Formal Book

formalizing “Proofs from THE BOOK” by Martin Aigner and Günter M. Ziegler

Moritz Firsching, Nick Kuhn, Pietro Monticone, Ralf Stephan, Christopher Schmidt, Christoph S

November 23, 2024

Chapter 1

Six proofs of the infinity of primes

Theorem 1.1 (Euclid's proof)**.** *A finite set $\{p_1, \dots, p_r\}$ cannot be the collection of* all *prime numbers.*

Proof. For any finite set $\{p_1, \dots, p_r\}$, consider the number $n = p_1 p_2 \dots p_r + 1$. This n has a prime divisor p. But p is not one of the p_is: otherwise p would be a divisor of n and of the product $p_1 p_2 \dots p_r$, and thus also of the difference $n - p_1 p_2 \dots p_r = 1$, which is impossible. So a finite set $\{p_1, \dots, p_r\}$ cannot be the collection of *all* prime numbers. □

Theorem 1.2 (Second Proof)**.** *Any two Fermat numbers $F_n := 2^{2^n} + 1$ are relatively prime.*

Proof. Let us first look at the Fermat numbers $F_n = 2^{2^n} + 1$ for $n = 0, 1, 2, \dots$. We will show that any two Fermat numbers are relatively prime; hence there must be infinitely many primes. To this end, we verify the recursion

$$\prod_{k=0}^{n-1} F_k = F_n - 2,$$

from which our assertion follows immediately. Indeed, if m is a divisor of, say, F_k and F_n (with $k < n$), then m divides 2, and hence $m = 1$ or 2. But $m = 2$ is impossible since all Fermat numbers are odd. To prove the recursion we use induction on n. For $n = 1$, we have $F_0 = 3$ and $F_1 - 2 = 3$. With induction we now conclude

$$\prod_{k=0}^{n} F_k = \left(\prod_{k=0}^{n-1} F_k \right) F_n = (F_n - 2) F_n = (2^{2^n} - 1)(2^{2^n} + 1) = 2^{2^{n+1}} - 1 = F_{n+1} - 2.$$

□

Theorem 1.3 (Third Proof)**.** *There is no largest prime.*

Proof. Suppose $\mathbb{P}$ is finite and p is the largest prime. We consider the so-called *Mersenne number* $2^p - 1$ and show that any prime factor q of $2^p - 1$ is bigger than p, which will yield the desired conclusion. Let q be a prime dividing $2^p - 1$, so we have $2^p \equiv 1 \pmod{q}$. Since p is prime, this means that the element 2 has order p in the multiplicative group $\mathbb{Z}_q \;\; \{0\}$ of the field $\mathbb{Z}_q$. This group has $q - 1$ elements. By Lagrange's theorem, we know that the order of every element divides the size of the group, that is, we have $p \mid q - 1$, and hence $p < q$. □

Theorem 1.4 (Fourth Proof)**.** *The prime counting function is unbounded*

Proof. Let $\pi(x) := \#\{p \leq x : p \in \mathbb{P}\}$ be the number of primes that are less than or equal to the real number x. We number the primes $\mathbb{P} = \{p_1, p_2, p_3, \dots\}$ in increasing order. Consider the natural logarithm $\log x$, defined as

$$\log x = \int_1^x \frac{1}{t} dt.$$

Now we compare the area below the graph of $f(t) = \frac{1}{t}$ with an upper step function. (See also the appendix for this method.) Thus for $n \leq x < n + 1$ we have

$$\log x \leq 1 + \frac{1}{2} + \frac{1}{3} + \dots + \frac{1}{n-1} + \frac{1}{n} \leq \sum \frac{1}{m},$$

where the sum extends over all $m \in \mathbb{N}$ which have only prime divisors $p \leq x$.

Since every such m can be written in a unique way as a product of the form $\prod_{p \leq x} p^{k_p}$, we see that the last sum is equal to

$$\prod_{p \in \mathbb{P}, p \leq x} \left(\sum_{k \geq 0} \frac{1}{p^k} \right).$$

The inner sum is a geometric series with ratio $\frac{1}{p}$, hence

$$\log x \leq \prod_{p \leq x} \frac{1}{1 - \frac{1}{p}} = \prod_{p \leq x} \frac{p}{p-1} = \prod_{k=1}^{\pi(x)} \frac{p_k}{p_k - 1}.$$

Now clearly $p_k \geq k + 1$, and thus

$$\frac{p_k}{p_k - 1} = 1 + \frac{1}{p_k - 1} \leq 1 + \frac{1}{k} = \frac{k+1}{k},$$

and therefore

$$\log x \leq \prod_{k=1}^{\pi(x)} \frac{k+1}{k} = \pi(x) + 1.$$

Everybody knows that $\log x$ is not bounded, so we conclude that $\pi(x)$ is unbounded as well, and so there are infinitely many primes. □

Theorem 1.5 (Fifth Proof)**.** *The set of primes $\mathbb{P}$ is infinite.*

Proof. Consider the following curious topology on the set $\mathbb{Z}$ of integers. For $a, b \in \mathbb{Z}, b > 0$, we set

$$N_{a,b} = \{a + nb : n \in \mathbb{Z}\}.$$

Each set $N_{a,b}$ is a two-way infinite arithmetic progression. Now call a set $O \subseteq \mathbb{Z}$ open if either O is empty, or if to every $a \in O$ there exists some $b > 0$ with $N_{a,b} \subseteq O$. Clearly, the union of open sets is open again. If O_1, O_2 are open, and $a \in O_1 \cap O_2$ with $N_{a,b_1} \subseteq O_1$ and $N_{a,b_2} \subseteq O_2$, then $a \in N_{a,b_1 b_2} \subseteq O_1 \cap O_2$. So we conclude that any finite intersection of open sets is again open. Therefore, this family of open sets induces a bona fide topology on $\mathbb{Z}$.

Let us note two facts:

(A) Any nonempty open set is infinite.

(B) Any set $N_{a,b}$ is closed as well.

Indeed, the first fact follows from the definition. For the second, we observe

$$N_{a,b} = \mathbb{Z} \quad \bigcup_{i=1}^{b-1} N_{a+i,b},$$

which proves that $N_{a,b}$ is the complement of an open set and hence closed.

So far, the primes have not yet entered the picture — but here they come. Since any number $n \neq 1, -1$ has a prime divisor p, and hence is contained in $N_{0,p}$, we conclude

$$\mathbb{Z} \quad \{1, -1\} = \bigcup_{p \in \mathbb{P}} N_{0,p}.$$

Now if $\mathbb{P}$ were finite, then $\bigcup_{p \in \mathbb{P}} N_{0,p}$ would be a finite union of closed sets (by (B)), and hence closed. Consequently, $\{1, -1\}$ would be an open set, in violation of (A). □

Theorem 1.6 (Sixth Proof)**.** *The series* $\sum_{p \in \mathbb{P}} \frac{1}{p}$ *diverges.*

Proof. Our final proof goes a considerable step further and demonstrates not only that there are infinitely many primes, but also that the series $\sum_{p \in \mathbb{P}} \frac{1}{p}$ diverges. The first proof of this important result was given by Euler (and is interesting in its own right), but our proof, devised by Erdős, is of compelling beauty.

Let $p_1, p_2, p_3, \dots$ be the sequence of primes in increasing order, and assume that $\sum_{p \in \mathbb{P}} \frac{1}{p}$ converges. Then there must be a natural number k such that $\sum_{i \geq k+1} \frac{1}{p_i} < \frac{1}{2}$. Let us call $p_1, \dots, p_k$ the small primes, and $p_{k+1}, p_{k+2}, \dots$ the big primes. For an arbitrary natural number N, we therefore find

$$\sum_{i \geq k+1} \frac{N}{p_i} < \frac{N}{2}. \tag{1}$$

Let N_b be the number of positive integers $n \leq N$ which are divisible by at least one big prime, and N_s the number of positive integers $n \leq N$ which have only small prime divisors. We are going to show that for a suitable N

$$N_b + N_s < N,$$

which will be our desired contradiction, since by definition $N_b + N_s$ would have to be equal to N.

To estimate N_b, note that $\left\lfloor \frac{N}{p_i} \right\rfloor$ counts the positive integers $n \leq N$ which are multiples of p_i. Hence by (1) we obtain

$$N_b \leq \sum_{i \geq k+1} \left\lfloor \frac{N}{p_i} \right\rfloor < \frac{N}{2}. \tag{2}$$

Let us now look at N_s. We write every $n \leq N$ which has only small prime divisors in the form $n = a_n b_n^2$, where a_n is the square-free part. Every a_n is thus a product of different small primes, and we conclude that there are precisely 2^k different square-free parts. Furthermore, as $b_n^2 \leq n \leq N$, we find that there are at most $\sqrt{N}$ different square parts, and so

$$N_s \leq 2^k \sqrt{N}.$$

Since (2) holds for any N, it remains to find a number N with $2^k \sqrt{N} < \frac{N}{2}$, or $2^{k+1} < \sqrt{N}$, and for this $N = 2^{2k+2}$ will do. □

1.1 Appendix: Infinitely many more proofs

Theorem 1.7. *If the sequence $S = (s_1, s_2, s_3, \dots)$ is almost injective and of subexponential growth, then the set $\mathbb{P}_S$ of primes that divide some member of S is infinite.*

Proof. □

Theorem 1.8 (Infinity of primes)**.** *There are infinitely many primes. (Six + infinitely many proofs)*

Proof. See theorems in this chapter. □

Chapter 2

Bertrand's postulate

Theorem 2.1. *For any positive natural number, there is a prime which is greater than it, but no more than twice as large.*

Proof. TODO: make this follow the book proof more closely! □

2.1 Appendix: Some estimates

Theorem 2.2. *For all $n \in \mathbb{N}$*

$$\log n + \frac{1}{n} < H_n < \log n + 1.$$

Proof. TODO □

Theorem 2.3. *For all $n \in \mathbb{N}$*

$$n! = n(n-1)! < ne^{n \log n - n + 1} = e\left(\frac{n}{e}\right)^n.$$

Proof. TODO □

Theorem 2.4.

$$\binom{n}{k} \leq \frac{n^k}{k!} \leq \frac{n^k}{2^{k-1}}$$

Proof. TODO □

Chapter 3

Binomial coefficients are (almost) never powers

Theorem 3.1 (Sylvester's theorem). *For all natural n, k such that $n \geq 2k$, at least one of the numbers $n, n-1, \dots, n-k-1$ has a prime divisor p greater than k, or, equivalently the binomial coefficient $\binom{n}{k}$ always has a prime factor $p > k$.*

Proof. TODO □

Theorem 3.2 (Binomial coefficients are (almost) never powers). *The equation $\binom{n}{k} = m^l$ has no integer solutions with $l \geq 2$ and $4 \leq k \leq n-4$.*

Proof. Note first that we may assume $n \geq 2k$ because of $\binom{n}{k} = \binom{n}{n-k}$. Suppose the theorem is false, and that $\binom{n}{k} = m^\ell$. The proof, by contradiction, proceeds in the following four steps.

