Time limit: 80 minutes.
Maximum score: 181 points.
Instructions: For this test, you work in teams of eight to solve a multi-part, proof-oriented series of problems.

Problems that use the words "compute", "list", or "draw" only call for an answer; no explanation or proof is needed. Unless otherwise stated, all other questions require explanation or proof. Answers should be written on sheets of scratch paper, clearly labeled, with every problem *on its own sheet*. If you have multiple pages for a problem, number them and write the total number of pages for the problem (e.g. 1/2, 2/2).

Write your team ID number in the top right corner clearly on each sheet of paper that you submit. Only submit one set of solutions for the team. Do not turn in any scratch work. After the test, put the sheets you want graded into your packet. If you do not have your packet, ensure your sheets are labeled *extremely clearly* and stack the loose sheets neatly.

In your solution for a given problem, you may cite the statements of earlier problems (but not later ones) without additional justification, even if you haven't solved them.

The problems are ordered by content, NOT DIFFICULTY. It is to your advantage to attempt problems from throughout the test.
No calculators.

Common notation

We will use set notation throughout power round. Here is a guide to set notation. The format used is:

(math symbol): (meaning in words)

Sets

- $\varnothing$: empty set
- $a \in A$: a is an element of A
- $|A|$: the size of A
  Example. If $A = \{1, 2, 3\}$, then $|A| = 3$.
- $A \subseteq B$: A is a subset of B (i.e. all elements of A are elements of B)
  Example. $\{1, 2\} \subseteq \{1, 2\}$, $\varnothing \subseteq \{1, 2\}$ but $\{1, 2\} \not\subseteq \{1, 3\}$.
- $A \subset B$: A is a proper subset of B (i.e. $A \subseteq B$ and $A \neq B$)
  Example. $\{1, 2\} \subset \{1, 2, 3\}$, but $\{1, 2\} \not\subset \{1, 2\}$.
- $A \cap B$: the intersection of sets A and B
  Example. $\{1, 2\} \cap \{2, 3\} = \{2\}$.
- $A \cup B$: the union of sets A and B
  Example. $\{1, 2\} \cup \{2, 3\} = \{1, 2, 3\}$.
- $A \setminus B$: the set of elements in A but not in B
  Example. $\{1, 2\} \setminus \{2, 3\} = \{1\}$
- $\mathbb{N}$: the set of natural numbers (i.e. $\{1, 2, 3, ...\}$)
- $\mathbb{Z}$: the set of integers
- $\mathbb{Z}_{\geq 0}$: the set of non-negative integers
- $\mathbb{Q}$: the set of rational numbers
- $\mathbb{R}$: the set of real numbers
- $\mathbb{Z}_m$: the set of integers mod m (further explained in Section 2)

Functions

- $f : X \to Y$: f is a function taking values from set X and outputting values from set Y.
- $f : X \to Y$ is an *injection* if $f(x_1) \neq f(x_2)$ whenever $x_1 \neq x_2$.
- $f : X \to Y$ is a *surjection* if for every $y \in Y$, there exists $x \in X$ such that $f(x) = y$.

1 Introduction

The topic of this power round is sumsets, which are sets of sums. We start off with the definition of a sumset.

Definition: Let $A, B \subseteq \mathbb{R}$ be two non-empty sets. Then their **sumset** $A + B$ is defined as follows:

$$A + B = \{a + b \mid a \in A, b \in B\}.$$

In words, this means that $A+B$ consists of all possible sums of an element of A and an element of B. For example, $\{1, 2\} + \{10, 20\} = \{11, 12, 21, 22\}$ and $\{1, 2\} + \{3, 4\} = \{4, 5, 6\}$.

