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 $\{0, 1, 4, 9\} + \{2, 3, 5, 7\}$.

   Solution to Problem 1:

   Answer. $\{2, 3, 4, 5, 6, 7, 8, 9, 11, 12, 14, 16\}$

   Straightforward computation yields:

+	0	1	4	9
2	2	3	6	11
3	3	4	7	12
5	5	6	9	14
7	7	8	11	16

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.

   Solution to Problem 2: I claim that both sides are equal to $\{a+b+c \mid a \in A, b \in B, c \in C\}$. Note that $A+(B+C) = A+\{b+c \mid b \in B, c \in C\} = \{a+(b+c) \mid a \in A, b \in B, c \in C\}$ and $(A + B) + C = \{a + b \mid a \in A, b \in B\} + C = \{(a + b) + c \mid a \in A, b \in B, c \in C\}$. Since addition in reals is associative, these two sets will be equal.

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

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

   Find $|S_n|$.

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

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

Find $|S_n|$.

Solution to Problem 3:

(a) The answer is $|S_n| = 2n + 1$. It is easily seen by induction that $S_n = \{0, 1, \dots, 2n\}$.

(b) The answer is $|S_n| = 3n$. We will show by induction that $S_n = \{0, 1, ..., 3n - 2, 3n\}$. This is clearly true for $n = 1$, and it is simple to verify that

$$\{0, 1, ..., 3n - 2, 3n\} + \{0, 1, 3\} = \{0, 1, ..., 3n + 1, 3n + 3\}.$$

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

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

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

Solution to Problem 4:

(a) No. Consider $C = \{0, 1, 2, ..., 10\}$, $A = \{0, 4, 11\}$, $B = \{0, 5, 11\}$

(b) No. Take $A = \{0, 1, 3, 4\}$, $B = \{0, 1, 2, 3, 4\}$. Then $A + A = B + B = \{0, 1, 2, ..., 8\}$, and so $A + A + A = B + B + B$. Hence,

$$\begin{aligned}\underbrace{A + A + ... + A}_{2019\ A\text{'s}} &= \underbrace{(A + A + A) + ... + (A + A + A)}_{673\ (A+A+A)\text{'s}} \\ &= \underbrace{(B + B + B) + ... + (B + B + B)}_{673\ (B+B+B)\text{'s}} \\ &= \underbrace{B + B + ... + B}_{2019\ B\text{'s}}.\end{aligned}$$

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.

Solution to Problem 5: The answer to both parts is yes since any set $A = A + \{0\}$.

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.

Solution to Problem 6:

(a) **Answer.** The only solution(s) are as follows:

$$A = \{0, 2, 3, 5\}, \quad B = \{0, 4, 6, 8\}, \quad C = \{0, 1, 3, 7\} \text{ or } \{0, 1, 3, 5, 7\}.$$

An idea that can help in the search of the subset is that the maximum and minimum elements are preserved by sumset addition (i.e. $\max A + \max B = \max(A + B)$). Hence, we are able to solve for the maximum elements of each set. In particular, for this problem,

$$(\max A, \max B, \max C) = (5, 8, 7).$$

To actually find the set, we note that if $x \notin A + B$, then $x, x - \max B \notin A$ and $x, x - \max A \notin B$. Performing this algorithm, we get the desired solution, which can be verified.

(b) There does not exist such a triplet. We reuse the reasoning in the part above to obtain

$$(\max A, \max B, \max C) = (5, 8, 7).$$

The fact that $B + C$ contains 14 implies that either $6 \in C$ (then $C + A$ should contain 11, contradiction) or $7 \in B$ (then $A + B$ should contain 12), both of which lead to a contradiction.

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]** $n = 13$.

Solution to Problem 7:

(a) *Answer.* 0 ways
Note that $\max(A + B + C) = \max A + \max B + \max C \geq 9$.

(b) *Answer.* 9 ways. Again, we use the fact that $\max(A + B + C) = \max A + \max B + \max C$, so without loss of generality, let $(\max A, \max B, \max C) = (3, 3, 4)$. C is of the form $\{0, 1, 2, 3, 4\} \setminus \{x\}$ where $x = 1, 2, 3$. Hence, there are $3 \times 3 = 9$ ways in total.

(c) *Answer.* 477 ways.
Assume without loss of generality that $\max A \leq \max B \leq \max C$. First, note that 0 must appear in all three sets, so we must now pick the remaining three numbers for each set.