1. By Sylvester's theorem 3.1, there is a prime factor p of $\binom{n}{k}$ greater than k, hence p^ℓ divides $n(n-1)\dots(n-k+1)$. Clearly, only one of the factors $n-i$ can be a multiple of p (because $p > k$), and we conclude $p^\ell \mid n-i$, and therefore
$$n \geq p^\ell > k^\ell \geq k^2.$$

2. Consider any factor $n-j$ of the numerator and write it in the form $n-j = a_j m_j^\ell$, where a_j is not divisible by any nontrivial ℓ-th power. We note by (1) that a_j has only prime divisors less than or equal to k. We want to show next that $a_i \neq a_j$ for $i \neq j$. Assume to the contrary that $a_i = a_j$ for some $i < j$. Then $m_i > m_j + 1$ and
$$\begin{aligned} k &> (n-i)-(n-j) = a_j(m_i^\ell - m_j^\ell) \geq a_j((m_j+1)^\ell - m_j^\ell) && (3.1)\\ &> a_j \ell m_j^{\ell-1} \geq \ell(a_j m_j^\ell)^{1/2} \geq \ell(n-k+1)^{1/2} && (3.2)\\ &\geq \ell\left(\frac{n}{2}\right)^{1/2} > n^{1/2}, && (3.3)\end{aligned}$$
which contradicts $n > k^2$ from above.

3. Next we prove that the a_i's are the integers $1, 2, \dots, k$ in some order. (According to Erdős, this is the crux of the proof.) Since we already know that they are all distinct, it suffices to prove that
$$a_0 a_1 \dots a_{k-1} \text{ divides } k!.$$

Substituting $n-j=a_j m_j^\ell$ into the equation $\binom{n}{k}=m^\ell$, we obtain

$$a_0 a_1 \dots a_{k-1}(m_0 m_1 \dots m_{k-1})^\ell = k! m^\ell.$$

Canceling the common factors of $m_0 \dots m_{k-1}$ and m yields

$$a_0 a_1 \dots a_{k-1} u^\ell = k! v^\ell$$

with $\gcd(u,v)=1$. It remains to show that $v=1$. If not, then v contains a prime divisor p. Since $\gcd(u,v)=1$, p must be a prime divisor of $a_0 a_1 \dots a_{k-1}$ and hence is less than or equal to k. By the theorem of Legendre (see page 8), we know that $k!$ contains p to the power $\sum_{i\geq 1}\left\lfloor \frac{k}{p^i}\right\rfloor$. We now estimate the exponent of p in $n(n-1)\dots(n-k+1)$. Let i be a positive integer, and let $b_1 < b_2 < \dots < b_s$ be the multiples of p^i among $n, n-1, \dots, n-k+1$. Then $b_s = b_1 + (s-1)p^i$ and hence

$$(s-1)p^i = b_s - b_1 \leq n-(n-k+1) = k-1,$$

which implies

$$s \leq \left\lfloor \frac{k-1}{p^i} \right\rfloor + 1 \leq \left\lfloor \frac{k}{p^i} \right\rfloor + 1.$$

So for each i, the number of multiples of p^i among $n, \dots, n-k+1$, and hence among the a_j's, is bounded by $\left\lfloor \frac{k}{p^i}\right\rfloor + 1$. This implies that the exponent of p in $a_0 a_1 \dots a_{k-1}$ is at most

$$\sum_{i=1}^{\ell-1}\left(\left\lfloor \frac{k}{p^i}\right\rfloor + 1\right)$$

with the reasoning that we used for Legendre's theorem in Chapter 2. The only difference is that this time the sum stops at $i=\ell-1$, since the a_j's contain no ℓ-th powers.

Taking both counts together, we find that the exponent of p in v^ℓ is at most

$$\sum_{i=1}^{\ell-1}\left(\left\lfloor \frac{k}{p^i}\right\rfloor + 1\right) - \sum_{i\geq 1}\left\lfloor \frac{k}{p^i}\right\rfloor \leq \ell - 1,$$

and we have our desired contradiction, since v^ℓ is an ℓ-th power.

This suffices already to settle the case $\ell = 2$. Indeed, since $k \geq 4$, one of the a_i's must be equal to 4, but the a_i's contain no squares. So let us now assume that $\ell \geq 3$.

4. Since $k \geq 4$, we must have $a_{i_1}=1$, $a_{i_2}=2$, $a_{i_3}=4$ for some i_1, i_2, i_3, that is,

$$n-i_1 = m_1^\ell, \quad n-i_2 = 2m_2^\ell, \quad n-i_3 = 4m_3^\ell.$$

We claim that $(n-i_2)^2 \neq (n-i_1)(n-i_3)$. If not, put $b=n-i_2$ and $n-i_1=b-x, n-i_3=b+y$, where $0<|x|,|y|<k$. Hence

$$b^2 = (b-x)(b+y) \quad \text{or} \quad (y-x)b = xy,$$

where $x=y$ is plainly impossible. Now we have by part (1)

$$|xy| = b|y-x| \geq b > n-k > (k-1)^2 \geq |xy|,$$

which is absurd.

So we have $m_2^2 \neq m_1 m_3$, where we assume $m_2 > m_1 m_3$ (the other case being analogous), and proceed to our last chain of inequalities. We obtain

$$\begin{aligned} 2(k-1)n > n^2 - (n-k+1)^2 &> (n-i_2)^2 - (n-i_1)(n-i_3) && (3.4)\\ = 4[m_2^\ell - (m_1 m_3)^\ell] &\geq 4[(m_1 m_3 + 1)^\ell - (m_1 m_3)^\ell] && (3.5)\\ \geq 4\ell m_1^{\ell-1} m_3^{\ell-1}. & && (3.6) \end{aligned}$$

Since $\ell \geq 3$ and $n \geq k^\ell \geq k^3 > 6k$, this yields

$$\begin{aligned} 2(k-1)n m_1 m_3 > 4\ell m_1^\ell m_3^\ell &= \ell(n-i_1)(n-i_3) && (3.7)\\ > \ell(n-k+1)^2 > 3(n-\frac{n}{6})^2 &> 2n^2. && (3.8) \end{aligned}$$

Now since $m_i \leq n^{1/\ell} \leq n^{1/3}$ we finally obtain

$$kn^{2/3} \geq k m_1 m_3 > (k-1) m_1 m_3 > n,$$

or $k^3 > n$. With this contradiction, the proof is complete.

□

Chapter 4

Representing numbers as sums of two squares

Lemma 4.1 (Lemma 1)**.** *For primes $p = 4m+1$ the equation $s^2 \equiv -1(\mod p)$ has two solutions $s \in \{1, 2, \dots, p-1\}$, for $p = 2$ there is one such solution, while for primes of the form $p = 4m+3$ there is no solution.*

Proof. For $p = 2$ take $s = 1$. For odd p, we construct the equivalence relation on $\{1, 2, \dots, p-1\}$ that is generated by identifying every element with its additive inverse and with its multiplicative inverse in $\mathbb{Z}_p$. Thus the "general" equivalence classes will contain four elements

$$\{x, -x, \overline{x}, -\overline{x}\}$$

since such a 4-element set contains both inverses for all its elements. However, there are smaller equivalence classes if some of the four numbers are not distinct:

- $x \equiv -x$ is impossible for odd p.
- $x \equiv \overline{x}$ is equivalent to $x^2 \equiv 1$. This has two solutions, namely $x = 1$ and $x = p-1$, leading to the equivalence class $\{1, p-1\}$ of size 2.
- $x \equiv -\overline{x}$ is equivalent to $x^2 \equiv -1$. This equation may have no solution or two distinct solutions $x_0, p - x_0$: in this case the equivalence class is $\{x_0, p - x_0\}$.

The set $\{1, 2, \dots, p-1\}$ has $p-1$ elements, and we have partitioned it into quadruples (equivalence classes of size 4), plus one or two pairs (equivalence classes of size 2). For $p - 1 = 4m+2$ we find that there is only the one pair $\{1, p-1\}$, the rest is quadruples, and thus $s^2 \equiv -1 \pmod p$ has no solution. For $p - 1 = 4m$ there has to be the second pair, and this contains the two solutions of $s^2 \equiv -1$ that we were looking for. □

Lemma 4.2 (Lemma 2)**.** *No number $n = 4m + 3$ is a sum of two squares.*

Proof. The square of any even number is $(2k)^2 = 4k^2 \equiv 0 \pmod 4$, while squares of odd numbers yield $(2k+1)^2 = 4(k^2+k)+1 \equiv 1 \pmod 4$. Thus any sum of two squares is congruent to 0, 1 or 2 $\pmod 4$. □ □

Proposition 4.3 (First proof)**.** *Every prime of the form $p = 4m+1$ is a sum of two squares, that is, it can be written as $p = x^2 + y^2$ for some natural numbers $x, y \in \mathbb{N}$.*

Proof. Consider the pairs (x', y') of integers with $0 \le x', y' \le \sqrt{p}$, that is, $x', y' \in \{0, 1, \dots, \lfloor\sqrt{p}\rfloor\}$. There are $(\lfloor\sqrt{p}\rfloor + 1)^2$ such pairs. Using the estimate $\lfloor x\rfloor + 1 > x$ for $x = \sqrt{p}$, we see that we have more than p such pairs of integers. Thus for any $s \in \mathbb{Z}$, it is impossible that all the values $x' - sy'$ produced by the pairs (x', y') are distinct modulo p. That is, for every s there are two distinct pairs

$$(x', y'), (x'', y'') \in \{0, 1, \dots, \lfloor\sqrt{p}\rfloor\}^2$$

with $x' - sy' \equiv x'' - sy'' \pmod{p}$. Now we take differences: We have $x' - x'' \equiv s(y' - y'') \pmod{p}$. Thus if we define $x := |x' - x''|$, $y := |y' - y''|$, then we get

$$(x, y) \in \{0, 1, \dots, \lfloor\sqrt{p}\rfloor\}^2 \quad \text{with} \quad x \equiv \pm sy \pmod{p}.$$

Also we know that not both x and y can be zero, because the pairs (x', y') and (x'', y'') are distinct.

