Chapter 15

Combinatorial number theory

15.1. Partitions

Exercise 15.1.1. Deduce that the number of partitions of n into odd parts is equal to the number of partitions of n with no repeated parts.

Exercise 15.1.2. Prove that there is a bijection between self-conjugate partitions and partitions where all the entries are odd and distinct. Give an elegant form for the generating function for the number of self-conjugate partitions.

15.2. Jacobi's triple product identity

Exercise 15.2.1. Prove that

$$\prod_{\ell\geq 1}(1-t^{\ell})(1-t^{2\ell-1}) = \prod_{n\geq 1}(1-t^{2n})(1-t^{2n-1})^2 = \sum_{m\in\mathbb{Z}}(-1)^m t^{m^2}.$$

Exercise 15.2.2. By writing $1+t^k$ as $(1-t^{2k})/(1-t^k)$ or otherwise, deduce that

$$\sum_{m\geq 0} t^{\frac{m^2+m}{2}} = \frac{(1-t^2)(1-t^4)(1-t^6)\cdots}{(1-t)(1-t^3)(1-t^5)\cdots}.$$

Exercise 15.2.3. Interpret this combinatorially, in terms of the number of partitions of m into unequal parts.

Exercise 15.2.4. Show that if $(12/.)$ is the Jacobi symbol, then

$$t\prod_{n\geq 1}(1-t^{24n}) = \sum_{m\geq 1}\left(\frac{12}{m}\right)\, t^{m^2}.$$

Exercise 15.2.5. Write the power series on the right-hand side of (15.2.3) as $\sum_{n\geq 1} f(n)t^n$.

(a)† Prove that $f(pq) = f(p)f(q)$ for any distinct primes p, q.

(b)‡ Prove that $f(\cdot)$ is a multiplicative function.

Exercise 15.2.6 (Proof of Jacobi's triple product identity)**.** Define

$$P_N(x,z) := \prod_{k=1}^{N}(1-x^{2k})(1+x^{2k-1}z)(1+x^{2k-1}z^{-1}) = \sum_{n\in\mathbb{Z}} c_{N,n}(x)\ z^n.$$

(a) Prove that $c_{N,n}(x) \in \mathbb{Z}[x]$; $c_{N,n}(x) = 0$ for $n > N$, and $c_{N,-n}(x) = c_{N,n}(x)$.
(b) Prove that $P_{N+1}(x,z) = (1-x^{2N+2})(1+x^{2N+1}z)(1+x^{2N+1}z^{-1})P_N(x,z)$.
(c)† Deduce that

$$c_{N+1,n}(x) = (1-x^{2N+2})(x^{2N+1}c_{N,n-1}(x) + (1+x^{4N+2})c_{N,n}(x) + x^{2N+1}c_{N,n+1}(x)).$$

(d) Prove that $c_{N,n}(x) = x^{n^2}\prod_{m=N-n+1}^{N}(1-x^{2m})\cdot\prod_{m=N+n+1}^{2N}(1-x^{2m})$ for $0 \le n \le N$, for all $N \ge 1$.
(e) Show that if $|x| < 1$, then $\lim_{N\to\infty} c_{N,n}(x) = x^{n^2}$ for every integer n.
(f) Deduce Jacobi's triple product identity.

15.3. The Freiman-Ruzsa Theorem

Exercise 15.3.1. Give an example of a set A of n integers for which $|2A| = n(n+1)/2$.

Exercise 15.3.2. Explain the bijection between $A \cdot B$ and $\log A + \log B$.

Exercise 15.3.3. Deduce the sum-product inequality for any $\epsilon > 2/3$.

15.4. Expansion and the Plünnecke-Ruzsa inequality

15.5. Schnirelman's Theorem

15.6. Classical additive number theory

Exercise 15.6.1. Justify that if $N \ge r(N(r-1)-1)+2$, then there must be some color c for which there are $\ge N(r-1)$ edges adjacent to v of color c. Show by induction that we may take $N(r) \le 3\ r!$

Exercise 15.6.2. Prove that $W(2,3) = 9$.

Exercise 15.6.3. Deduce that if the positive integers are partitioned into r sets, then at least one of the sets must contain arbitrarily long arithmetic progressions.

Exercise 15.6.4. Prove that if we color any arithmetic progression of integers of length $W(r,k)$ with r colors, then it will contain a monochromatic k-term arithmetic progression.

Exercise 15.6.5. Partition the integers into two sets neither of which has an infinitely long arithmetic progression.

Exercise 15.6.6. Show that if $N \ge N_{k,\delta}$ and A is a subset of an arithmetic progression of length N, with $|A| \ge \delta N$, then A contains an arithmetic progression of length k .

Exercise 15.6.7. Deduce van der Waerden's Theorem from Szemerédi's Theorem.

Exercise 15.6.8. Show that a, b, c are in arithmetic progression if and only if $a + c = 2b$.

