Analytic Number Theory Fall 2016, Assignment 4

Deadline: Thursday January 12

The total number of points is 70. Grade=(number of points)/7.

---

17. In this exercise we will use a p-adic version of the material in §8.1 to study Waring's problem for squares in $\mathbb{Z}/p\mathbb{Z}$. Recall that $\mathrm{e}_p(z) := \mathrm{e}^{\frac{2\pi i z}{p}}$ for $z \in \mathbb{R}$. You will need some results from Sections 4.4 (Gauss sums) and 4.5 (Quadratic reciprocity) from the lecture notes; only the results are needed and not the proofs.

For an odd prime p and any integer a coprime to p we define

$$S(p,a) := \sum_{\substack{y \in \mathbb{Z} \\ 1 \leqslant y \leqslant p}} \mathrm{e}_p\left(ay^2\right).$$

5 *a)* For an odd prime p we denote by χ_p the quadratic Legendre symbol modulo p, i.e., $\chi_p(x) = 1$ if p does not divide x and $y^2 \equiv x \,(\operatorname{mod} p$ is solvable, $\chi_p(x) = -1$ if $y^2 \equiv x \,(\operatorname{mod} p$ is not solvable, and $\chi_p(x) = 0$ if p divides x. You may use that this is a primitive Dirichlet character modulo p.

Show that if $\gcd(p,a) = 1$ then we have

$$S(p,a) = \tau(a, \chi_p),$$

where the notation $\tau(a, \chi_p)$ was introduced in §4.4 of the lecture notes. Furthermore show that

$$S(p,a) = \chi_p(a)\tau(1, \chi_p).$$

Hint. Prove that for all fixed integers x the number of $y(\text{mod } p)$ satisfying the equation $x \equiv y^2(\text{mod } p)$ is $1 + \chi_p(x)$. Then gather together all terms in $S(p,a)$ with a fixed value $y^2(\text{mod } p)$. For the last equality use Theorem 4.21.

5 *b)* For any integer n and any positive integer m prove that

$$\#\left\{(x_1, \ldots, x_m) \in (\mathbb{Z} \cap [1,p])^m : \sum_{i=1}^{m} x_i^2 \equiv n(\text{mod } p)\right\}$$

equals

$$p^{m-1} + \frac{\tau(1,\chi_p)^m}{p} \sum_{\alpha=1}^{p-1} \mathrm{e}_p(-\alpha n)\chi_p(\alpha)^m.$$

Hint. Use the same idea as in the first lines of the proof of Lemma 11.4 with $k=1$ and then the result of the previous exercise.

5 *c)* In case that m is even, prove that the sum over α in part (b) equals $p-1$ if p divides n and equals -1 otherwise. In case that m is odd, prove that the sum over α in part (b) equals 0 if p divides n and equals $\chi_p(-n)\tau(1,\chi_p)$ otherwise.
Hint. In case that m is even, prove and use that $\sum_{1\leqslant \alpha \leqslant p} \mathrm{e}_p(-\alpha n) = 0$ when $p \nmid n$.

5 *d)* Assume that $m \geqslant 3$ and let n be a fixed integer. Prove that the equation

$$y_1^2 + y_2^2 + \cdots + y_m^2 \equiv n (\mathrm{mod}\ p)$$

always has a solution.
Hint. Use parts $(b),(c),(d)$ to prove that the number of solutions, say N, satisfies

$$\left| N - p^{m-1} \right| \leqslant |\tau(1,\chi_p)|^m,$$

and then use Theorem 4.22.

5 *e)* For any odd prime p denote by $f(p)$ the function

$$f(p) := \#\Big\{(x_1,x_2,x_3) \in (\mathbb{Z} \cap [1,p])^3 : \sum_{i=1}^{3} x_i^2 \equiv 1(\mathrm{mod}\ p)\Big\}.$$

Prove that the function

$$\frac{f(p)-p^2}{p}, \ p \text{ odd prime},$$

changes sign infinitely often if p runs through the primes.
Hint. Use part (c) and Theorem 4.23 to find a simple expression for $f(p)$.

18. Let n and d be positive integers and define for all coprime integers a, m the sums

$$S_d(m,a) := \sum_{x \in \mathbb{Z} \cap [1,m]} \mathrm{e}_m\left(a x^d\right)$$

and

$$T_d(m) := \sum_{\substack{1 \leqslant a \leqslant m \\ \gcd(a,m)=1}} S_d(m,a)^n.$$

10 *a)* Assume that q_1, q_2 are coprime integers. Let $q := q_1 q_2$ and for any $a_1, a_2 \in \mathbb{Z}$ define

$$a := a_1 q_2 + a_2 q_1.$$

Prove that

$$S_d(q_1, a_1) S_d(q_2, a_2) = S_d(q, a).$$

Hint. Follow the proof of Lemma 11.2.

10 *b)* For any fixed positive integer d prove that the function $T_d(m)$ of m is multiplicative.
Hint. Follow the proof of Lemma 11.3.