Now let s be a solution of $s^2 \equiv -1 \pmod{p}$, which exists by Lemma 1. Then $x^2 \equiv s^2y^2 = -y^2 \pmod{p}$, and so we have produced

$$(x, y) \in \mathbb{Z}^2 \quad \text{with} \quad 0 < x^2 + y^2 < 2p \quad \text{and} \quad x^2 + y^2 \equiv 0 \pmod{p}.$$

But p is the only number between 0 and $2p$ that is divisible by p. Thus $x^2 + y^2 = p$: done! □

Proposition 4.4 (Second proof)**.** *Every prime of the form $p = 4m + 1$ is a sum of two squares, that is, it can be written as $p = x^2 + y^2$ for some natural numbers $x, y \in \mathbb{N}$.*

Proof. We study the set

$$S := \{(x, y, z) \in \mathbb{Z}^3 : 4xy + z^2 = p,\ x > 0,\ y > 0\}.$$

This set is finite. Indeed, $x \ge 1$ and $y \ge 1$ implies $y \le \frac{p}{4}$ and $x \le \frac{p}{4}$. So there are only finitely many possible values for x and y, and given x and y, there are at most two values for z.

1. The first linear involution is given by

   $$f : S \to S, \quad (x, y, z) \mapsto (y, x, -z),$$

   that is, "interchange x and y, and negate z." This clearly maps S to itself, and it is an *involution*: Applied twice, it yields the identity. Also, f has no fixed points, since $z = 0$ would imply $p = 4xy$, which is impossible. Furthermore, f maps the solutions in

   $$T := \{(x, y, z) \in S : z > 0\}$$

   to the solutions in $S\ \ T$, which satisfy $z < 0$. Also, f reverses the signs of $x - y$ and of z, so it maps the solutions in

   $$U := \{(x, y, z) \in S : (x - y) + z > 0\}$$

   to the solutions in $S\ \ U$. For this we have to see that there is no solution with $(x-y)+z = 0$, but there is none since this would give $p = 4xy + z^2 = 4xy + (x - y)^2 = (x + y)^2$.

   What do we get from the study of f? The main observation is that since f maps the sets T and U to their complements, it also interchanges the elements in $T\ \ U$ with these in $U\ \ T$. That is, there is the same number of solutions in U that are not in T as there are solutions in T that are not in U — so T and U have the same cardinality.

2. The second involution that we study is an involution on the set U:

$$g : U \to U, \quad (x, y, z) \mapsto (x - y + z, y, 2y - z).$$

First we check that indeed this is a well-defined map: If $(x, y, z) \in U$, then $x - y + z > 0$, $y > 0$ and $4(x-y+z)y+(2y-z)^2 = 4xy+z^2$, so $g(x, y, z) \in S$. By $(x-y+z)-y+(2y-z) = x > 0$ we find that indeed $g(x, y, z) \in U$.

Also g is an involution: $g(x, y, z) = (x - y + z, y, 2y - z)$ is mapped by g to $((x - y + z) - y + (2y - z), y, 2y - (2y - z)) = (x, y, z)$.

And finally g has exactly one fixed point:

$$(x, y, z) = g(x, y, z) = (x - y + z, y, 2y - z)$$

implies that $y = z$, but then $p = 4xy + y^2 = (4x + y)y$, which holds only for $y = z = 1$ and $x = \frac{p-1}{4}$.

But if g is an involution on U that has exactly one fixed point, then *the cardinality of U is odd.*

3. The third, trivial, involution that we study is the involution on T that interchanges x and y:

$$h : T \to T, \quad (x, y, z) \mapsto (y, x, z).$$

This map is clearly well-defined, and an involution. We combine now our knowledge derived from the other two involutions: The cardinality of T is equal to the cardinality of U, which is odd. But if h is an involution on a finite set of odd cardinality, then *it has a fixed point*: There is a point $(x, y, z) \in T$ with $x = y$, that is, a solution of

$$p = 4x^2 + z^2 = (2x)^2 + z^2.$$

□

Proposition 4.5 (Third proof). *Every prime of the form $p = 4m + 1$ is a sum of two squares, that is, it can be written as $p = x^2 + y^2$ for some natural numbers $x, y \in \mathbb{N}$.*

Proof. Again we fix a prime number $p = 4n + 1$ and consider the set of solutions

$$T = \{(x, y, z) \in \mathbb{N}^3 : 4xy + z^2 = p\}.$$

Each element of this set gives rise to a *winged square*: This is the figure consisting of a square and four rectangles in the plane that you get if you start with a square of side length z and at each vertex attach a rectangle of side-lengths x and y in a rotation-symmetric way, such that the edge of length x points away from the square, while the edge of length y runs along the side of the square.

We consider two winged squares “the same” if they are congruent. One way to make this unique, such that the representation of the winged square depends only on its boundary curve, is to require that the L formed by the two edges in the upper right-hand corner is at least as high as it is wide. If this condition is not satisfied, then a mirror image (reflected, e.g., in a vertical axis), will repair this. So each solution in T corresponds to a *unique* winged square of area $4xy + z^2 = p$, and indeed this is reversible: From each winged square we can read off a solution.

Taking the union of the square and the four rectangles, we get for each winged square what we will call a *unique winged shape*: This is a polyomino of area p with four-fold rotation symmetry, which has twelve vertices: eight convex ones with inner right angle and four non-convex ones with outer right angle. (We can't get a square shape, since p is a prime, so it can't be a square number.) Again we will consider winged shapes "the same" if they are congruent, so we might assume that the L shape in the upper right-hand corner is at least as high as it is wide.

Now we are getting very close to the punch line: For each winged shape we get *either one or two* winged squares, by simultaneously drawing, in a rotation-symmetric way, vertical and horizontal lines to the interior starting at the non-convex vertices. We get *only one* solution if the shape has the symmetry of a square, that is, if the two arms of the L shapes have the same length. This happens exactly if $y = z$, but then $p = 4xz + z^2 = (4x + z)z$; assuming that p is a prime, this implies that $z = 1$ and $x = n$. In other words: Exactly one winged shape yields a single winged square, while all other winged shapes yield two winged squares each. Consequently, *the number $|T|$ of winged squares is odd.*

However, the winged squares with non-square rectangles (with $x \neq y$) come in pairs, as we can always flip the four rectangular wings between vertical and horizontal format (that is, exchange x and y). As $|T|$ is odd, this implies that there is an odd number of winged squares whose wings are squares, that is, T contains an odd number of triples (x, y, z) with $x = y$, and hence at least one, and this yields a solution to $(2x)^2 + z^2 = p$. □

Theorem 4.6. *A natural number n can be represented as a sum of two squares if and only if every prime factor of the form $p = 4m + 3$ appears with an even exponent in the prime decomposition of n.*

Proof. TODO □

Chapter 5

The law of quadratic reciprocity

Theorem 5.1 (Fermat's little theorem). *For $a \not\equiv 0 \mod p$,*

$$a^{p-1} \equiv 1 \mod p$$

Proof. TODO □

Theorem 5.2 (Euler's criterion). *For $a \not\equiv 0(\mod p)$,*

$$(\frac{a}{p}) \equiv a^{\frac{p-1}{2}} \mod p$$

Proof. TODO □

Theorem 5.3 (Product Rule).

$$(\frac{ab}{p}) = (\frac{a}{p}) \cdot (\frac{b}{p})$$

Proof. TODO □

Theorem 5.4 (Lemma of Gauss). *TODO*

Proof. TODO □

Theorem 5.5 (Quadratic reciprocity I). *TODO*

Proof. TODO □

Theorem 5.6. *The multiplicative group of a finite field is cyclic*

Proof. TODO □

Theorem 5.7 (A). *TODO*

Proof. TODO □

Theorem 5.8 (B). *TODO*

Proof. TODO □

Theorem 5.9 (Quadratic reciprocity II). *TODO*

Proof. TODO □

Chapter 6

Every finite division ring is a field

Theorem 6.1 (Wedderburn's theorem)**.** *Every finite division ring is commutative*

Proof. TODO □

Chapter 7

The spectral theorem and Hadamard's determinant problem

Lemma 7.1. *If A is a real symmetric $n \times n$ matrix that is not diagonal, that is $\mathrm{Od}(A) > 0$, then there exists $U \in O(n)$ such that $\mathrm{Od}(U^T AU) < \mathrm{Od}(A)$.*

Proof. TODO □

Theorem 7.2. *For every real symmetric matrix A there is a real orthogonal matrix Q such that $Q^T AQ$ is diagonal.*

Proof. TODO □

Theorem 7.3. *There exists an $n \times n$ matrix with entries ± 1 whose determinant is greater than $\sqrt{n!}$.*

Proof. TODO □

Chapter 8

Some irrational numbers

Theorem 8.1. *e is irrational*

Proof. TODO □

Theorem 8.2. *e^2 is irrational*

Proof. TODO □

Theorem 8.3 (Little Lemma)**.** *TODO*

Proof. TODO □

Theorem 8.4. *e^4 is irrational*

Proof. TODO □

Lemma 8.5. *TODO*

Proof. TODO □

Lemma 8.6. *TODO*

Proof. TODO □

Lemma 8.7. *TODO*

Proof. TODO □

Theorem 8.8. *e^r is irrational for every $r \in \mathbb{Q} \quad \{0\}$.*

Proof. TODO □

Theorem 8.9. *π^2 is irrational.*

Proof. TODO □

Theorem 8.10. *For every odd integer $n \geq 3$, the number*

$$A(n) := \frac{1}{\pi} \arccos\left(\frac{1}{\sqrt{n}}\right)$$

is irrational.

Proof. TODO □

Chapter 9

Four times $\pi^2/6$

Theorem 9.1 (Euler's series: Proof 1)**.**

$$\sum_{n\geq 1} \frac{1}{n^2} = \frac{\pi^2}{6}$$

Proof. TODO □

Theorem 9.2 (Euler's series: Proof 2)**.**

$$\sum_{k\geq 0} \frac{1}{(2 * k + 1)^2} = \frac{\pi^2}{8}$$

Proof. TODO □

Theorem 9.3 (Euler's series: Proof 3)**.**

$$\sum_{n\geq 1} \frac{1}{n^2} = \frac{\pi^2}{6}$$

Proof. TODO □

Theorem 9.4 (Euler's series: Proof 4)**.**

$$\sum_{n\geq 1} \frac{1}{n^2} = \frac{\pi^2}{6}$$

Proof. TODO □

Theorem 9.5 (Four proofs of Euler's series)**.** *Collecting the proofs from the chapter*

Proof. □

Chapter 10

Hilbert's third problem: decomposing polyhedra

Lemma 10.1 (Pearl Lemma)**.** *If P and Q are equidecomposable, then one can place a positive number of pearls (that is, assign positive integers) to all the segments of the decompositions $P = P_1 \cup \cdots \cup P_n$ and $Q = Q_1 \cup \cdots \cup Q_n$ in such a way that each edge of a piece P_k receives the same number of pearls as the corresponding edge of Q_k.*

Proof. Assign a variable x_i to each segment in the decomposition of P and a variable y_j to each segment in the decomposition of Q. Now we have to find positive *integer* values for the variables x_i and y_j in such a way that the x_i-variables corresponding to the segments of any edge of some P_k yield the same sum as the y_j-variables assigned to the segments of the corresponding edge of Q_k. This yields conditions that require that "some x_i-variables have the same sum as some y_j-values", namely

$$\sum_{i:s_i\subseteq e} x_i - \sum_{j:s'_j\subseteq e'} y_j = 0$$

where the edge $e \subseteq P_k$ decomposes into the segments s_i, while the corresponding edge $e' \subseteq Q_k$ decomposes into the segments s'_j. This is a linear equation with integer coefficients.

