Number Theory Homework #2 *Spring 2026*

Instructor: *Chan Ieong Kuan*

Solutions by: ***Haoyu Zhu***

Exercises

3 Quandratic Gauss Sums

1. Exercise 6.10:

   Proof. We compute directly:

   $$\sum_{a=1}^{p-1} g_a = \sum_{a=1}^{p-1} \left(\frac{a}{p}\right) g_1 = g_1 \sum_{a=1}^{p-1} \left(\frac{a}{p}\right) = 0.$$

   □

2. Exercise 6.15: we prove it for any general character $\chi \in \hat{\mathbb{F}_p^*} - \epsilon$.

   Proof. Let p be an odd prime, $\zeta = e^{2\pi i/p}$, and $g_1 = \sum_{t=1}^{p-1} \chi(t)\zeta^t$ with $|g_1| = \sqrt{p}$. For any integers $m \leq n$, define $S = \sum_{t=m}^{n} \chi(t)$. We have for $t \pmod p$:

   $$\chi(t) = \frac{1}{g_1} \sum_{a=1}^{p-1} \chi(a)\zeta^{at}.$$

   Thus

   $$S = \frac{1}{g_1} \sum_{a=1}^{p-1} \chi(a) \sum_{t=m}^{n} \zeta^{at}.$$

   For each a with $1 \leq a \leq p-1$, the geometric series's absolute value satisfies

   $$\left| \sum_{t=m}^{n} \zeta^{at} \right| \leq \frac{2}{|1-\zeta^a|},$$

   because $|\sum_{t=m}^{n} \zeta^{at}| = |\zeta^{am}| \cdot |1-\zeta^{a(n-m+1)}|/|1-\zeta^a| \leq 2/|1-\zeta^a|$. Now $|1-\zeta^a| = 2|\sin(\pi a/p)|$.we define b such that $a = p - b$. For $1 \leq a \leq p/2$, i.e. $a \leq b$, we have

$|\sin(\pi a/p)| \geq 2a/p$ (since $\sin x \geq 2x/\pi$ for $0 \leq x \leq \pi/2$). For $a > p/2$, i.e. $a > b$, we have $1 \leq b \leq p/2$; then $|1-\zeta^a| = |1-\zeta^{p-b}| = |1-\zeta^b| \geq 4b/p$. Consequently,

$$|1-\zeta^a| \geq \frac{4\min(a,b)}{p} = \frac{4\min(a,p-a)}{p}.$$

Hence

$$\left|\sum_{t=m}^{n} \zeta^{at}\right| \leq \frac{2}{4\min(a,p-a)/p} = \frac{p}{2\min(a,p-a)}.$$

Since $\chi(a)$ is the root of unity, its module is 1. Therefore,

$$|S| \leq \frac{1}{|g_1|}\sum_{a=1}^{p-1} 1 \cdot \frac{p}{2\min(a,p-a)} = \frac{\sqrt{p}}{2}\sum_{a=1}^{p-1}\frac{1}{\min(a,p-a)}.$$

The sum over a can be evaluated as

$$\sum_{a=1}^{p-1}\frac{1}{\min(a,p-a)} = 2\sum_{a=1}^{(p-1)/2}\frac{1}{a} < 2\log p.$$

In conclusion, we have

$$\left|\sum_{t=m}^{n}\chi(t)\right| < \frac{\sqrt{p}}{2}\cdot 2\log p = \sqrt{p}\log p.$$

Remark that when $m = 0$, we can extend the definition of χ to $\mathbb{F}_p$ by forcing $\chi(0) = 0$. Now we can deduce the statement where χ is the legendre symbol without difficulty. □

4 Finite Fields

3. Exercise 7.8:

Proof. Let $\mathbb{F}_{2^n}$ be a finite field of characteristic 2. Denote its multiplicative group by $\mathbb{F}_{2^n}^\times$, which is cyclic of order $2^n - 1$. Since 2 and $2^n - 1$ are coprime (because $2^n - 1$ is odd), the map

$$\varphi : \mathbb{F}_{2^n}^\times \longrightarrow \mathbb{F}_{2^n}^\times, \qquad \varphi(x) = x^2$$

is a group automorphism. In particular, φ is bijective sending one generator to another generator, so every element of $\mathbb{F}_{2^n}^\times$ is a square. Hence the subgroup of squares in $\mathbb{F}_{2^n}^\times$ is the whole group $\mathbb{F}_{2^n}^\times$. In addition, $0 = 0^2$, so the subgroup of squares of $\mathbb{F}_{2^n}$ is itself. □

4. Exercise 7.15:

Proof. Since $\gcd(q, n) = 1$, the characteristic p of $\mathbb{F}_q$ does not divide n. The derivative $f'(x) = nx^{n-1}$ is nonzero (because $n \not\equiv 0 \bmod p$) and has only the root 0, which is not a root of f. Hence $\gcd(f, f') = 1$ and f is separable.