We will split cases based on $M = (\max A, \max B, \max C)$ (temporarily ignoring the ordering for this triple). Since the maximum is always attained, our main concern is that all middle values are attained. Define the *spread* of a set to be the maximum difference between adjacent elements of a set. In each case, we will try to set up

additions of the form $X+Y$ where $X = \{0, 1, 2, ..., k-1\}$ (we say X is *contiguous*) and Y has spread at most k. This will mean that $X+Y = \{0, 1, 2, ..., k-1+\max Y\}$.
Case 1: $M = (3, x, y)$. Then because $x \le 5$, so B has spread at most 3. Hence $A+B$ is contiguous and $\max A+B \ge 6$. But clearly $y \le 7$, so the spread of C is at most 7, hence $A+B+C$ is contiguous for any choice of B and C. Hence, our options are $M = (3, 3, 7)$, $M = (3, 4, 6)$, and $M = (3, 5, 5)$, so the number of ways to choose the remaining 2 elements for each of the three sets is

$$3\binom{2}{2}\binom{6}{2} + 6\binom{3}{2}\binom{5}{2} + 3\binom{4}{2}\binom{4}{2} = 45 + 180 + 108 = 333.$$

Case 2: $M = (4, 4, 5)$. In this case, we are required to characterize A and B separately. Write:

$$A = \{0, 1, 2, 3, 4\} \setminus \{a\}, \qquad B = \{0, 1, 2, 3, 4\} \setminus \{b\}$$

where neither a nor b can be 0 or 4. Note that if a, b are distinct, then $x \notin A$ implies $x \in B$ and vice versa. This means that when we write some number as $x + y \le 8$, we can always find either $x \in A$ and $y \in B$ or $x \in B$ and $y \in A$, so $A + B$ does not miss a number in between.
Otherwise $a = b$, and this is not a problem unless $a = 1$ (then $1 \notin A + B$) or $a = 3$ (then $7 \notin A + B$).
If $A + B$ is contiguous, then $A + B + C$ has to be contiguous. Otherwise, it is only a problem if C also doesn't contain one of 1 or $\max C - 1$. Hence, the total for this case is

$$3\binom{3}{2}\binom{3}{2}\binom{4}{2} - (3)(2)\binom{2}{2}\binom{2}{2}\binom{3}{2} = 162 - 18 = 144.$$

Hence the total is $333 + 144 = 477$.

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.

Solution to Problem 8: The minimum value is $k = \lceil \sqrt[n]{m} \rceil$.
Note that the RHS is of size at most k^n, so we require $k^n \ge m$. We claim that $k = \lceil \sqrt[n]{m} \rceil$ is sufficient. Let $S_i = \{0, k^{i-1}, 2k^{i-1}, ..., (k-1)k^{i-1}\}$, then any number N between 0 to $m - 1 \le k^n - 1$ (inclusive) may be expressed as

$$N = a_0 + a_1 k + a_2 k^2 + ... + a_{n-1} k^{n-1}$$

where $a_i \in \{0, 1, ..., k-1\}$ (this is precisely the base-k representation of N). It is clear that by construction, $N \in S_1 + S_2 + ... + S_n$.

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.

Solution to Problem 9:

(a) **Method 1**: Going according to the hint, we claim that

$$A = \{\text{nonnegative integers which can be expressed without 2's and 3's in base 4}\},$$
$$B = \{-2a \mid a \in A\}.$$

Our main claim is the following: every integer n is uniquely represented as

$$n = \sum_{i=0}^{k} b_i(-2)^i$$

where $b_i \in \{0, 1\}$ and $b_k \neq 0$.

We can prove this inductively: b_0 is uniquely determined by taking mod 2, so we can consider $\frac{b_0 - n}{2}$, which is closer to 0 than n unless $n \in \{-1, 0, 1\}$. Assuming it has a unique decomposition, then n will also have a unique decomposition.

If we now group the terms $b_i(-2)^i$ where i is even, we get an element of A. Similarly, if we group those terms where i is odd, we get an element of B.

Method 2: Use the same method as in part (b).