We note, however, that positive *real* values satisfying all these requirements exist, namely the (real) lengths of the segments! Thus we are done, in view of the following lemma. □

Lemma 10.2 (Cone Lemma)**.** *If a system of homogeneous linear equations with integer coefficients has a positive* real *solution, then it also has a positive* integer *solution.*

Proof. The name of this lemma stems from the interpretation that the set

$$C = \{x \in \mathbb{R}^N : Ax = 0, x > 0\}$$

given by an integer matrix $A \in \mathbb{Z}^{M\times N}$ describes a (relatively open) rational cone. We have to show that if this is nonempty, then it also contains integer points: $C \cap \mathbb{N}^N \neq \emptyset$.

If C is nonempty, then so is $\overline{C} := \{x \in \mathbb{R}^N : Ax = 0, x \geq 1\}$, since for any positive vector a suitable multiple will have all coordinates equal to or larger than 1. (Here 1 denotes the vector with all coordinates equal to 1.) It suffices to verify that $\overline{C} \subseteq C$ contains a point with *rational* coordinates, since then multiplication with a common denominator for all coordinates will yield an integer point in $\overline{C} \subseteq C$.

There are many ways to prove this. We follow a well-trodden path that was first explored by Fourier and Motzkin [8, Lecture 1]: By "Fourier-Motzkin elimination" we show that the lexicographically smallest solution to the system

$$Ax = 0, x \geq 1$$

exists, and that it is rational if the matrix A is integral.

Indeed, any linear equation $a^T x = 0$ can be equivalently enforced by two inequalities $a^T x \geq 0, -a^T x \geq 0$. (Here a denotes a column vector and a^T its transpose.) Thus it suffices to prove that any system of the type

$$Ax \geq b, x \geq 1$$

with integral A and b has a lexicographically smallest solution, which is rational, provided that the system has any real solution at all.

For this we argue with induction on N. The case $N = 1$ is clear. For $N > 1$ look at all the inequalities that involve x_N. If $x' = (x_1, \dots, x_{N-1})$ is fixed, these inequalities give lower bounds on x_N (among them $x_N \geq 1$) and possibly also upper bounds. So we form a new system $A'x' \geq b$, $x' \geq 1$ in $N - 1$ variables, which contains all the inequalities from the system $Ax \geq b$ that do not involve x_N, as well as all the inequalities obtained by requiring that all upper bounds on x_N (if there are any) are larger or equal to all the lower bounds on x_N (which include $x_N \geq 1$). This system in $N - 1$ variables has a solution, and thus by induction it has a lexicographically minimal solution x'_*, which is rational. And then the smallest x_N compatible with this solution x'_* is easily found, it is determined by a linear equation or inequality with integer coefficients, and thus it is rational as well. □

Theorem 10.3 (Bricard's condition)**.** *TODO*

Proof. TODO □

Theorem 10.4 (Example 1)**.** *TODO*

Proof. TODO □

Theorem 10.5 (Example 2)**.** *TODO*

Proof. TODO □

Theorem 10.6 (Example 3)**.** *TODO*

Proof. TODO □

Theorem 10.7 (Hilbert's third problem)**.** *TODO*

Proof. □

Chapter 11

Lines in the plane and decompositions of graphs

Theorem 11.1. *In any configuration of n points in the plane, not all on a line, there is a line which contains exactly two of the points.*

Proof. TODO □

Theorem 11.2. *Let P be a set of $n \geq 3$ points in the plane, not all on a line. Then the set $\mathcal{L}$ of lines passing through at least two points contains at least n lines.*

Proof. TODO □

Theorem 11.3. *Let X be a set of $n \geq 3$ elements, and let $A_1, \ldots, A_m$ be proper subsets of X, such that every pair of elements of X is contained in precisely one set A_i. Then $m \geq n$ holds.*

Proof. TODO □

Theorem 11.4. *If K_n is decomposed into complete bipartite subgraphs $H_1, \ldots, H_m$, then $m \geq n - 1$.*

Proof. TODO □

Chapter 12

The slope problem

Theorem 12.1. *If $n \geq 3$ points in the plane do not lie on one single line, then they determine at least $n - 1$ different slopes, where equality is possible only if n is odd and $n \geq 5$.*

Proof.

1. TODO
2. TODO
3. TODO
4. TODO
5. TODO
6. TODO

□

Chapter 13

Three applications of Euler's formula

Theorem 13.1 (Euler's formula)**.** *If G is a connected plane graph with n vertices, e edges and f faces, then*

$$n - e + f = 2.$$

Proof. TODO □

Proposition 13.2. *Let G be any simple plane graph with $n > 2$ vertices. Then G has at most $3 * n - 6$ edges.*

Proof. TODO □

Proposition 13.3. *Let G be any simple plane graph with $n > 2$ vertices. Then G has a vertex of degree at most 5.*

Proof. TODO □

Proposition 13.4. *Let G be any simple plane graph with $n > 2$ vertices. If the edges of G are two-colored, then there is a vertex of G with at most two color-changes in the cyclic order of the edges around the vertex.*

Proof. TODO □

Theorem 13.5 (Sylvester-Gallai)**.** *Given any set of $n \geq 3$ points in the plane, not all on one line, there is always a line that contains exactly two of the points.*

Proof. TODO □

Theorem 13.6 (Monochromatic lines)**.** *Given any finite configuration of "black" and "white" points in the plane, not all on one line, there is always a "monochromatic" line: a line that contains at least two points of one color and none of the other.*

Proof. TODO □

Lemma 13.7. *Every elementary triangle $\Delta = \operatorname{conv}\{p_0, p_1, p_2\} \subset \mathbb{R}^2$ has area $A(\Delta) = 12$*

Proof. TODO □

Theorem 13.8 (Pick's theorem)**.** *The area of any (not necessarily convex) polygon $Q \subset \mathbb{R}^2$ with integral vertices is given by*

$$A(Q) = n_{int} + \frac{1}{2} n_{bd} - 1$$

where n_{int} and n_{bd} are the numbers of integral points in the interior respectively on the boundary of Q.

Proof. TODO □

Chapter 14

Cauchy's rigidity theorem

Lemma 14.1 (Cauchy's arm lemma)**.** *TODO*

Proof. TODO □

Theorem 14.2 (Cauchy's rigidity)**.** *If two* 3*-dimensional convex polyhedra P and P' are combinatorially equivalent with corresponding pairs of adjacent congruent, then also the angels between corresponding pairs of adjacent facets are equal (and thus P is congruent to P').*

Proof. TODO □

Chapter 15

The Borromean rings don't exist

Theorem 15.1. *If a link consists of disjoint perfect circles that are pairwise not linked, then the link is trivial*

Proof. TODO □

Theorem 15.2. *The Borromean rings are nontrivial, and they are also not equivalent to Tait's link No. 18*

Proof. TODO □

Theorem 15.3. *The Borromean rings cannot be build from three perfect circles*

Proof. TODO □

Chapter 16

Touching simplices

Theorem 16.1. *For every $d \geq 2$, there is a family of 2^d pairwise touching d-simplices in $\mathbb{R}^d$ together with a transversal line that hits the interior of every single on of them.*

Proof. TODO □

Theorem 16.2. *For all $d \geq 1$, we have $f(d) < 2^{d+1}$.*

Proof. TODO □

Chapter 17

Every large point set has an obtuse angle

Theorem 17.1. *For every d, one has the following chain of inequalities:*

$$2^d \leq_{(1)} \max\left\{\#S \mid S \subseteq \mathbb{R}^d, \angle(s_i, s_j, s_k) \leq \frac{\pi}{2} \text{ for every } \{s_i, s_j, s_k\} \subseteq S\right\} \tag{17.1}$$

$$\leq_{(2)} \max\{\#S \mid S \subseteq \mathbb{R}^d \text{ such that for any two points } \{s_i, s_j\} \subseteq S, \text{ there is a strip } S(i,j) \text{ that contains } S, \text{ with } s_i \text{ and } s_j \text{ lying in the parallel boundary hyperplanes of } S(i, \tag{17.2}$$

$$=_{(3)} \max\{\#S \mid S \subseteq \mathbb{R}^d \text{ such that the translates } P - s_i, s_i \in S, \text{ of the convex hull } P := conv(S) \text{ intersect in a common point, but they only touch}\} \tag{17.3}$$

$$\leq_{(4)} \max\{\#S \mid S \subseteq \mathbb{R}^d \text{ such that the translates } Q + s_i \text{ of some } d\text{-dimensional convex polytope } Q \subseteq \mathbb{R}^d \text{ touch pair} \tag{17.4}$$

$$=_{(5)} \max\{\#S \mid S \subseteq \mathbb{R}^d \text{ such that the translates } Q^* + s_i \text{ of some } d\text{-dimensional centrally symmetric convex polyto} \tag{17.5}$$

$$\leq_{(6)} 2^d. \tag{17.6}$$

Proof. TODO □

Theorem 17.2. *For every $d \geq 2$, there is a set $S \subset \{0,1\}^d$ of $2\lfloor \frac{sqrt6}{9}(\frac{2}{\sqrt(3)})^d \rfloor$ points in $\mathbb{R}^n$ (vertices of the unit d-cube) that determine only acute angels. In particular, in dimension $d = 34$ there is a set of $72 > 2 * 34 - 1$ points with only acute angels.*

Proof. TODO □

Chapter 18

Borsuk's conjecture

Theorem 18.1 (Borsuk's conjecture)**.** *Let $q = p^m$ be a prime power, $n := 4q - 2$, and $d := \binom{n}{2} = (2q-1)(4q-3)$. Then there is a set $S \subseteq \{+1, -1\}^d$ of 2^{n-2} points in $\mathbb{R}^d$ such that every partition of S, whose parts have smaller diameter than S, has at least*

$$\frac{2^{n-2}}{\sum_{i=0}^{q-2} \binom{n-1}{i}}$$

parts. For $q = 9$ this implies that the Borsuk conjecture is false in dimension $d = 561$. Furthermore, $f(d) > (1.2)^{\sqrt{d}}$ holds for all large enough d.