19. Recall that if $R(n)$ denotes the number of representation of a positive integer n as a sum of 9 positive integer cubes then we have shown that

$$\lim_{n \to +\infty} \frac{R(n)}{n^2} = \frac{1}{2} \Gamma(4/3)^9 \mathfrak{S}(n),$$

where

$$\mathfrak{S}(n) := \sum_{q=1}^{\infty} \frac{S_n(q)}{q^9}$$

and

$$S_n(q) := \sum_{\substack{1 \leqslant a \leqslant q \\ \gcd(a,q)=1}} \mathrm{e}_q(-an) S(q,a)^9, \quad S(q,a) := \sum_{x=1}^{q} \mathrm{e}_q(ax^3).$$

The function $\mathfrak{S}(n)$ essentially contains information for the number of representations of n as a sum of 9 cubes in residue class rings $\mathbb{Z}/p^k\mathbb{Z}$ for prime powers p^k. The object of this exercise is to show that $\mathfrak{S}(n)$ has average 1. Define for each $x \geqslant 1$,

$$\mathbb{E}_x(\mathfrak{S}) := \frac{1}{x} \sum_{1 \leqslant n \leqslant x} \mathfrak{S}(n).$$

5 *a)* Prove that for all $\epsilon > 0$ we have

$$\mathfrak{S}(n) = \sum_{1 \leqslant q \leqslant x^{1/2}} \frac{S_n(q)}{q^9} + O_\epsilon(x^{-(1/8)+\epsilon})$$

and as a result that

$$\mathbb{E}_x(\mathfrak{S}) = \frac{1}{x} \sum_{1 \leqslant q \leqslant x^{1/2}} q^{-9} \sum_{1 \leqslant n \leqslant x} S_n(q) + O_\epsilon(x^{-(1/8)+\epsilon}).$$

Hint. Use Lemma 10.1 to prove that $q^{-9}|S_n(q)| \ll_\epsilon q^{-1-(1/4)+\epsilon}$. Then prove the estimate

$$\sum_{q>T} q^{-1-(1/4)+\epsilon} \ll \int_T^\infty u^{-1-(1/4)+\epsilon}\mathrm{d}u \ll T^{-(1/4)+\epsilon}.$$

5 *b)* For any integer m in the range $1 \leqslant m \leqslant q$ prove that whenever $n \in \mathbb{Z}$ satisfies $n \equiv m (\text{mod } q)$ then

$$S_n(q) = S_m(q).$$

As a consequence show that

$$\sum_{1\leqslant n\leqslant x} S_n(q) = \sum_{1\leqslant m\leqslant q} S_m(q) \sum_{\substack{1\leqslant n\leqslant x\\ n\equiv m (\text{mod } q)}} 1.$$

5 *c)* Recall that by splitting the interval $[1, x]$ in consecutive intervals of length q one can prove that

$$\sum_{\substack{1\leqslant n\leqslant x\\ n\equiv m (\text{mod } q)}} 1 = \frac{x}{q} + O(1),$$

with an absolute implied constant. Prove that for all $\epsilon > 0$,

$$\frac{1}{x}\sum_{1\leqslant m\leqslant q} S_m(q) \sum_{\substack{1\leqslant n\leqslant x\\ n\equiv m (\text{mod } q)}} 1 = \frac{1}{q}\sum_{1\leqslant m\leqslant q} S_m(q) + O_\epsilon\left(\frac{1}{x}q^{9-1/4+\epsilon}\right).$$

Hint. Use $q^{-9}|S_m(q)| \ll_\epsilon q^{-1-\frac{1}{4}+\epsilon}$.

5 *d)* Combining all parts of this exercise show that

$$\mathbb{E}_x(\mathfrak{S}) = 1 + \sum_{2\leqslant q\leqslant x^{1/2}} q^{-10} \sum_{1\leqslant m\leqslant q} S_m(q) + O_\epsilon(x^{-(1/8)+\epsilon}).$$

Hint. Use $q^{-9}|S_m(q)| \ll_\epsilon q^{-1-\frac{1}{4}+\epsilon}$.

5 *e)* Prove that if $q > 1$ then

$$\sum_{1\leqslant m\leqslant q} S_m(q) = 0$$

and conclude that $\mathbb{E}_x(\mathfrak{S}) = 1 + O_\epsilon(x^{-(1/8)+\epsilon})$ for all $\epsilon > 0$.

Remark. In part (e) you have proved that the singular series $\mathfrak{S}(n)$ is 1 on average and the error in this approximation converges quickly to zero, namely

$$\mathbb{E}_x(\mathfrak{S}) = 1 + O_\epsilon(x^{-\frac{1}{8}+\epsilon}).$$

Therefore, on average over all integers n, the value of $R(n)$ should be thought of as being very close to $\frac{1}{2}\Gamma(4/3)^9 n^2$.