(b) Yes. We will construct such sets inductively. Let $A_0 = B_0 = \varnothing$, and $A_1, A_2, \ldots$ and $B_1, B_2, \ldots$ be sequences of sets constructed as follows. We hope that

$$A = \bigcup_{i=0}^{\infty} A_i, \quad B = \bigcup_{i=0}^{\infty} B_i$$

will form our decomposition. For each $n \geq 0$, define

$$A_{n+1} = A_n \cup \{a\}, \quad B_{n+1} = B_n \cup \{b\}$$

The main idea is that we can use $a + b$ to "patch" up the number closest (but not equal to) 0 that is not already in $A_n + B_n$. Due to unique representation condition, we require

$$A_n + B_n, \quad \{a\} + B_n, \quad \{b\} + A_n, \quad \{a + b\}$$

to be disjoint for $n > 0$. To achieve this, we add the constraint that $a > \max(A_n + B_n - B_n)$ and $b < \min(A_n + B_n - A_n)$.

By construction, $A_n + B_n$ eventually covers every nonzero integer, so $A + B$ covers $\mathbb{Z} \setminus \{0\}$. Yet, every nonzero integer has a unique representation.

Explicitly, our construction gives that

$$A = \{1, -1, 5, 13, ...\}$$

$$B = \{0, -3, -10, ...\}$$

Comment. This method works for any $\mathbb{Z} \setminus S$ where $|S|$ is finite.

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).)

Solution to Problem 10:

(a) There are at most $|A| \cdot |B|$ pairs of the form (a, b).

(b) Let $A = \{a_1 < a_2 < ... < a_m\}$ and $B = \{b_1 < b_2 < ... < b_n\}$. Then

$$a_1 + b_1 < ... < a_m + b_1 < ... < a_m + b_n$$

so there are at least $m+n-1$ elements in $A+B$.

(c) Let $A = \{a_1 < a_2 < ... < a_m\}$ and $B = \{b_1 < b_2 < ... < b_n\}$. Let $C = \{c_1 < c_2 < ... < c_{m+n-1}\}$. Then consider the sequence:

$$a_1 + b_1 < ... < a_i + b_1 < ... < a_i + b_j < ... < a_m + b_j < ... < a_m + b_n$$

Hence $a_i + b_j = c_{i+j-1}$. This implies that $a_{i+1} - a_i = b_{j+1} - b_j$ for any $1 \leq i < m, 1 \leq i < n$, so A and B are arithmetic progressions with the same difference.

(d) Fix $A = \{1, 2, ..., m-1\}$. Then for any $b \in B$, $b, b+1, ..., b+(m-1) \in A+B$. So we can make $\min B = 0$, $\max B = s-m+1$, and spread out the rest of the elements of B so that no two differ by more than m.

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]** $3-4$

Solution to Problem 11:

(a) *Answer.* 7
(b) *Answer.* 11
(c) *Answer.* 0
(d) *Answer.* 12

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 $\{1,2,4\}-\{3,5\}$?

Solution to Problem 12:

(a) *Answer.* $\{0,1,2,3,4\}$
(b) *Answer.* $\{0,2,4,5,6\}$
(c) *Answer.* $\{1,3,4,5,6\}$

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.

Solution to Problem 13:

For any $x \in \mathbb{Z}_p$, we have that $|A|+|\{x\}-B| = |A|+|B| \geq p+1$ so by the Pigeonhole Principle, A and $\{x\}-B$ must intersect. Hence $x \in A+B$ for any $x \in \mathbb{Z}_p$. So, $|A+B| = p$ which satisfies Cauchy-Davenport.

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.

Solution to Problem 14:

(a) Note that $|A|+|B| = |A\cap B|+|A\cup B|$, but $A+B \supseteq (A\cap B)+(A\cup B)$, so $(A\cap B, A\cup B)$ is a smaller counterexample unless $|A \cap B| = |A|$, or $A \subseteq B$.

(b) Using the associative property from Problem 2, we have $(A+\{x\})+B = (A+B)+\{x\}$, which is simply a translation of $A + B$.

(c) For any $x \in B + (-A)$, we have $A + \{x\}$ intersects B. Then using part (b) and applying part (a), we have $A + \{x\} \subseteq B$. Hence $A + (B + (-A)) \subseteq B$.

(d) If $|A| > 1$, consider distinct $a, a' \in A$, then if $b \in B$, $b + a - a' \in B$, so by induction $b + k(a - a') \in B$. Since p is prime, we can obtain all possible elements by varying k, so $|B| = p$.