Proof. TODO □

Chapter 19

Sets, functions, and the continuum hypothesis

Theorem 19.1. *The set of $\mathbb{Q}$ of rational numbers is countable.*

Proof. TODO □

Theorem 19.2. *The set $\mathbb{R}$ of real numbers is* not *countable*

Proof. TODO □

Theorem 19.3. *The set $\mathbb{R}^2$ of all ordered pairs of real numbers (that is, the real plane) has the same size as $\mathbb{R}$.*

Proof. TODO □

Theorem 19.4. *If each of two sets M and N can be mapped injectively into the other, then there is a bijection from M to N, that is $|M| = |N|$.*

Proof. TODO □

Theorem 19.5. *If $c > \aleph_1$, then every family $\{f_\alpha\}$ satisfying (P_0) is countable. If, on the other hand, $c = \aleph_1$, then there exists some family $\{f_\alpha\}$ with property P_0 which has size c.*

Proof. TODO □

Appendix: On cardinal and ordinal numbers

Proposition 19.6. *Let μ be an ordinal number and denote by W_μ the set of ordinal numbers smaller than μ. Then the following holds:*

1. *The elements of W_μ are pairwise comparable.*
2. *If we order W_μ according to their magnitude, then W_μ is well-ordered and has ordinal number μ.*

Proof. TODO □

Proposition 19.7. *Any two ordinal numbers μ and ν satisfy precisely one of the relations $\mu < \nu$, $\mu = \nu$, or $\mu > \nu$.*

Proof. TODO □

Proposition 19.8. *Every set of ordinal numbers (ordered according to magnitude) is well-ordered.*

Proof. TODO □

Proposition 19.9. *For every cardinal number $\mathfrak{m}$, there is a definite next larger cardinal number.*

Proof. TODO □

Proposition 19.10. *Let the infinite set M have cardinality $\mathfrak{m}$, and let M be well ordered according to the initial ordinal number $\omega_{\mathfrak{m}}$. Then M has no last element.*

Proof. Indeed, if M had a last element m, then the segment M_m would have an ordinal number $\mu < \omega_{\mathfrak{m}}$ with $|\mu| = \mathfrak{m}$, contradicting the definition of $\omega_{\mathfrak{m}}$. □

Proposition 19.11. *Suppose $\{A_\alpha\}$ is a family of size $\mathfrak{m}$ of countable sets A_α, where $\mathfrak{m}$ is an infinite cardinal. Then the union $\bigcup_\alpha A_\alpha$ has size at most $\mathfrak{m}$.*

Proof. TODO □

Chapter 20

In praise of inequalities

Theorem 20.1. *Let $\langle a, b\rangle$ be an inner product on a real vector space V (with the norm $|a|^2 := \langle a, a\rangle$). Then*

$$\langle a, b\rangle^2 \leq |a|^2|b|^2$$

holds for all vectors $a, b \in V$, with equality if and only if a and b are linearly dependent.

Proof. The following (folklore) proof is probably the shortest. Consider the quadratic function

$$|xa + b|^2 = x^2|a|^2 + 2x\langle a, b\rangle + |b|^2$$

in the variable x. We may assume $a \neq 0$. If $b = \lambda a$, then clearly

$$\langle a, b\rangle^2 = |a|^2|b|^2.$$

If, on the other hand, a and b are linearly independent, then $|xa + b|^2 > 0$ for all x, and thus the discriminant $\langle a, b\rangle^2 - |a|^2|b|^2$ is less than 0. □

Theorem 20.2 (First proof)**.** *Let $a_1, \dots a_n$ be positive real numbers, then*

$$\frac{n}{\frac{1}{a_1} + \dots + \frac{1}{n_n}} \leq \sqrt[n]{a_1 a_2 \dots a_n} \leq \frac{a_1 \dots a_n}{n}$$

with equality in both cases if and only if all a_i's are equal.

Proof. TODO □

Theorem 20.3 (Another Proof)**.** *Let $a_1, \dots a_n$ be positive real numbers, then*

$$\frac{n}{\frac{1}{a_1} + \dots + \frac{1}{n_n}} \leq \sqrt[n]{a_1 a_2 \dots a_n} \leq \frac{a_1 \dots a_n}{n}$$

with equality in both cases if and only if all a_i's are equal.

Proof. TODO □

Theorem 20.4 (Still another Proof)**.** *Let $a_1, \dots a_n$ be positive real numbers, then*

$$\frac{n}{\frac{1}{a_1} + \dots + \frac{1}{n_n}} \leq \sqrt[n]{a_1 a_2 \dots a_n} \leq \frac{a_1 \dots a_n}{n}$$

with equality in both cases if and only if all a_i's are equal.

Proof. TODO □

Theorem 20.5. *Suppose all roots fo the polynomial $x^n + a_{n-1}x^{n-1} + \dots + a_0$ are real. Then the roots of are contained in the interval with the endpoints*

$$-\frac{n_{n-1}}{n} \pm \frac{n-1}{n}\sqrt{a_{n-1}^n - \frac{2n}{n-1}a_{n-2}}.$$

Proof. TODO □

Theorem 20.6. *Let $f(x)$ be a real polynomial of degree $n \geq 2$ with only real roots, such that $f(x) > 0$ for $-1 < x < 1$ amd $f(-1) = f(1) = 0$. Then*

$$\frac{2}{3}T \leq A \leq \frac{2}{3}R,$$

and equality holds in both cases only for $n = 2$.

Proof. TODO □

Theorem 20.7. *Suppose G is a graph on n vertices without triangles. Then G has at most $\frac{n^2}{4}$ edges, and equality holds only when n is even and G is the complete bipartite graph $K_{n/2,n/2}$.*

Proof. This proof, using Cauchy's inequality, is due to Mantel. Let $V = \{1, \dots, n\}$ be the vertex set and E the edge set of G. By d_i we denote the degree of i, hence $\sum_{i \in V} d_i = 2|E|$ (see chapter 28). Suppose ij is an edge. Since G has no triangles, we find $d_i + d_j \leq n$ since no vertex is a neighbor of both i and j.

It follows that

$$\sum_{ij \in E} (d_i + d_j) \leq n|E|.$$

Note that d_i appears exactly d_i times in the sum, so we get

$$n|E| \geq \sum_{ij \in E} (d_i + d_j) = \sum_{i \in V} d_i^2,$$

and hence with Cauchy's inequality applied to the vectors $(d_1, \dots, d_n)$ and $(1, \dots, 1)$,

$$n|E| \geq \sum_{i \in V} d_i^2 \geq \frac{\left(\sum d_i\right)^2}{n} = \frac{4|E|^2}{n},$$

and the result follows. In the case of equality we find $d_i = d_j$ for all i, j, and further $d_i = \frac{n}{2}$ (since $d_i + d_j = n$). Since G is triangle-free, $G = K_{n/2,n/2}$ is immediately seen from this.

□

Theorem 20.8. *Suppose G is a graph on n vertices without triangles. Then G has at most $\frac{n^2}{4}$ edges, and equality holds only when n is even and G is the complete bipartite graph $K_{n/2,n/2}$.*

Proof. TODO □

Chapter 21

The fundamental theorem of algebra

Lemma 21.1. *Let $p(z) = \sum_{k=0}^{n} c_k z^k$ be a complex polynomial of degree $n \geq 1$. If $p(a) \neq 0$, then every disk D around a contains an interior point b with $|p(b)| < |p(a)|$*

Proof. TODO □

Theorem 21.2. *Every nonconstant polynomial with complex coefficients has at least one root in the field of complex numbers.*

Proof. The rest is easy. Clearly, $p(z)z^{-n}$ approaches the leading coefficient c_n of $p(z)$ as $|z|$ goes to infinity. Hence $|p(z)|$ goes to infinity as well with $|z| \to \infty$. Consequently, there exists $R_1 > 0$ such that $|p(z)| > |p(0)|$ for all points z on the circle $\{z : |z| = R_1\}$. Furthermore, our third fact (C) tells us that in the compact set $D_1 = \{z : |z| \leq R_1\}$ the continuous real-valued function $|p(z)|$ attains the minimum value at some point z_0. Because of $|p(z)| > |p(0)|$ for z on the boundary of D_1, z_0 must lie in the interior. But by d'Alembert's lemma 21.1 this minimum value $|p(z_0)|$ must be 0 — and this is the whole proof. □

Chapter 22

One square and an odd number of triangles

Definition 22.1 (valutaion on $\mathbb{R}$)**.**

Definition 22.2 (Three-coloring of plane)**.** TODO

Definition 22.3 (Rainbow triangle)**.** TODO

Lemma 22.4. *For any blue point $p_0 = (x_b, y_b)$, green point (x_g, y_g), and red point (x_r, y_r), the v-value of the determinant*

$$\det \begin{bmatrix} x_b & y_b & 1 \\ x_g & y_g & 1 \\ x_r & y_r & 1 \end{bmatrix}$$

is at least 1*.*

Proof. TODO □

Corollary 22.5. *Any line of the plane receives at most two different colors. The area of a rainbow triangle cannot be* 0*, and it cannot be $\frac{1}{n}$ for odd n.*

Proof. Follow from 22.4 □

Lemma 22.6. *Every dissection of the unit square $S = [0,1]^2$ into finitely many triangles contains an odd number of rainbow triangles, and thus at least one.*

Proof. TODO □

Theorem 22.7 (Monsky's theorem)**.** *It is not possible to dissect a square into an odd number of triangles of equal algebra area.*

Proof. TODO □

Appendix: Extending valuations

Lemma 22.8. *A proper subring $R \subset K$ is a valuation ring with respect to some valuation v into some ordered group G if and only if $K = R \cup R^{-1}$.*

Proof. TODO □

Theorem 22.9. *The field of real numbers $\mathbb{R}$ has a non-Archimedean valuation to an ordered abelian group*

$$v : \mathbb{R} \to \{0\} \cup G$$

such that $v(\frac{1}{2}) > 1$.