Analogously, we also define:

$$A - B = \{a - b \mid a \in A, b \in B\}.$$

Many famous theorems and conjectures can be expressed in the terminology of sumsets. Goldbach's conjecture says that every even integer greater than 2 is the sum of two primes. In sumset notation, this is the statement that $\{4, 6, 8, \dots\} \subset \mathbb{P} + \mathbb{P}$, where $\mathbb{P}$ is the set of prime numbers. The Lagrange Four Squares theorem states that every nonnegative integer is the sum of four squares. In sumset notation, this statement is $\mathbb{S} + \mathbb{S} + \mathbb{S} + \mathbb{S} = \mathbb{Z}_{\geq 0}$ where $\mathbb{S}$ are all the perfect squares including 0.

1. **[1]** Compute $\{0, 1, 4, 9\} + \{2, 3, 5, 7\}$.

2. **[1]** Show that the sumset operation + is associative, i.e. for sets $A, B, C \subset \mathbb{R}$,

   $$A + (B + C) = (A + B) + C.$$

   Subsequently, it makes sense to talk about $A + B + C$ (or even more additions) without brackets.

3. (a) **[2]** Let $S = \{0, 1, 2\}$, and define

   $$S_n = \underbrace{S + S + \ldots + S}_{n\ S's}.$$

   Find $|S_n|$.

   (b) **[2]** Let $S = \{0, 1, 3\}$, and define

   $$S_n = \underbrace{S + S + \ldots + S}_{n\ S's}.$$

   Find $|S_n|$.

4. For this problem, all sets are sets over $\mathbb{R}$. In this problem, we will be thinking about how the sumset + might be similar to the usual +.

   (a) **[3]** Let A, B, C be finite sets. Does $A+C = B+C$ necessarily imply $A = B$? Justify your answer.

   (b) **[5]** Let A, B be finite sets. Does

   $$\underbrace{A + A + \ldots + A}_{2019\ A\text{'s}} = \underbrace{B + B + \ldots + B}_{2019\ B\text{'s}}$$

   necessarily imply $A = B$? Justify your answer.

To further familiarize yourself with sumsets, here are *reverse sumset problems*: problems about determining unknown sumsets in sumset equations.

5. (a) **[1]** Can $\{1, 2, ..., 2019\}$ be expressed as $A + B$, where A, B are two finite subsets of $\mathbb{Z}$? Justify your answer.

   (b) **[2]** Can $\{1, 2, ..., 1004, 1006, ..., 2019\}$ be expressed as $A+B$, where A, B are two finite subsets of $\mathbb{Z}$? Justify your answer.

6. (a) **[5]** Does there exist a triplet of finite subsets (A, B, C) of $\mathbb{Z}_{\geq 0}$ such that the following "system of equations" holds? Justify your answer.
   - $A + B = \{0, 2, 3, 4, 5, 6, 7, 8, 9, 10, 11, 13\}$
   - $B + C = \{0, 1, 3, 4, 5, 6, 7, 8, 9, 11, 13, 15\}$
   - $C + A = \{0, 1, 2, 3, 4, 5, 6, 7, 8, 9, 10, 12\}$

   (b) **[5]** Consider the above problem, except that instead

   $$B + C = \{0, 1, 3, 4, 5, 6, 7, 8, 9, 11, 13, \mathbf{14}, 15\}$$

   Does there exist such a triplet of finite subsets (A, B, C)? Justify your answer.

7. Determine the number of ways $\{0, 1, 2, ..., n\}$ can be expressed as $A+B+C$, where A, B, C are subsets of non-negative integers of size 4 for

   (a) **[3]** $n = 8$,

   (b) **[5]** $n = 10$,

   (c) **[11]** $n = 13$.

8. **[5]** Given positive integers m, n, suppose that $S_1, S_2, ..., S_n$ are sets of integers where $|S_1| = |S_2| = ... = |S_n| = k$ for some positive integer k, and that

   $$\{0, 1, ..., m - 1\} \subseteq S_1 + S_2 + ... + S_n.$$

   Show that the minimum possible value of k in terms of m and n is $\lceil \sqrt[n]{m} \rceil$. Justify your answer.

