Number Theory

Jacob Denson

October 15, 2018

Table Of Contents

Chapter 1

Generating Functions

Example. *Suppose we are working in a country with only a one, a two, and a three penny coin. Given an integer n, let $r(n)$ denote the number of ways that a person can be paid n pennies using these three coins. Since this is a question about the additivity of numbers, we can likely understand it using generating functions. Formally,*

$$r(n) = \#\{(a,b,c) : a + 2b + 3c = n\}$$

We note

$$\left(\sum_{a=0}^{\infty} z^a\right)\left(\sum_{b=0}^{\infty} z^{2b}\right)\left(\sum_{c=0}^{\infty} z^{3c}\right) = \sum_{a,b,c} z^{a+2b+3c} = \sum_{n=0}^{\infty} r(n) z^n$$

Thus, for $|z| < 1$,

$$\sum_{n=0}^{\infty} r(n) z^n = \frac{1}{(1-z)(1-z^2)(1-z^3)}$$

We can now perform a partial fraction decomposition, writing

$$\frac{1}{(1-z)(1-z^2)(1-z^3)} = \frac{1}{(1-z)^3(1+z)(\omega - z)(\omega + z)}$$

where $\omega = e(1/3)$ is a primitive third root of unity. Some intense linear algebra shows this is equal to

$$\frac{z+2}{9(z^2+z+1)} + \frac{17z^2 - 52z + 47}{72(1-z)^3} + \frac{1}{8(1+z)}$$

which can be further decomposed into

$$-\frac{\omega^2+3\omega+2}{9(1-z/\omega)}+\frac{\omega^2-\omega+2}{9(1-z/\omega^2)}$$
$$+\frac{1}{6(1-z)^3}+\frac{1}{4(1-z)^2}+\frac{17}{72(1-z)}+\frac{1}{8(1+z)}$$

where $\omega = e(1/3)$. *Taking power series and summing up, we find*

$$\begin{aligned} r(n) &= -\frac{\omega^2+3\omega+2}{9\omega^n}+\frac{\omega^2-\omega+2}{9\omega^{2n}}+\frac{(n+1)(n+2)}{12}+\frac{n+1}{4}+\frac{17}{72}+\frac{(-1)^n}{8} \\ &= \frac{6n^2+36n+47+9(-1)^n}{72}+\begin{cases} 0 & n \equiv 0 (mod\ 3) \\ -2/9 & n \equiv 1\ or\ 2 (mod\ 3) \end{cases} \\ &= \frac{(n+3)^2}{12}+\frac{9(-1)^n-7}{72}+\begin{cases} 0 & n \equiv 0 (mod\ 3) \\ -16/72 & n \equiv 1\ or\ 2 (mod\ 3) \end{cases} \end{aligned}$$

We know $r(n)$ *is an integer, and since*

$$\frac{9+7+16}{72}=\frac{32}{72}<\frac{1}{2}$$

So $r(n)$ *is the closest integer to* $(n+3)^2/12$.

Chapter 2

Additive Combinatorics

Given a subset A of an abelian group, we say A is **sum free** if $A + A$ is disjoint from A.

Theorem 2.1. *If A is an arbitrary finite subset of positive natural numbers, then A contains a sum-free subset of size greater than $|A|/3$.*

Proof. The idea of this proof rests on two observations. If $B \subset [1,N]$, and $p > 2N$, then $B + p\mathbf{Z}$ is sumfree in $\mathbf{Z}_p$ if and only if B is sumfree. Thus we can turn out problem into a problem modulo p. Next, we notice that if f is an automorphism, then a subset B of an abelian group is sumfree if and only if $f(B)$ is sumfree. The presense of many automorphisms of $\mathbf{Z}_p$ (one for each natural number between 1 and $p-1$) enables us to exploit randomness to construct a sumfree subset in A. If $X \subset \mathbf{Z}_p$ is sumfree, and does *not* contain zero, we consider the sets $X, 2X, \dots, (p-1)X$, which are all sumfree. For every $a \in X$, and nonzero $b \in \mathbf{Z}_p$, there is a unique $c \in \{1, \dots, p-1\}$ such that $ca = b$. Thus every nonzero $b \in \mathbf{Z}_p$ occurs in $|X|/(p-1)$ of the sets $X, \dots, (p-1)X$. Thus means if we choose a nonzero $x \in \mathbf{Z}_p$ uniformly at random, then

$$\mathbf{E}|(A + \mathbf{Z}_p) \cap xX| = \sum_{a \in A + \mathbf{Z}_p} \mathbf{P}(a \in xX) = \frac{|A||X|}{p-1}$$