Proof. TODO □

Chapter 23

A theorem of Pólya on polynomials

Theorem 23.1. *Let $f(z)$ be a complex polynomial of degree at least 1 and leading coefficient 1. Set $C = \{z \in \mathbb{C} : |f(z)| \leq 2\}$ and let $\mathcal{R}$ be the orthogonal projection of C onto the real axis. Then there are intervals $I_1, \ldots, I_t$ on the real line which together cover $\mathcal{R}$ and satisfy*

$$\ell(I_1) + \cdots + \ell(I_t) \leq 4.$$

Proof. □

Theorem 23.2. *Let $p(x)$ be a real polynomial of degree $n \geq 1$ with leading coefficient 1, and all roots real. Then the set $\mathcal{P} = \{x \in \mathbb{R} : |p(x)| \leq 2\}$ can be covered by intervals of total length at most 4.*

Proof. □

Corollary 23.3. *Let $p(x)$ be a real polynomial of degree $n \geq 1$ with leading coefficient 1, and suppose that $|p(x)| \leq 2$ for all x in the interval $[a, b]$. Then $b - a \leq 4$.*

Proof. TODO □

23.1 Appendix: Chebyshev's theorem

Theorem 23.4 (Chebyshev's theorem)**.** *Let $p(x)$ be a real polynomial of degree $n \geq 1$ with leading coefficient 1. Then*

$$\max_{-1 \leq x \leq 1} |p(x)| \geq \frac{1}{2^{n-1}}.$$

Proof. TODO □

Theorem 23.5 (Fact 1)**.** *If b is a multiple root of $p'(x)$, then b is also a root of $p(x)$.*

Proof. Let $b_1 < \cdots < b_r$ be the roots of $p(x)$ with multiplicities $s_1, \ldots, s_r$, $\sum_{j=1}^{r} s_j = n$. From $p(x) = (x - b_j)^{s_j} h(x)$ we infer that b_j is a root of $p'(x)$ if $s_j \geq 2$, and the multiplicity of b_j in $p'(x)$ is $s_j - 1$. Furthermore, there is a root of $p'(x)$ between b_1 and b_2, another root between b_2 and $b_3, \ldots$, and one between b_{r-1} and b_r, and all these roots must be single roots, since $\sum_{j=1}^{r}(s_j - 1) + (r - 1)$ counts already up to the degree $n - 1$ of $p'(x)$. Consequently, the multiple roots of $p'(x)$ can only occur among the roots of $p(x)$. □

Theorem 23.6 (Fact 2)**.** *We have $p'(x)^2 \geq p(x)p''(x)$ for all $x \in \mathbb{R}$.*

Proof. If $x = a_i$ is a root of $p(x)$, then there is nothing to show. Assume then x is not a root. The product rule of differentiation yields

$$p'(x) = \sum_{k=1}^{n} \frac{p(x)}{x - a_k}, \quad \text{that is,} \quad \frac{p'(x)}{p(x)} = \sum_{k=1}^{n} \frac{1}{x - a_k}.$$

Differentiating this again we have

$$\frac{p''(x)p(x) - p'(x)^2}{p(x)^2} = -\sum_{k=1}^{n} \frac{1}{(x - a_k)^2} < 0.$$

□

Chapter 24

Van der Waerden's permanent conjecture

Theorem 24.1. *Let $M = (m_{ij})$ be a doubly stochastic $n \times n$ matrix. Then*

$$\operatorname{per} M \geq \frac{n!}{n^n}$$

and equality holds if and only if $m_{ij} = \frac{1}{n}$

Proof. TODO □

Proposition 24.2 (Gurvit's proposition)**.** *If $p(x) \in \mathbb{R}_+[x_1, \dots, x_n]$ is a H-stable and homogeneous of degree n, then either $p' \cong 0$, or p' is H-stable and homogeneous of degree $n-1$. In either case*

$$\operatorname{cap}(p') \geq \operatorname{cap} \cdot g(\deg_n p).$$

Proof. TODO □

Chapter 25

On a lemma of Littlewood and Offord

Theorem 25.1. *Let $a_1, \dots, a_n$ be vectors in $\mathbb{R}^d$, each of length at least 1, and let $R_1, \dots, R_k$ be k open regions of $\mathbb{R}^d$, where $|x - y| < 2$ for any x, y that lie in the same region R_i. Then the number of linear combinations $\sum_{i=1}^{n} \epsilon_i a_i$, $\epsilon_i \in \{1, -1\}$, that can lie in the union $\bigcup_i R_i$ of the regions is at most the sum of the k largest binomial coefficients $\binom{n}{j}$.*

In particular, we get the bound $\binom{\lfloor n/2 \rfloor}{n}$ for $k = 1$.

Proof. TODO □

Chapter 26

Cotangent and the Herglotz trick

Lemma 26.1 (A)**.** *The functions f and g are defined for all non-integral values and are continuous there.*

Proof. TODO □

Lemma 26.2 (B)**.** *Both f and g are* periodic *of period 1, that is $f(x+1) = f(x)$ and $g(x+1) = g(x)$ hold for all $x \in \mathbb{R}\ \ \mathbb{Z}$.*

Proof. TODO □

Lemma 26.3 (C)**.** *Both f and g are* odd *functions, that is we have $f(-x) = -f(x)$ and $g(-x) = -g(x)$ for all $x \in \mathbb{R}\ \ \mathbb{Z}$.*

Proof. TODO □

Lemma 26.4 (D)**.** *The two functions f and g satisfy the same functional equation: $f(\frac{x}{2}) + f(\frac{x+1}{2}) = 2f(x)$ and $g(\frac{x}{2}) + g(\frac{x+1}{2}) = gf(x)$.*

Proof. TODO □

Lemma 26.5 (E)**.** *By setting $h(x) := 0$ for $x \in \mathbb{Z}$, h becomes a continuous function on all of $\mathbb{R}$ that shares the properties given in 26.2, 26.3, 26.4.*

Proof. TODO □

Theorem 26.6.

$$\pi \cot \pi x = \frac{1}{x} + \sum_{n=1}^{\infty} \left(\frac{1}{x+n} + \frac{1}{x-n} \right)$$

for $x \in \mathbb{R}\ \ \mathbb{Z}$.

Proof. □

Chapter 27

Buffon's needle problem

Theorem 27.1 (Buffon's needle problem)**.** *If a short needle, of length ℓ, is dropped on paper that is ruled with equally spaced lines of distance $d \geq \ell$, then the probability that the needle comes to lie in a position where it crosses one of the lines is exactly*

$$p = \frac{2\ell}{\pi d}.$$

Proof. TODO □

Chapter 28

Pigeon-hole and double counting

Theorem 28.1 (Pigeon-hole princinple)**.** *If n objects are placed in r boxes, where $r < n$, then at least one of the boxes contains more than one object.*

Proof. obvious □

Theorem 28.2 (Double counting)**.** *Suppose that we are given two finite sets R and C and a subset $S \subseteq R \times C$. Whenever $(p, q) \in S$, then we say p and q are incident. If r_p denotes the number of elements that are incident to $p \in R$, and c_q denotes the number of elements that are incident to $q \in C$, then*

$$\sum_{p \in R} r_p = |S| = \sum_{q \in C} c_q. \tag{3}$$

Proof. "nothing to prove" □

28.1 Numbers

Theorem 28.3 (Claim)**.** *Consider the numbers $1, 2, 3, \ldots 2n$, and take away $n+1$ of them. Then there are two among these $n+1$ numbers which are relatively prime.*

Proof. obvious □

Theorem 28.4 (Claim)**.** *Suppose again $A \subset \{1, 2, \ldots, 2n\}$ with $|A| = n + 1$. Then there are always two numbers in A such that one divides the other.*

Proof. Write every number $a \in A$ in the form $a = 2^k m$, where m is an odd number between 1 and $2n - 1$. Since there are $n + 1$ numbers in A, but only n different odd parts, there must be two numbers in A with the same odd part. Hence one is a multiple of the other. □

28.2 Sequences

Theorem 28.5 (Claim)**.** *In any sequence $a_1, a_2, \ldots, a_{mn+1}$ of $mn+1$ distinct real numbers, there exists an increasing subsequence*

$$a_{i_1} < a_{i_2} < \cdots < a_{i_{m+1}} \quad (i_1 < i_2 < \cdots < i_{m+1})$$

of length $m + 1$, or a decreasing subsequence

$$a_{j_1} > a_{j_2} > \dots > a_{j_{n+1}} \quad (j_1 < j_2 < \dots < j_{n+1})$$

of length $n + 1$, or both.

Proof. This time the application of the pigeon-hole principle is not immediate. Associate to each a_i the number t_i, which is the length of a longest increasing subsequence starting at a_i. If $t_i \geq m + 1$ for some i, then we have an increasing subsequence of length $m + 1$. Suppose then that $t_i \leq m$ for all i. The function $f : a_i \mapsto t_i$ mapping $\{a_1, \dots, a_{mn+1}\}$ to $\{1, \dots, m\}$ tells us by (1) that there is some $s \in \{1, \dots, m\}$ such that $f(a_i) = s$ for $\frac{mn}{m} + 1 = n + 1$ numbers a_i. Let $a_{j_1}, a_{j_2}, \dots, a_{j_{n+1}}$ $(j_1 < \dots < j_{n+1})$ be these numbers. Now look at two consecutive numbers $a_{j_i} < a_{j_{i+1}}$, then we would obtain an increasing subsequence of length s starting at $a_{j_{i+1}}$, and consequently an increasing subsequence of length $s + 1$ starting at a_{j_i}, which cannot be since $f(a_{j_i}) = s$. We thus obtain a decreasing subsequence $a_{j_1} > a_{j_2} > \dots > a_{j_{n+1}}$ of length $n + 1$. □

28.3 Sums

Theorem 28.6 (Claim)**.** *Suppose we are given n integers $a_1, \dots, a_n$, which need not be distinct. Then there is always a set of consecutive numbers $a_{k+1}, a_{k+2}, \dots, a_\ell$ whose sum $\sum_{i=k+1}^{\ell} a_i$ is a multiple of n.*

Proof. For the proof we set $N = \{0, 1, \dots, n\}$ and $R = \{0, 1, \dots, n-1\}$. Consider the map $f : N \to R$, where $f(m)$ is the remainder of $a_1 + \dots + a_m$ upon division by n. Since $|N| = n + 1 > n = |R|$, it follows that there are two sums $a_1 + \dots + a_k, a_1 + \dots + a_\ell$ $(k < \ell)$ with the same remainder, where the first sum may be the empty sum denoted by 0. It follows that

$$\sum_{i=k+1}^{\ell} a_i = \sum_{i=1}^{\ell} a_i - \sum_{i=1}^{k} a_i$$

has remainder 0 — end of proof. □

28.4 Numbers again

TODO

28.5 Graphs

Lemma 28.7 (Handshaking)**.** *Let G be a finite simple graph with vertex set V and edge set E and let $d(v)$ denote the degree of a vertex v. Then*

$$\sum_{v \in V} d(v) = 2|E|.$$

Proof. For the proof consider $S \subseteq V \times E$, where S is the set of pairs (v, e) such that $v \in V$ is an end-vertex of $e \in E$. Counting S in two ways gives on the one hand $\sum_{v \in V} d(v)$, since every vertex contributes $d(v)$ to the count, and on the other hand $2|E|$, since every edge has two ends. □

Theorem 28.8. *If the graph G on n vertices contains no 4-cycles, then*

$$|E| \leq \lfloor \frac{n}{4}(1 + \sqrt{4n - 3}) \rfloor$$

Proof. TODO □

28.6 Sperner's Lemma

Lemma 28.9 (Sperner's Lemma)**.** *Suppose that some "big" triangle with vertices V_1, V_2, V_3 is triangulated (that is, decomposed into a finite number of "small" triangles that fit together edge-by-edge). Assume that the vertices in the triangulation get "colors" from the set $\{1, 2, 3\}$ such that V_i receives the color i (for each i), and only the colors i and j are used for vertices along the edge from V_i to V_j (for $i \neq j$), while the interior vertices are colored arbitrarily with 1, 2, or 3. Then in the triangulation there must be a small "tricolored" triangle, which has all three different vertex colors.*

Proof. We will prove a stronger statement: The number of tricolored triangles is not only nonzero, it is always *odd*.