9. We say that the sets A, B form a *decomposition* of $\mathbb{Z}$ (denoted as $A \oplus B = \mathbb{Z}$) if every $z \in \mathbb{Z}$ can be **uniquely expressed** as $a + b$ where $a \in A$ and $b \in B$.

   (a) **[3]** There is obviously at least one pair of sets A, B where $A \oplus B = \mathbb{Z}$ (because $\{0\} \oplus \mathbb{Z} = \mathbb{Z}$). Find a pair of such sets where both A and B contain an infinite number of elements, and provide a justification why they form a decomposition of $\mathbb{Z}$.

   To help you out, we will list down the small values for a possible pair of sets A, B. See if you can spot the pattern!

   $$A = \{0, 1, 4, 5, 16, 17, 20, 21, ...\}$$
   $$B = \{..., -42, -40, -34, -32, -10, -8, -2, 0\}$$

   (b) **[7]** Does there exist infinite sets A, B where $A \oplus B = \mathbb{Z} \setminus \{0\}$? Justify your answer.

An important idea that you will see recurring in this power round is that the size of $|A+B|$ can give us information regarding the structure of A and B. To start our investigation, let's think about the following: for finite subsets $A, B \subseteq \mathbb{R}$, how small (or large) can $|A + B|$ be?

10. (a) **[1]** Show that $|A + B| \leq |A| \cdot |B|$.

(b) **[3]** Show that $|A+B| \geq |A|+|B|-1$.

(c) **[5]** Determine all pairs of finite sets A, B where $|A+B| = |A|+|B|-1$.

(d) **[5]** Let $m, n, s \in \mathbb{N}$ satisfy $m+n-1 \leq s \leq mn$. Give a construction for finite subsets $A, B \subset \mathbb{R}$ where $|A| = m$, $|B| = n$ and $|A+B| = s$.

(Collectively, this means there are no other restrictions on $|A+B|$ other than parts (a) and (b).)

The proofs to these facts adapt easily to work for $\mathbb{N}, \mathbb{Z}$ and $\mathbb{Q}$.

2 Mod p

In this section, we will be thinking about sumsets under modular arithmetic.

In modular arithmetic, we consider the integers modulo some positive integer m. This means that every integer is characterized only by its remainder upon division by m, which we constrain to be between 0 and $m-1$, inclusive. In effect, two integers are considered the same, or are *congruent*, exactly when they have the same remainder upon division by m (or equivalently $m \mid (a-b)$).

Definition: We denote the integers mod m by $\mathbb{Z}_m$.

In this power round, when we work over $\mathbb{Z}_m$, we will evaluate all terms only in terms of their remainder upon division by m. Specifically, we require simplified numbers to be between 0 and $m-1$, inclusive. For instance, if we work in mod 5, $2+2=4$ but $2+3=0$ (since over $\mathbb{Z}$, $2+3=5$ and the remainder of 5 upon division by 5 is 0). Similarly, $3+3=1$, and $1-4=2$.

11. Evaluate the following sums in $\mathbb{Z}_{13}$:

(a) **[1]** $3+4$

(b) **[1]** $12+12$

(c) **[1]** $5+8$

(d) **[1]** $3-4$

We can also consider sumsets in $\mathbb{Z}_m$ where addition is done mod m. The following exercise practices computing sumsets with modular arithmetic.

12. Evaluate the following sumsets:

(a) **[1]** Working in $\mathbb{Z}_5$, what is $\{0,1\}+\{1,2,3\}$?

(b) **[1]** Working in $\mathbb{Z}_7$, what is $\{1,2,4\}+\{3,5\}$?

(c) **[1]** Working in $\mathbb{Z}_7$, what is $\{1,2,4\}-\{3,5\}$?