Since xX is sumfree, so too is $(A + \mathbf{Z}_p) \cap xX$, and so lower bounding the expectation gives rise to a large sumfree sert. In $\mathbf{Z}_p$, a good candidate for a sumfree set should be an interval, since an arithmetic progression has a small sumset, and all arithmetic progressions are mapped to an interval by an automorphism. Thus, taking $X = \{k, \dots, 2k-1\}$, where $4k - 2 < p + k$, we get a squarefree set. Thus taking p congruent to two modulo 3, and setting $3k = p + 1$, we find a sumfree set of size

$$\frac{k}{p-1}|A| = \frac{p+1}{3(p-1)}|A| > |A|/3$$

which completes the proof. □

A fundamental problem in additive combinatorics is the *inverse sumset* problem. If $A + B$ or $A - B$ is small, what can one say about A and B? More specifically, if $A + A$ is small, what can one say about A? We have $|A| \leqslant |A+A| \leqslant [|A|^2 + |A|]/2$, and so we refer to the value $\sigma(A) = |A+A|/|A|$ as the **doubling constant** of the set A. We have $1 \leqslant |A| \leqslant (|A|+1)/2$.

Example. *Geometric progressions have the largest doubling constant possible. If*

$$A = \{1, a, a^2, \dots, a^{N-1}\}$$

then the sum of any two elements of A is distinct, so $|A + A| = (N^2 + N)/2$, *and so* $\sigma(A) = (N+1)/2$.

A set A with $\sigma(A)$ maximal among sets of size N is known as a **Sidon set**. This means that all pairwise sums of any two $a_0, a_1 \in A$ are distinct, modulo the trivial equalities $a_0 + a_1 = a_1 + a_0$. This is a 'generic' behaviour: If A is a subset of N points chosen uniformly at random frmo $[0,1]$, then A is Sidon with probability one. It is more interesting to characterize when $\sigma(A)$ is small.

Example. *In the other extreme, the main example of sets with small doubling constant is an arithmetic progression. If* $A = b_0 + [0, N-1]a$, *then* $A + A = 2b_0 + [0, 2N-2]a$, *which consists of* $2N - 1$ *points, so* $\sigma(A) = 2 - 1/N$.

Example. *If* $A \subset B$, *and* $|A| = \alpha|B|$, *then* $|A + A| \leqslant |B + B|$, *so*

$$\sigma(A) \leqslant \frac{|B+B|}{K|B|} = \sigma(B)/\alpha$$

Thus if $\sigma(B)$ *is small, and A contains a large percentage of B, then* $\sigma(A)$ *is also small. In the other direction, if* $|B| = \beta|A|$, *then*

$$|B+B| \leqslant |A+A| + |A+(B-A)| + |(B-A)+(B-A)| \leqslant \sigma(A)|A| + (\beta-1)|A|^2 + \beta^2|A|^2$$

so

$$\sigma(B) \leqslant \sigma(A)/\beta + (\beta + 1 - 1/\beta)|B|$$

Thus if $\sigma(A)$ is small, and B doesn't contain many more points than A, then $\sigma(B)$ is also small.

Example. *If we consider N and M, and a resultant 'rank 2' arithmetic progression $A = c + [0,N]a + [0,M]b$, then $\sigma(A) \leqslant 4$. These sets can look very different from the original arithmetic progressions we were considering.*

The constant $\sigma(A)$ indicates the amount of additive structure in A. There are other variants of the measure of additive structure in A, like the additive energy $E(A,A)$ and approximate group structures, which are closely related to one another.

2.1 Graph Theoretic Techniques

Theorem 2.2 (Turán)**.** *Let G be a graph of n vertices. Then G contains an independant set of size at least*

$$\sum_{v \in G} \frac{1}{\deg(v) + 1}$$

In particular, if the vertices have degree bounded by d, then there is an independant set of size $|G|(d+1)^{-1}$.

Proof. Let $\pi : V \to \{1, \dots, n\}$ be a uniformly randomly chosen bijection. Let S be the set of all vertices v in V such that for any neighbour w of v, $\pi(v)$ is larger than $\pi(w)$. Then S is an independant set, and it suffices to show S is large in expectation. We find by the hockey stick identity that

$$\begin{aligned}
\mathbf{P}(v \in S) &= \frac{1}{n!} \sum_{m=1}^{n} \binom{m-1}{\deg(v)} \deg(v)!(n-1-\deg(v))! \\
&= \frac{\deg(v)!(n-1-\deg(v))!}{n!} \binom{n}{\deg(v)+1} \\
&= \frac{1}{\deg(v)+1}
\end{aligned}$$

and so

$$\mathbf{E}|S| = \sum_{v \in G} \mathbf{P}(v \in S) = \sum_{v \in G} \frac{1}{\deg(v)+1}$$

and this gives the required set. □

Given $B \subset A$, we say B is sumfree with respect to A if no element of A is the sum of two distinct elements of B. Given A, we let $\phi(A)$ denote the largest sumfree subset with respect to A. We let $\phi(n)$ be the smallest value of $\phi(A)$ among all sets $A \subset \mathbf{R}$ of size n.