Consider the dual graph to the triangulation, but don't take all its edges — only those which cross an edge that has endvertices with the (different) colors 1 and 2. Thus we get a "partial dual graph" which has degree 1 at all vertices that correspond to tricolored triangles, degree 2 for all triangles in which the two colors 1 and 2 appear, and degree 0 for triangles that do not have both colors 1 and 2. Thus only the tricolored triangles correspond to vertices of odd degree (of degree 1).

However, the vertex of the dual graph which corresponds to the outside of the triangulation has odd degree: in fact, along the big edge from V_1 to V_2, there is an odd number of changes between 1 and 2. Thus an odd number of edges of the partial dual graph crosses this big edge, while the other big edges cannot have both 1 and 2 occurring as colors.

Now since the number of odd-degree vertices in any finite graph is even (by equation (4)), we find that the number of small triangles with three different colors (corresponding to odd inside vertices of our dual graph) is odd. □

Theorem 28.10 (Brower's Fixpoint (for $n = 2$))**.** *Every continuous function $f : B^2 \longrightarrow B^2$ of an 2-dimensional ball to itself has a fixed point (a point $x \in B^2$ with $f(x) = x$).*

Proof. TODO □

Chapter 29

Tiling rectangles

Theorem 29.1 (First proof)**.** *Whenever a rectangle is tiled by rectangles all of which have at least one side of integer length, then the tiled rectangle has at least one side of integer length.*

Proof. TODO □

Theorem 29.2 (Second proof)**.** *Whenever a rectangle is tiled by rectangles all of which have at least one side of integer length, then the tiled rectangle has at least one side of integer length.*

Proof. TODO □

Theorem 29.3 (Third proof)**.** *Whenever a rectangle is tiled by rectangles all of which have at least one side of integer length, then the tiled rectangle has at least one side of integer length.*

Proof. TODO □

Chapter 30

Three famous theorems on finite sets

Theorem 30.1. *The size of a largest antichain of an n-set is* $\binom{n}{\lfloor n/2 \rfloor}$.

Proof. TODO □

Lemma 30.2. *Let* $n \geq 2k$*, and suppose we are given* t *distinct arcs* $A_1, \dots A_t$ *of length* k*, such that any two arcs have an edge in common. Then* $t \leq k$.

Proof. TODO □

Theorem 30.3. *The largest size of an intersection k-family in an n-set is* $\binom{n-1}{k-1}$.

Proof. TODO □

Theorem 30.4 (Marriage theorem)**.** *Let* $A_1, \dots A_n$ *be a collection of subset of a finite set* X*. Then there exists a system of distinct representatives if and only if the union of any* m *sets* A_i *contains at least* m *elements, for* $1 \leq m \leq n$.

Proof. TODO □

Chapter 31

Shuffling cards

Lemma 31.1. *Let $\mathbb{Q} : \mathfrak{S}_n \longrightarrow \mathbb{R}$ be any probability distribution that defines a shuffling process $\mathbb{Q}^*k$ with a strong uniform stopping rule whose stopping time is T. Then for all $k \geq 0$,*

$$||\mathbb{Q}^*k - \mathbb{U}|| \leq \mathit{Prob}[T > k].$$

Proof. If X is a random variable with values in $\mathfrak{S}_n$, with probability distribution $\mathbb{Q}$, then we write $\mathbb{Q}(S)$ for the probability that X takes a value in $S \subseteq \mathfrak{S}_n$. Thus $\mathbb{Q}(S) = \text{Prob}[X \in S]$, and in the case of the uniform distribution $\mathbb{Q} = \mathbb{U}$ we get

$$\mathbb{U}(S) = \text{Prob}[X \in S] = \frac{|S|}{n!}.$$

For every subset $S \subseteq \mathfrak{S}_n$, we get the probability that after k steps our deck is ordered according to a permutation in S as

$$\begin{aligned}
\mathbb{Q}^*k(S) = \text{Prob}[X_k \in S] &= \sum_{j \leq k} \text{Prob}[X_k \in S \wedge T = j] + \text{Prob}[X_k \in S \wedge T > k] \\
&= \sum_{j \leq k} \mathbb{U}(S) \cdot \text{Prob}[T = j] + \text{Prob}[X_k \in S | T > k] \cdot \text{Prob}[T > k] \\
&= \mathbb{U}(S)(1 - \text{Prob}[T > k]) + \text{Prob}[X_k \in S | T > k] \cdot \text{Prob}[T > k] \\
&= \mathbb{U}(S) + (\text{Prob}[X_k \in S | T > k] - \mathbb{U}(S)) \cdot \text{Prob}[T > k].
\end{aligned}$$

This yields

$$|\mathbb{Q}^*k(S) - \mathbb{U}(S)| \leq \text{Prob}[T > k]$$

since

$$\text{Prob}[X_k \in S | T > k] - \mathbb{U}(S)$$

is a difference of two probabilities, so it has absolute value at most 1. □

Theorem 31.2. *Let $c \geq 0$ and $k := \lceil n \log n + cn \rceil$. Then after performing k top-in-at-random shuffles on a deck of n cards, the variation distance from the uniform distribution satisfies*

$$d(k) := ||\mathit{Top}^*k - \mathbb{U}|| \leq e^{-c}.$$

Proof. TODO □

Theorem 31.3. *After performing k riffle shuffles on a deck of n cards, the variation distance from a uniform distribution satisfies*

$$||Rif^{*}k - \mathbb{U}|| \leq 1 - \prod_{i=1}^{n-1} \left(1 - \frac{i}{2^k}\right).$$

Proof. TODO □

Chapter 32

Lattice paths and determinants

Lemma 32.1. *Let $G = (V, E)$ be a finite weighted acyclic directed graph, $A = \{A_1, \dots, A_n\}$ and $\mathcal{B} = \{B_1, \dots, B_n\}$ two n-sets of vertices, and M the path matrix from A to $\mathcal{B}$. Then*

$$\det M = \sum_{\mathcal{P} \textit{ vertex-disjoint path system}} \textit{sign}(\mathcal{P})\, w(\mathcal{P}). \tag{3}$$

Proof. TODO □

Theorem 32.2. *Let $G = (V, E)$ be a finite weighted acyclic directed graph, $A = \{A_1, \dots, A_n\}$ and $\mathcal{B} = \{B_1, \dots, B_n\}$ two n-sets of vertices, and M the path matrix from A to $\mathcal{B}$. Then*

$$\det M = \sum_{\mathcal{P} \textit{ vertex-disjoint path system}} \textit{sign}(\mathcal{P})\, w(\mathcal{P}). \tag{3}$$

Proof. TODO □

Chapter 33

Cayley's formula for the number of trees

Theorem 33.1 (First proof (bijection))**.** *There are n^{n-2} different labeled trees on n nodes.*

Proof. TODO □

Theorem 33.2 (Second proof (Linear Algebra))**.** *There are n^{n-2} different labeled trees on n nodes.*

Proof. TODO □

Theorem 33.3 (Second proof (Recursion))**.** *There are n^{n-2} different labeled trees on n nodes.*

Proof. TODO □

Theorem 33.4 (Second proof (Double Counting))**.** *There are n^{n-2} different labeled trees on n nodes.*

Proof. TODO □

Chapter 34

Identities versus bijections

Theorem 34.1.

$$\prod_{k\geq 1}(1-x^k) = 1+\sum_{j\geq 1}(-1)^j(x^{\frac{3j^2-j}{2}} + x^{3j^2+j}2).$$

Proof. TODO □

Chapter 35

The finite Kakeya problem

Let F be a finite field.

Lemma 35.1. *Every nonzero polynomial $p(x) \in F[x_1, \dots, x_n]$ of degree d has at most dq^{n-1} roots in F^n.*

Proof. We use induction on n, with fact (1) above as the starting case $n = 1$. Let us split $p(x)$ into summands according to the powers of x_n,

$$p(x) = g_0 + g_1 x_n + g_2 x_n^2 + \dots + g_\ell x_n^\ell,$$

where $g_i \in F[x_1, \dots, x_{n-1}]$ for $0 \le i \le \ell \le d$, and g_ℓ is nonzero. We write every $v \in F^n$ in the form $v = (a, b)$ with $a \in F^{n-1}$, $b \in F$, and estimate the number of roots $p(a, b) = 0$.

Case 1. Roots (a, b) with $g_\ell(a) = 0$. Since $g_\ell \neq 0$ and $\deg g_\ell \le d - \ell$, by induction the polynomial g_ℓ has at most $(d-\ell)q^{n-2}$ roots in F^{n-1}, and for each a there are at most q different choices for b, which gives at most $(d-\ell)q^{n-1}$ such roots for $p(x)$ in F^n.

Case 2. Roots (a, b) with $g_\ell(a) \neq 0$. Here $p(a, x_n) \in F[x_n]$ is not the zero polynomial in the single variable x_n, it has degree ℓ, and hence for each a by (1) there are at most ℓ elements b with $p(a, b) = 0$. Since the number of a's is at most q^{n-1} we get at most ℓq^{n-1} roots for $p(x)$ in this way.