Exercise 15.6.9. Write $a = \sum_{i=1}^{k} a_i(2m)^{i-1} \in C := C(0,1,2m,\dots,(2m)^{k-1}; m,\dots,m)$.
(a) Show that a is an integer in the range $0 \le a \le (2m)^k - 1$.
(b) Show that $a, b, c \in C$ are in arithmetic progression if and only if the vectors $\mathbf{a}= (a_1,\dots,a_k)$, $\mathbf{b}$, and $\mathbf{c}$ are collinear.
(c) Show that $|\mathbf{a}|^2$ is an integer in the range $0 \le |\mathbf{a}|^2 \le km^2$.
(d) Let $C_r = \{\mathbf{a} \in C : \ |\mathbf{a}| = r\}$. Show no three distinct elements of C_r are collinear.
(e) Prove that there exists an r for which C_r contains $\ge m^k/(1+km^2)$ elements.
(f)† By selecting $k = [\sqrt{\log N}]$ and $m = [N^{1/k}/2]$ prove that if N is sufficiently large, then $S(N) > Ne^{-c\sqrt{\log N}}$ for some constant $c > 0$.

15.7. Challenging problems

Exercise 15.7.1.† Prove that for every set of integers $a_1, \dots, a_n$ there exists a non-empty subset which sums to an integer divisible by n.

Exercise 15.7.2.† Suppose that $1 \le a_1 < \cdots < a_n$ are positive integers, and let the integers $0 = b_1 < b_2 \le \cdots \le b_{2^n}$ be all the sums of subsets of the a_i, that is, the numbers $\sum_{i \in I} a_i$ for each $I \subset \{1, 2, \dots, n\}$.

(a) Write down the generating function, $\sum_{j=1}^{2^n} x^{b_j}$, in terms of polynomials involving the a_i. Henceforth we will assume that the b_j are all distinct.

(b) Prove that $b_j \ge j - 1$ for each j.

(c) Deduce that if $0 \le x \le 1$, then $\sum_{j=1}^{2^n} x^{b_j} \le \frac{1-x^{2^n}}{1-x}$.

(d) Deduce further that $\prod_{i=1}^{n}(1 + x^{a_i}) \le \prod_{k=1}^{n}(1 + x^{2^{k-1}})$.

(e) Prove that if $a > 0$, then $\int_0^1 \frac{\log(1+x^a)}{x} dx = \frac{1}{a} \int_0^1 \frac{\log(1+y)}{y} dy$.

(f) Deduce that $\sum_{i=1}^{n} \frac{1}{a_i} \le 2 - \frac{1}{2^n}$ with equality only when each $a_i = 2^{i-1}$.

Exercise 15.7.3.† Let $a_1, \dots, a_N$ be a sequence of distinct real numbers. Prove that if m is the length of the longest decreasing subsequence, and n is the length of the longest increasing subsequence, then $mn \ge N$.

Appendix 15A. Summing sets modulo p

15.8. The Cauchy-Davenport Theorem

Exercise 15.8.1. Suppose that A is a subset of $\mathbb{Z}/p\mathbb{Z}$ with at least two elements. Show that if $n \ge \frac{p-1}{|A|-1}$, then $nA = \mathbb{Z}/p\mathbb{Z}$.

Exercise 15.8.2. Use Theorem 15.9 to show that if A and B are finite sets of integers, then $|A + B| \ge |A| + |B| - 1$.

Exercise 15.8.3. Suppose that A is a subset of $\mathbb{Z}/N\mathbb{Z}$ and that A additively generates all of $\mathbb{Z}/N\mathbb{Z}$; that is, there exists r for which $rA = \mathbb{Z}/N\mathbb{Z}$. Prove that $NA = \mathbb{Z}/N\mathbb{Z}$.

Exercise 15.8.4. We give another proof of Theorem 15.8.

(a) Show that any sequence of $2m$ (not necessarily distinct) residues mod p either has $m + 1$ identical residues, or can be partitioned into m sets of two distinct residues.

(b) Prove that if $A_1, \dots, A_{p-1}$ are subsets of $\mathbb{Z}/p\mathbb{Z}$ which each contain two distinct residues, then $A_1 + \cdots + A_{p-1} = \mathbb{Z}/p\mathbb{Z}$.

(c) Deduce Theorem 15.8.

Appendix 15B. Summing sets of integers

15.9. The Frobenius postage stamp problem, III

Exercise 15.9.1. Let $A = \{a, b, c\}$ where $a < b < c$ are integers for which $(b - a, c - b) = 1$. Prove that if N is sufficiently large, then

$$NA = \{n \in \mathbb{Z} : \ aN \le n \le cN\} \setminus (aN + \mathcal{E}(b - a, c - a)) \setminus (cN - \mathcal{E}(c - b, c - a)).$$

Exercise 15.9.2. Suppose that $a_1 = 0$.

(a) Use exercise 15.8.3 to show that if $m \geq a_k^2$, then $m \in \mathcal{P}(a_1, \ldots, a_k)$.

(b) Let $N \geq 2a_k$. Prove that if $a_k^2 \leq m \leq a_k(N - a_k)$, then $m \in NA$.

(c) Let $N \geq a_k^2$. Prove that if $m \leq a_k^2$ and $m \in \mathcal{P}(a_1, \ldots, a_k)$, then $m \in NA$.

(d) Let $N \geq a_k^2$. Deduce that if $m \geq a_k N - a_k^2$ and $m \in a_k N - \mathcal{P}(a_k - a_1, \ldots, a_k - a_k)$, then $m \in NA$.

(e) Prove that if N is sufficiently large, then

$$NA = \{n \in \mathbb{Z} : \ 0 \leq n \leq a_k N\} \setminus \mathcal{E}(a_1, \ldots, a_k) \setminus (a_k N - \mathcal{E}(a_k - a_1, \ldots, a_k - a_k)).$$

(f) State the general result when a_1 is not necessarily 0.