Theorem 2.3 (Choi)**.** *If A is any set of n real numbers, there is a set $B \subset A$ of cardinality $\log n - O(1)$ sumfree with respect to A. Thus $\phi(n) \geqslant \log n - O(1)$.*

Proof. Assume first that A is a subset of positive reals. Order $A = \{a_1 > a_2 > \cdots > a_n > 0\}$. Consider the graph G with vertices A, and edges (a_n, a_m) if $a_n + a_m \in A$. By Turán's theorem, since $\deg(a_i) \leqslant n - i$, we find an independant set S with

$$|S| \geqslant \sum_{i=1}^{n} \frac{1}{n-i+1} = \sum_{i=1}^{n} \frac{1}{i} = \log n - O(1)$$

In general, any set A of n real numbers either contains $n/2 - O(1)$ positive real numbers or $n/2 - O(1)$ negative real numbers, and the theorem then follows in this case. □

The $n/(d+1)$ bound for graphs of bounded degree d cannot be improved for general graphs G. However, it is surprising that one can improve the bound by a $\log d$ factor, provided that the resultant graph has no three cycles.

Theorem 2.4. *If G has no three cycles with maximal degree d, then G contains an independant set of size $\Omega(n \log d/d)$.*

Proof. Choose a set I uniformly from the set of all independant sets in G. For each $v \in V$, define the random variable

$$X_v = d|I \cap \{v\}| + |N(v) \cap I| = \begin{cases} d & v \in I \\ |N(v) \cap I| & v \notin I \end{cases}$$

Any vertex can be in the neighbourhood of at most d other vertices, so

$$\sum_v X_v = d|I| + \sum_{v \notin I} |N(v) \cap I| \leqslant 2d|I|$$

Taking expectations gives that

$$\mathbf{E}|I| \geqslant \frac{1}{2d} \sum_v \mathbf{E}(X_v)$$

Thus it suffices to show that $\mathbf{E}(X_v)$ is large for each v. TODO: FINISH LATER. □

The Balog-Szemerédi theorem says that if $E(A,B) \geqslant K_0 n^2$ and $|A +_G B| \leqslant K_1 n$, then one can find $A_0 \subset A$ and $B_0 \subset B$ such that $|A_0|, |B_0|$, and $|A_0 + B_0|$ are $\Theta_{K_0,K_1}(n)$. Gower's recently strengthened the theorem to showing the constants in the bound are polynomial in $1/K_0$ and K_1. We shall find that this result can be converted into a graph problem.

If $E(A,B) \gtrsim |A|^{3/2}|B|^{3/2}$, then there is $A_0 \subset A$ and $B_0 \subset B$ with $|A_0| \sim |A|$, $|B_0| \sim |B|$, and $|A_0 + B_0| \lesssim |A_0|^{1/2}|B_0|^{1/2}$. In particular, if A and B have n elements, and $E(A,B) \gtrsim n^3$, then there is $A_0 \subset A$ and $B_0 \subset B$ with $|A_0|, |B_0| \sim n$, and $|A_0 + B_0| \lesssim n$. Can we generalize this theorem to more general operations than addition, i.e. linear transformations of the coordinates?

Lemma 2.5. *If G is a bipartite graph with $|E| \geqslant |A||B|/K$ for some $K \geqslant 1$, then for any $0 < \varepsilon < 1$, there is $A_0 \subset A$ such that $|A_0| \geqslant |A|/K\sqrt{2}$, and such that $1 - \varepsilon$ of the pairs of vertices in A_0 are connected by $\varepsilon|B|/2K^2$ paths of length 2 in G.*

Proof. By decreasing K, we may assume that $|E| = |A||B|/K$. Now

$$\frac{\mathbf{E}_b|N(b)|}{|A|} = \frac{\mathbf{E}_a|N(a)|}{|B|} = \frac{|E|}{|A||B|} = \frac{1}{K}$$

and

$$\frac{\mathbf{E}_b|N(b)|^2}{|A|^2} = \mathbf{E}_{a,a'} \frac{|N(a) \cap N(a')|}{|B|}$$

□

Let $A_1, \dots, A_k$ be additive sets with cardinality n, and consider a k uniform k-partite hypergraph H on $A_1, \dots, A_k$. If H has $\Omega(n^k)$ edges and $|\bigoplus^H A_i| = O(n)$, then we can find $A_i' \subset A_i$ with $|A_i'| = \Omega(n)$ and $|A_1' + \cdots + A_k'| = \Omega(n)$. If we let H be