(e) We assumed at the start of the problem that a counterexample exists, and thus a counterexample with minimal $|A|$ exists. From parts (a) - (d), this counterexample satisfies either $|A| = 1$ or $|B| = p$. However, in either case, the inequality holds (i.e. our assumption that it was a counterexample was incorrect). Hence, no counterexamples exists and the Cauchy-Davenport theorem is true.

(f) It does not hold. For instance, consider $A = B = \{0, 2\}$ mod 4. The very last step fails.

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.

Solution to Problem 15:

(a) **Approach 1**: by induction. If adding a_i does not give a new value, then the previous set is invariant after shifting $+a_i$, and so it must contain everything. Otherwise, each a_i added gives at least one new value.

Approach 2: use Cauchy-Davenport on $\{0, a_1\} + \{0, a_2\} + \dots$.

(b) Without the loss of generality, let $a_1 \le a_2 \le ... \le a_{2p-1}$. Consider the set $\{a_{p+k} - a_k | 1 \le k \le p - 1\}$. If some $a_{p+k} - a_k = 0$, that means $a_k = a_{k+1} = ... = a_{p+k}$, so we have found at least p equal elements and their sum is thus divisible by p. Otherwise, $a_{p+k} - a_k \ne 0$, so using part (a), the subset sums take at least p distinct values (i.e. all of $\mathbb{Z}_p$). Therefore, there exists a subset $S \subseteq \{1, 2, ..., p - 1\}$ such that

$$\sum_{k\in S}(a_{p+k} - a_k) = -(a_1 + a_2 + ... + a_p).$$

We may rewrite this as (denoting $[p] = \{1, 2, 3, ...p\}$ for convenience)

$$\sum_{k\in S} a_{p+k} + \sum_{i\in[p]\setminus S} a_i = 0.$$

(c) Yes. A counterexample for $2p - 2$ is

$$\underbrace{0, 0, ..., 0}_{p-1 \text{ 0's}}, \underbrace{1, 1, ..., 1}_{p-1 \text{ 1's}}.$$

(d) Yes. If $p \mid n$, starting from $2n - 1$ numbers, we take $2p - 1$ of them and apply the hypothesis for prime p. This gives us a group of p numbers whose sum is divisible by p. We can repeat this operation as long as there are at least $2p - 1$ numbers remaining. At the very end, we have extracted $2(n/p) - 1$ numbers which are all divisible by p. Then we may repeat this exact argument for some prime $q \mid (n/p)$.

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.

Solution to Problem 16:

(a) *Answer.* Min: $2n - 1$. Max: $\binom{n+1}{2}$.
The minimum value is at least $2n - 1$ (by problem 10(b)). The minimum is attained at $A = \{0, 1, 2, ..., n - 1\}$.
The maximum value is at most the number of unordered pairs of elements of A. So, there are $\frac{n^2-n}{2}$ unordered pairs of the form (a, b) where $a \neq b$ and n pairs of the form (a, a). In total, this is $\frac{n^2+n}{2} = \binom{n+1}{2}$. This maximum value is attained when $A = \{1, 10, 10^2, ..., 10^{n-1}\}$.

(b) If the maximum value is attained, this means that each unordered pair of elements in A must have a unique sum. This is exactly the conclusion.

(c) *Answer.* 5 integers.
Construction. 1, 2, 3, 5, 8.
Bound. If instead 6 integers were selected, they will form 15 pairwise sums. But all possible pairwise sums range from $3, 4, ..., 17$. Notice that 3 and 17 can be each expressed in exactly one way:

$$3 = 1 + 2, \quad 17 = 8 + 9$$

This means that $1, 2, 8$, and 9 all have to be chosen, which is impossible because $1 + 9 = 2 + 8$.

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.

Solution to Problem 17:

(a) Suppose that $a_i - a_j = a_k - a_l$. Then $a_i + a_l = a_j + a_k$, so $(a_i, a_l) = (a_j, a_k)$ (which means that $a_i - a_j = 0$ and $i = j$), or $(a_i, a_j) = (a_k, a_l)$ which means nonzero differences are unique. From here on, we have a counting argument since there are n^2 pairs of which n have difference 0. So, there $|A - A| = n^2 - n + 1$.

(b) By pigeonhole, at least one set has 15 elements. If this set were Sidon, there would be at least 221 possible differences. But differences of numbers in the set $\{1, 2, ..., 100\}$ range from -100 to 100, a contradiction.