In this section, we will consider the behavior of sumsets over $\mathbb{Z}_p$, where p is a prime number. Consider $A, B \subseteq \mathbb{Z}_p$ for some given prime number p. It is natural to wonder about (again!) what $|A+B|$ could be. $|A+B| \leq |A| \cdot |B|$ still holds true, of course, but now the lower bound $|A+B| \geq |A|+|B|-1$ is less clear - methods used earlier should fail in this case.

In fact, what if $A = B = \{0, 1, ..., p-1\}$? Then $|A|+|B|-1$ exceeds p, but that can't happen. There are only p possible elements in $\mathbb{Z}_p$! The interesting thing is that once we take this restriction into account, the correct bound appears.

Theorem. (Cauchy-Davenport) For nonempty $A, B \subseteq \mathbb{Z}_p$, we have

$$|A+B| \geq \min\{p, |A|+|B|-1\}.$$

Let's try an easy case.

13. **[5]** Prove Cauchy-Davenport when $|A| + |B| \geq p + 1$.

    You should not use Cauchy-Davenport or reuse any parts of its proof from the next problem.

Now we will work through the proof of Cauchy-Davenport.
The rough approach we will take is as follows: we first start with counterexample sets A, B for contradiction. We consider two possible transformations applied to A and B such that $|A|$ (possibly) decreases, while both $|A| + |B|$ and $|A + B|$ are kept intact.

14. For the sake of establishing a contradiction, suppose there exists a counterexample sets A and B. In particular, we will consider the pair of sets such that $|A|$ is as small as possible.

    (a) **[3]** Supposing that $A \cap B \neq \varnothing$ (i.e. A and B intersect), by considering the sets $A \cap B$ and $A \cup B$, show that then $A \subseteq B$.

    (b) **[1]** Show that $|(A + \{x\}) + B| = |A + B|$ for any $x \in \mathbb{Z}_p$.

    (c) **[2]** Show that $B + A - A \subseteq B$. (Hint: consider which x cause $A + \{x\}$ and B to intersect.)

    (d) **[3]** Show that either $|A| = 1$ or $|B| = p$.

    (e) **[2]** Conclude that the original inequality is true.

    (f) **[3]** Does the Cauchy-Davenport inequality hold mod n where n is not a prime? If yes, prove the Cauchy-Davenport inequality for general n. Otherwise, provide a counterexample and state which of the above steps hold/do not hold.

15. (a) **[3]** Given nonzero $a_1, a_2, ..., a_i \in \mathbb{Z}_p$, show that their subset sums (sums of the form $\sum_{k \in S} a_k$ where $S \subseteq \{1, 2, ..., i\}$) take at least $\min\{i + 1, p\}$ distinct values.
    Note: If $S = \varnothing$, we define $\sum_{k \in S} a_k = 0$.

    (b) **[7]** Given integers $a_1, ..., a_{2p-1}$, show that we may select a subset of p of them such that their sum is divisible by p.

    (c) **[4]** In part (b), is $2p - 1$ the minimal possible value? Justify your answer.

    (d) **[7]** Does part (b) hold for general n (not necessarily prime)? Justify your answer.

3 Sidon Sets

Now that we've seen what happens if $|A + A|$ is small, what happens if it is big?

16. (a) **[2]** If A is an n-element subset of $\mathbb{N}$ what are the minimum and maximum possible values of $|A + A|$? Justify your answer.

    (b) **[1]** Given positive integer n, show that set $A = \{a_1, a_2, ..., a_n\} \subset \mathbb{N}$ attains the maximum possible value of $|A + A|$ in part (a) if and only if the following holds for any $i, j, k, l \in \{1, 2, ..., n\}$:

$$a_i + a_j = a_k + a_l \qquad \Rightarrow \qquad \{i, j\} = \{k, l\}$$

    Definition: If a set A satisfies this property, we say that A is **Sidon**.

    (c) **[3]** What is the maximal size of a Sidon subset of $\{1, 2, 3, ..., 9\}$? Justify your answer.

