Because π is primary, $a + b \equiv 1 \pmod 4$. If $a + b = 1$, then $\chi_\pi(a)\chi_\pi(1+i) = \chi_\pi(1) = 1 = i^{3(a+b-1)/4}$. If not, the Law of Biquadratic Reciprocity (Proposition 9.9.8) gives

$$\chi_\pi(a+b) = \chi_{a+b}(\pi).$$

Now $b \equiv -a \pmod{a+b}$, so

$$\pi = a + bi \equiv a - ai = a(1-i) \equiv -ia(1+i) \pmod{a+b}.$$

Therefore,

$$\chi_{a+b}(\pi) = \chi_{a+b}(-1)\chi_{a+b}(a)\chi_{a+b}(i)\chi_{a+b}(1+i).$$

Since $a + b \equiv 1 \pmod 4$, Proposition 9.8.6 gives $\chi_{a+b}(i) = (-1)^{(a+b-1)/4}$, and Proposition 9.8.5 (given the fact that $(a+b, a) = 1$ because $(a,b) = 1$) gives $\chi_{a+b}(a) = 1$. Also $\chi_{a+b}(-1) = \chi_{a+b}(i^2) = (\chi_{a+b}(i))^2 = (-1)^{(a+b-1)/2} = 1$ since $a + b \equiv 1 \pmod 4$. From the first part, $\chi_{a+b}(1+i) = i^{(a+b-1)/4}$. Hence

$$\chi_{a+b}(\pi) = 1 \cdot 1 \cdot (-1)^{(a+b-1)/4} \cdot i^{(a+b-1)/4} = i^{(a+b-1)/2} \cdot i^{(a+b-1)/4} = i^{3(a+b-1)/4}.$$

Thus $\chi_\pi(a)\chi_\pi(1+i) = i^{3(a+b-1)/4}$, completing the proof. □

7. Exercise 9.36:

Proof. Suppose $q = (a, b) > 1$, $q \in \mathbb{Z}$. Write $a = qa_1$, $b = qb_1$, where $(a_1, b_1) = 1$. Then $\pi = q(a_1 + ib_1)$. Since π is irreducible and q is not a unit, $a_1 + ib_1$ must be a unit. Hence π is associate to the integer q, so q is a prime in $\mathbb{Z}[i]$ and therefore the rational prime $q \equiv 3 \pmod 4$.

If the unit $a_1 + ib_1$ were $\pm i$, then $\pi = \pm iq$ would give $a = 0$, which contradicts π being primary (since a primary Gaussian integer has $a \equiv 1 \pmod 2$). Thus $a_1 + ib_1 = \pm 1$. As π is primary, the sign must be -1 and $\pi = -q$. Then $\pi \equiv 1 \pmod 4$, and $\chi_\pi(a) = \chi_{-q}(-q) = 0$.

Remark *However, this is strange because we usually do not accept gcd* $(-q, 0) = q$*, and when* $\pi = -q \equiv 1 \pmod 4$*, it cannot be irreducible. I might make some mistakes.* □

8. Exercise 9.37:

Proof. We use Exercise 9.34 and 35 and inherit their setup of π. Let $\pi = a + ib$ be a primary irreducible in $\mathbb{Z}[i]$ with $(a, b) = 1$. From Exercise 9.35,

$$\chi_\pi(a)\chi_\pi(1 + i) = i^{3(a+b-1)/4}.$$

Case 1: $\pi \equiv 1 \pmod 4$

Write $a = 4A + 1$, $b = 4B$ with $A, B \in \mathbb{Z}$. By Exercise 9.34(a),

$$\chi_\pi(a) = i^{(a-1)/2}, \qquad \chi_\pi(a)^{-1} = (-i)^{(a-1)/2} = i^{(a-1)/2}.$$

Hence

$$\chi_\pi(1 + i) = i^{3(a+b-1)/4} \cdot i^{-(a-1)/2} = i^{\frac{3a+3b-3-2a+2}{4}} = i^{\frac{a+3b-1}{4}}.$$

We must show $\frac{a+3b-1}{4} \equiv \frac{a-b-b^2-1}{4} \pmod 4$. Their difference is

$$\frac{a + 3b - 1}{4} - \frac{a - b - b^2 - 1}{4} = \frac{4b + b^2}{4} = 4B + 4B^2 \equiv 0 \pmod 4.$$

Thus $\chi_\pi(1 + i) = i^{(a-b-b^2-1)/4}$.

Case 2: $\pi \equiv 3 + 2i \pmod 4$

Write $a = 4A - 1$, $b = 4B + 2$ with $A, B \in \mathbb{Z}$. By Exercise 9.34(b),

$$\chi_\pi(a) = -i^{(-a-1)/2}, \qquad \chi_\pi(a)^{-1} = -i^{(a+1)/2} = i^{(a-3)/2}.$$

Then

$$\chi_\pi(1+i) = i^{3(a+b-1)/4} \cdot i^{(a-3)/2} = i^{\frac{3a+3b-3+2a-6}{4}} = i^{\frac{5a+3b-9}{4}}.$$

Compute the difference between this exponent and $\frac{a-b-b^2-1}{4}$:

$$\frac{5a+3b-9}{4} - \frac{a-b-b^2-1}{4} = a+b-2+\frac{b^2}{4} = 4A+4B+(B+1)4B.$$

Hence $\frac{5a+3b-9}{4} \equiv \frac{a-b-b^2-1}{4} \pmod 4$, and therefore

$$\chi_\pi(1+i) = i^{(a-b-b^2-1)/4}.$$

□