Comment. Note that if we considered the sums, this estimate would have failed.

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.

Solution to Problem 18:

(a) Obviously not: if it contains $N, N+1, N+2$, then $(N+1)+(N+1) = N+(N+2)$.

(b) Yes. We proceed via induction. Suppose that there exists finite Sidon set $A_k \subset \mathbb{N}$ such that $A_k + A_k$ covers k consecutive elements $[m, m - k + 1]$.

The key observation is that $A'_k = A_k + \{x\}$ satisfies the exact same condition because $A'_k + A'_k$ contains $[m + 2x, m - k + 2x + 1]$ (and not $m + 2x + 1$.). Hence the strategy is to add $\{1, N\}$ to A'_k where x and N are so large so that for $a' \in A'_k$, $1 + a', N + a'$ are respectively too small and too large to interfere with $A'_k + A'_k$, whereas $1 + N$ adds to the length of the consecutive sequence.

Naturally, we need to take $N = m+2x$, and $x > 2\max A_k$. Then, $1+x < 2(\min A+x)$ while

$$(N + \min A'_k) - (2 \max A'_k) = m + x + \min A_k - (2 \max A_k) > 0.$$

Hence, $A_{k+1} = A'_k \cap \{1, N\}$ covers $k + 1$ consecutive numbers, and clearly we have a valid base case $A_1 = \{1\}$. The conclusion follows.

Comment. This is the same idea as problem 16(b) (about decompositions).

(c) Pick $X = A \cap [1, N]$ and $Y = A \cap [N + 1, 2N]$ for a big enough value of N.

Speaking in very rough terms (and for big enough N so that k is insignificant), $X+Y$ is at least size $2\sqrt{N}$ because its pair sums cover $(k, 2N]$. X is at least size $\sqrt{2N}$. But if we count differences:

$$\begin{aligned} N - 1 &\geq \binom{|X|}{2} + \binom{|Y|}{2} \\ &\geq \binom{|X|}{2} + \binom{2\sqrt{N} - |X|}{2} \\ &\geq \binom{\sqrt{2N}}{2} + \binom{(2-\sqrt{2})\sqrt{N}}{2} \\ &\gtrsim 1.1N \end{aligned}$$

where $3 - 2\sqrt{2} > 0.1$.

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.

Solution to Problem 19:

(a) Because substituting A with A' gets us a tighter inequality. Suppose otherwise that $|A' + B| < \alpha|A'|$. Then, let $|A' + B| = \alpha'|A'|$, where $\alpha' < \alpha$. So proving the inequality for (A', B) gives us:

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

(b) i. Use $|P|+|Q|=|P\cap Q|+|P\cup Q|$ for $P=X+C$ and $Q=X+\{x\}$.

ii. Consider $a'=a+c-x$ where $a'\in A', a\in A, c\in C$. Then, for any $b\in B$, $x+b+a'=a+b+c$ and the conclusion follows.

iii. We have

$$\begin{aligned}|A+B+(C\cup\{x\})| &= |A+B+C|+|A+B|-|(A+B+C-\{x\})\cap(A+B)|\\ &= |A+B+C|+|A+B|-|(A+B+C)\cap(A+B+\{x\})|\\ &\geq |A+B+C|+|A+B|-|\{x\}+B+A'|\\ &= |A+B+C|+|A+B|-|A'+B|\\ &\geq \alpha(|A+C|+|A|-|A'|)\\ &= \alpha(|A+(C\cup\{x\}|).\end{aligned}$$

(c) Set $C=(k-1)B$, then $|A+kB|\leq\alpha|A+(k-1)B|$ and the result follows by induction.

(d) Express every $w\in Y-Z$ as $w=y(w)-z(w)$, where $y:W\to Y$ and $z:W\to Z$. Consider the injection $(x,w)\mapsto(x+y(w),x+z(w))$. Then, if $x_1+y(w_1)=x_2+y(w_2)$ and $x_1+z(w_1)=x_2+z(w_2)$, subtracting we get $w_1=y(w_1)-z(w_1)=y(w_2)-z(w_2)=w_2$ and subsequently $x_1=x_2$. So we have an injection and the size of $X\times(Y-Z)$ must be smaller than the size of $(X+Y)\times(X+Z)$.

(e) Note that

$$|A|\cdot|kB-lB|\leq|A+kB|\cdot|A+lB|\leq\alpha^{k+l}|A|^2.$$