C3.10 Additive and Combinatorial Number Theory, Hilary 2020
Exercises 2

Question 1. Let $q \geqslant 1$ be an integer, and suppose that a is coprime to q. Define

$$G^*_{a,q} := \frac{1}{q} \sum_{x \in (\mathbb{Z}/q\mathbb{Z})^*} e(-ax^k/q).$$

(Thus the definition is the same as that of the Gauss sum, only the sum over x is restricted to x coprime to q.) Show that if q is an odd prime power then

$$|G^*_{a,q}| \leqslant kq^{-1/2}.$$

Question 2. Let $s \geqslant 3$ be an integer. Suppose that $p \geqslant k^{(2s-2)/(s-2)}$. Show that there are $x_1, \dots, x_s \in \mathbb{Z}/p\mathbb{Z}$, not all zero, such that $x_1^k + \cdots + x_s^k \equiv N (\operatorname{mod} p)$.

Question 3. Let $k \geqslant 3$. Show that there are infinitely many q and $(a, q) = 1$ such that $|G_{a,q}| \gg q^{-1/k}$.

Question 4. Let k, s be positive integers. As in lectures, write

$$\beta_p(N) = \lim_{n \to \infty} \beta_{p,n}(N),$$

where

$$\beta_{p,n}(N) = p^{-(s-1)n}\{(x_1, \dots, x_s) \in (\mathbb{Z}/p^n\mathbb{Z})^s : x_1^k + \cdots + x_s^k \equiv N (\operatorname{mod} p^n)\}.$$

Show that $\beta_p(N) \gg_p 1$ in the following cases:

(i) $k = 2$, $s \geqslant 5$;

(ii) $k = 3$, $s \geqslant 9$ (*Hint: you may find it helpful to use Question 2*).

(You need not replicate things that were done in lectures carefully – just discuss the bits that are different.)

State, without careful proof, what conclusion follows about $\mathfrak{S}_{k,s}(N)$ in these cases.

Question 5. In this question, you may assume the *Cauchy-Davenport theorem*, which states that if $A, B \subseteq \mathbb{Z}/p\mathbb{Z}$ then either $A + B = \mathbb{Z}/p\mathbb{Z}$ or $|A + B| \geqslant |A| + |B| - 1$. (This is a result of additive combinatorics, but we won't prove it in the course; you may be interested in looking up a proof.)

Suppose that $p \geqslant 2k$. Show that every element of $\mathbb{Z}/p\mathbb{Z}$ is a sum of $2k$ kth powers.

Question 6. Let k be a positive integer, and let p be a prime. Suppose that $N \in \mathbb{Z}/p\mathbb{Z}$ is not $0 (\operatorname{mod} p)$. Write

$$S(r) = \sum_{x=1}^{p-1} e(rx^k/p).$$

(i) Show that if N is not the sum of two kth powers modulo p then

$$\sum_r S(r)^2 S(-Nr) = 0.$$

(ii) Show that

$$\sum_r |S(r)|^2 \leqslant kp(p-1).$$

(iii) Conclude that if $p > Ck^4$, for a sufficiently large absolute constant C, then every nonzero element of $\mathbb{Z}/p\mathbb{Z}$ is a sum of two kth powers. (*Hint: look at the expression in (i) and consider the contributions from* $r = 0$ *and* $r \neq 0$ *separately.*)

Question 7. Let k be a positive integer. Let M be a real number, and define a sequence $M_1, M_2, \dots, M_k$ by $M_1 := M$, $M_{i+1} := \frac{1}{10} M_i^{1-1/k}$. Show that if M is sufficiently large in terms of k then the integers $n_1^k + \cdots + n_k^k$, $n_i \in [M_i, 2M_i]$, are all distinct.

Deduce that, for large X, the number of integers $\leqslant X$ expressible as a sum of k kth powers is $\gg_k X^{1-(1-1/k)^k}$.

ben.green@maths.ox.ac.uk