Let ζ be a primitive n-th root of unity in K. Then all roots of $x^n - 1$ are ζ^k for $k = 0, 1, \ldots, n-1$, so $K = \mathbb{F}_q(\zeta)$. We need to determine $[\mathbb{F}_q(\zeta) : \mathbb{F}_q]$.

Consider the multiplicative group $\mathbb{F}_q(\zeta)^\times$, which is cyclic. The order of ζ is n. The Frobenius automorphism $\sigma : \mathbb{F}_q(\zeta) \to \mathbb{F}_q(\zeta)$ defined by $\sigma(x) = x^q$ fixes $\mathbb{F}_q$ pointwise. Its restriction to the Galois group $\mathrm{Gal}(\mathbb{F}_q(\zeta)/\mathbb{F}_q)$ is generated by σ. For any integer m, $\sigma^m(\zeta) = \zeta^{q^m}$. The degree $[\mathbb{F}_q(\zeta) : \mathbb{F}_q]$ equals the order of σ in the Galois group, i.e., the smallest positive integer f such that $\sigma^f(\zeta) = \zeta$. This condition is $\zeta^{q^f} = \zeta$, i.e., $\zeta^{q^f - 1} = 1$, which holds iff $n \mid (q^f - 1)$ because ζ has order n. Thus f is the smallest positive integer with $q^f \equiv 1 \pmod{n}$. Therefore

$$[\mathbb{F}_q(\zeta) : \mathbb{F}_q] = f.$$

In fact, the splitting field of $x^n - 1$ over $\mathbb{F}_q$ is $\mathbb{F}_{q^f}$ when q, n are coprime. □

5 Gauss and Jacobi Sums

5. Exercise 8.1:

Proof. Case $a = 0$: The equation $x^m = 0$ has the unique solution $x = 0$, so $N = 1$. In the character sum, only the trivial character contributes $\varepsilon(0) = 1$; all other characters vanish at 0. Hence the sum equals 1, matching N.

Case $a \neq 0$: *Subcase 1: a is an mth power.* Write $a = b^m$ with $b \in \mathbb{F}_p^\times$. The solutions are $x = b\zeta$ where $\zeta^m = 1$. The number of mth roots of unity in $\mathbb{F}_p$ is exactly $d = \gcd(m, p-1)$, so $N = d$. For any character χ with $\chi^d = \varepsilon$, we have

$$\chi(a) = \chi(b^m) = \chi(b)^m.$$

Since $d \mid m$, write $m = d \cdot m'$. Then $\chi(b)^m = (\chi(b)^d)^{m'} = \varepsilon(b)^{m'} = 1$. Thus each such χ contributes 1 to the sum. The set $\{\chi : \chi^d = \varepsilon\}$ is a subgroup of the character group of size d (the character group is cyclic of order $p-1$, and the subgroup of characters whose order divides d has exactly d elements). Hence the righthand side equals d, so $N = d$.

Subcase 2: a is not an mth power. Then $x^m = a$ has no solution, so $N = 0$. Define a character ρ of order d and $\rho(a) \neq 1$ and $\rho^d = \varepsilon$. Moreover,

$$\{\chi : \chi^d = \varepsilon\} = \{\rho^j : 0 \leq j < d\}.$$

Therefore

$$T = \sum_{\chi^d = \varepsilon} \chi(a) = \sum_{j=0}^{d-1} \rho^j(a) = \sum_{j=0}^{d-1} \big(\rho(a)\big)^j = \frac{1-\rho(a)^d}{1-\rho(a)} = 0,$$

since $\rho(a)^d = 1$ and $\rho(a) \neq 1$. Hence the character sum equals 0, matching $N = 0$.

All cases have been covered, so the formula holds for every $a \in \mathbb{F}_p$. □

6. Exercise 8.2:

Proof. Since $d = (d, p-1)$, we conclude that $N(x^m = a) = \sum \chi(a) = N(x^d = a)$. What's more, $N(\sum_i a_i x^{m_i} = b) = \prod_{\sum_i b_i = b} N(a_i x^{m_i} = b_i) = \prod_{\sum_i b_i = b} N(a_i x^{d_i} = b_i) = N(\sum_i a_i x^{d_i} = b)$. □