17. (a) **[2]** Prove that for a Sidon set A of size n, $|A - A| = n^2 - n + 1$.

    (b) **[5]** The set $\{1, 2, ..., 100\}$ is split into 7 subsets. Prove that at least one of them is not a Sidon set.

18. (a) **[2]** Does there exist a finite Sidon set $A \subset \mathbb{N}$ where A contains 100 consecutive values? Justify your answer.
    (b) **[7]** Does there exist a finite Sidon set $A \subset \mathbb{N}$ where $A + A$ contains 100 consecutive values? Justify your answer.
    (c) **[13]** Does there exists a Sidon set $A \subseteq \mathbb{N}$ where $A + A$ contains all natural numbers greater than k for some natural number k? Justify your answer.

4 Plünnecke's Inequality

For this section: all sets are finite subsets of $\mathbb{Z}$. Define for $n \in \mathbb{N}$, $nA = \underbrace{A + ... + A}_{nA\text{'s}}$

Let's think about the size $|A+A|$ as compared to $|A|$ - we call the ratio $|A+A|/|A|$ the **doubling factor** of A. From the results proved in Problem 10 (a),(b), we know that the doubling factor of A could be as big as $|A|$ or as small as $2 - \frac{1}{|A|}$. But if the doubling factor is $2 - \frac{1}{|A|}$, Problem 10 (c) tells us that we would know a fair bit about the structure of A.

Next, we consider the size of nA. We know that $|nA| \leq |A|^n$. However, if the doubling factor of A is small, we expect $|nA|$ to be a lot less than $|A|^n$. For instance, if $A = \{1, 2, ..., m\}$, the doubling factor is slightly less than 2, and $|nA| = mn - n + 1$, which is a lot less than $|A|^n = m^n$.

Below, we generalize slightly. If $|A + B|$ is small in relation to $|A|$, then sums involving only B are a lot smaller than the maximum bound. Specifically, the next problem will walk you through the proof of the following:

Theorem. (Plünnecke) For sets A, B, let $|A + B| = \alpha|A|$. Then for any $k, l \in \mathbb{N}$,

$$|kB - lB| \leq \alpha^{k+l}|A|$$

A good way to understand this is: if adding a copy of B increases the size of A by a factor of α, then the effect of adding B on a sum like $kB - lB$ is at most a factor of α as well ("in the long run" and "on average").

19. (a) **[3]** Assume that Plünnecke's theorem is true when A' is any non-empty subset $A' \subseteq A$ satisfying $|A' + B| \geq \alpha|A'|$. Prove Plünnecke's theorem in general.
    This means that for the rest of the proof, we can work with the additional assumption that any non-empty subset $A' \subseteq A$ satisfies $|A' + B| \geq \alpha|A'|$.
    (b) With the additional assumption above, we will show that $|A + B + C| \leq \alpha|A + C|$ for any finite set C. The statement is trivial for $|C| = 1$. Now we induct. Assume that we add an element x to C.
        i. **[2]** Show that for any set X,
        $$|X + (C \cup x)| = |X + C| + |X| - |(X + C - \{x\}) \cap X|.$$
        ii. **[2]** Show that
        $$\{x\} + B + A' \subseteq (A + B + C) \cap (A + B + \{x\})$$
        where $A' = (A + C - \{x\}) \cap A$.
        iii. **[7]** Complete the inductive step, and conclude that the inequality is true.
    (c) **[2]** Conclude that $|A + kB| \leq \alpha^k|A|$.
    (d) **[6]** (Rusza's inequality) For sets X, Y, Z, show that
    $$|X| \cdot |Y - Z| \leq |X + Y| \cdot |X + Z|.$$
    (Hint: consider an injection from $X \times (Y - Z) \to (X + Y) \times (X + Z)$)
    (e) **[2]** Conclude that Plünnecke's inequality is true.