Summing the two cases gives at most

$$(d - \ell)q^{n-1} + \ell q^{n-1} = dq^{n-1}$$

roots for $p(x)$, as asserted. □

Lemma 35.2. *For every set $E \subseteq F^n$ of size $|E| < \binom{n+d}{d}$ there is a nonzero polynomial $p(x) \in F[x_1, \dots, x_n]$ of degree at most d that vanishes on E.*

Proof. Consider the vector space V_d of all polynomials in $F[x_1, \dots, x_n]$ of degree at most d. A basis for V_d is provided by the monomials $x_1^{s_1} \dots x_n^{s_n}$ with $\sum s_i \le d$:

$$1, x_1, \dots, x_n, x_1^2, x_1 x_2, \dots, x_1^3, \dots, x_n^d.$$

The following pleasing argument shows that the number of monomials $x_1^{s_1} \dots x_n^{s_n}$ of degree at most d equals the binomial coefficient $\binom{n+d}{d}$. What we want to count is the number of n-tuples $(s_1, \dots, s_n)$ of nonnegative integers with $s_1 + \dots + s_n \le d$. To do this, we map every n-tuple $(s_1, \dots, s_n)$ to the increasing sequence

$$s_1 + 1 < s_1 + s_2 + 2 < \dots < s_1 + \dots + s_n + n,$$

which determines an n-subset of $\{1, 2, \dots, d+n\}$. The map is bijective, so the number of monomials is $\binom{n+d}{d}$.

Next look at the vector space F^E of all functions $f : E \to F$; it has dimension $|E|$, which by assumption is less than $\binom{n+d}{d} = \dim V_d$. The evaluation map $p(x) \mapsto (p(a))_{a \in E}$ from V_d to F^E is a linear map of vector spaces. We conclude that it has a nonzero kernel, containing as desired a nonzero polynomial that vanishes on E. □

Theorem 35.3 (finite Kakeya problem). *Let $K \subseteq F^n$ be a Kakeya set. Then*

$$|K| \geq \binom{|F| + n - 1}{n} \geq \frac{|F|^n}{n!}.$$

Proof. The second inequality is clear from the definition of binomial coefficients. For the first, set again $q = |F|$ and suppose for a contradiction that

$$|K| < \binom{q + n - 1}{n} = \binom{n + q - 1}{q - 1}.$$

By Lemma 35.2 there exists a nonzero polynomial $p(x) \in F[x_1, \dots, x_n]$ of degree $d \leq q - 1$ that vanishes on K. Let us write

$$p(x) = p_0(x) + p_1(x) + \cdots + p_d(x), \tag{1}$$

where $p_i(x)$ is the sum of the monomials of degree i; in particular, $p_d(x)$ is nonzero. Since $p(x)$ vanishes on the nonempty set K, we have $d > 0$. Take any $v \in F^n \ \{0\}$. By the Kakeya property for this v there exists a $w \in F^n$ such that

$$p(w + tv) = 0 \quad \text{for all } t \in F.$$

Here comes the trick: Consider $p(w + tv)$ as a polynomial in the single variable t. It has degree at most $d \leq q - 1$ but vanishes on all q points of F, whence $p(w + tv)$ is the zero polynomial in t. Looking at (1) above we see that the coefficient of t^d in $p(w + tv)$ is precisely $p_d(v)$, which must therefore be 0. But $v \in F^n \ \{0\}$ was arbitrary and $p_d(0) = 0$ since $d > 0$, and we conclude that $p_d(x)$ vanishes on all of F^n. Since

$$dq^{n-1} \leq (q - 1)q^{n-1} < q^n,$$

Lemma 35.1, however, tells us that $p_d(x)$ must then be the zero polynomial — contradiction and end of the proof.

□

Chapter 36

Completing Latin squares

Lemma 36.1. *Any $(r \times n)$-Latin rectangle, $r < n$, can be extended to an $((r+1) \times n)$-Latin rectangle and hence can be completed to a Latin square.*

Proof. We apply Hall's theorem 30.4 (see Chapter 30). Let A_j be the set of numbers that do not appear in column j. An admissible $(r+1)$-st row corresponds then precisely to a system of distinct representatives for the collection $A_1, \dots, A_n$. To prove the lemma we therefore have to verify Hall's condition (H). Every set A_j has size $n-r$, and every element is in precisely $n-r$ sets A_j (since it appears r times in the rectangle). Any m of the sets A_j contain together $m(n-r)$ elements and therefore at least m different ones, which is just condition (H). □

Lemma 36.2. *Let P be a partial Latin square of order n with at most $n-1$ cells filled and at most $\frac{n}{2}$ distinct elements, then P can be completed to a Latin square of order n.*

Proof. TODO □

Theorem 36.3 (Smetaniuk's theorem)**.** *Any partial Latin square of order n with at most $n-1$ filled cells can be completed to a Latin square of the same order.*

Proof. □

Chapter 37

Permanents and the power of entropy

Theorem 37.1. *Let $M = (m_{ij})$ be an $n \times n$ matrix with entries in $\{0, 1\}$, and let $d_1, \dots, d_n$ be the row sums of M, that is, $d_i = \sum_{j=1}^{n} m_{ij}$. Then*

$$\operatorname{per} M \leq \prod_{i=1}^{n} (d_i!)^{1/d_i}.$$

Proof. TODO □

Theorem 37.2. *The number $L(n)$ of Latin squares of order n is bounded by*

$$\frac{n!^{2n}}{n^{n^2}} \leq L(n) \leq \prod_{k=1}^{n} k!^{n/k}$$

Proof. TODO □

37.1 Appendix: More about entropy

Theorem 37.3 (Fact A)**.**

$$H(X) \leq \log_2(|\operatorname{supp} X).$$

Proof. TODO □

Theorem 37.4 (Fact B)**.**

$$H(X, Y) = H(X) + H(Y|X).$$

Proof. TODO □

Theorem 37.5 (Fact B)**.**

$$H(Y|X) \leq \sum_{j=1}^{d} \operatorname{Prop}(X \in E_j) \log_2 j.$$

Proof. TODO □

Chapter 38

The Dinitz problem

Definition 38.1. Let $\vec{G} = (V, E)$ be a directed graph. A *kernel* $K \subseteq V$ is a subset of the vertices such that

(i) K is independent in G, and

(ii) for every $u \notin K$ there exists a vertex $v \in K$ with an edge $u \to v$.

Lemma 38.2. *Let $\vec{G} = (V, E)$ be a directed graph, and suppose that for each vertex $v \in V$ we have a color set $C(v)$ that is larger than the outdegree, $|C(v)| \geq d^+(v) + 1$. If every induced subgraph of $\vec{G}$ possesses a kernel, then there exists a list coloring of G with a color from $C(v)$ for each v.*

Proof. We proceed by induction on $|V|$. For $|V| = 1$ there is nothing to prove. Choose a color $c \in \mathcal{C} = \bigcup_{v \in V} C(v)$ and set

$$A(c) := \{v \in V : c \in C(v)\}.$$

By hypothesis, the induced subgraph $G_{A(c)}$ possesses a kernel $K(c)$. Now we color all $v \in K(c)$ with the color c (this is possible since $K(c)$ is independent), and delete $K(c)$ from G and c from C. Let G' be the induced subgraph of G on $V \;\; K(c)$ with $C'(v) = C(v) \;\; \{c\}$ as the new list of color sets. Notice that for each $v \in A(c) \;\; K(c)$, the outdegree $d^+(v)$ is decreased by at least 1 (due to condition (ii) of a kernel). So $d^+(v) + 1 \leq |C'(v)|$ still holds in $\vec{G}'$. The same condition also holds for the vertices outside $A(c)$, since in this case the color sets $C(v)$ remain unchanged. The new graph G' contains fewer vertices than G, and we are done by induction. □

Definition 38.3. A matching M of $G = (X \cup Y, E)$ is called *stable* if the following condition holds: Whenever $uv \in E \;\; M$, $u \in X$, $v \in Y$, then either $uy \in M$ with $y > v$ in $N(u)$ or $xv \in M$ with $x > u$ in $N(v)$, or both.

Lemma 38.4. *A stable matching always exists.*

Proof. Consider the following algorithm. In the first stage all men $u \in X$ propose to their top choice. If a girl receives more than one proposal she picks the one she likes best and keeps him on a string, and if she receives just one proposal she keeps that one on a string. The remaining men are rejected and form the reservoir R. In the second stage all men in R propose to their next choice. The women compare the proposals (together with the one on the string, if there is one), pick their favorite and put him on the string. The rest is rejected and forms the new set R. Now the men in R propose to their next choice, and so on. A man who has proposed to his last choice and is again rejected drops out from further consideration (as well as from the reservoir). Clearly, after some time the reservoir R is empty, and at this point the algorithm stops.

Claim. When the algorithm stops, then the men on the strings together with the corresponding girls form a stable matching.

Notice first that the men on the string of a particular girl move there in increasing preference (of the girl) since at each stage the girl compares the new proposals with the present mate and then picks the new favorite. Hence if $uv \in E$ but $uv \notin M$, then either u never proposed to v in which case he found a better mate before he even got around to v, implying $uy \in M$ with $y > v$ in $N(u)$, or u proposed to v but was rejected, implying $xv \in M$ with $x > u$ in $N(v)$. But this is exactly the condition of a stable matching. □

Theorem 38.5. *We have $\chi_\ell(S_n) = n$ for all n.*

Proof. As before we denote the vertices of S_n by (i,j), $1 \le i,j \le n$. Thus (i,j) and (r,s) are adjacent if and only if $i = r$ or $j = s$. Take any Latin square L with letters from $\{1,2,\dots,n\}$ and denote by $L(i,j)$ the entry in cell (i,j). Next make S_n into a directed graph $\vec{S}_n$ by orienting the horizontal edges $(i,j) \to (i,j')$ if $L(i,j) < L(i,j')$ and the vertical edges $(i,j) \to (i',j)$ if $L(i,j) > L(i',j)$. Thus, horizontally we orient from the smaller to the larger element, and vertically the other way around. (In the margin we have an example for $n = 3$.)

Notice that we obtain $d^+(i,j) = n-1$ for all (i,j). In fact, if $L(i,j) = k$, then $n-k$ cells in row i contain an entry larger than k, and $k-1$ cells in column j have an entry smaller than k.

By Lemma 38.2 it remains to show that every induced subgraph of $\vec{S}_n$ possesses a kernel. Consider a subset $A \subseteq V$, and let X be the set of rows of L, and Y the set of its columns. Associate to A the bipartite graph $G = (X \cup Y, A)$, where every $(i,j) \in A$ is represented by the edge ij with $i \in X, j \in Y$. In the example in the margin the cells of A are shaded.

The orientation on S_n naturally induces a ranking on the neighborhoods in $G = (X \cup Y, A)$ by setting $j' > j$ in $N(i)$ if $(i,j) \to (i,j')$ in $\vec{S}_n$ respectively $i' > i$ in $N(j)$ if $(i,j) \to (i',j)$. By Lemma 38.4, $G = (X \cup Y, A)$ possesses a stable matching M. This M, viewed as a subset of A, is our desired kernel! To see why, note first that M is independent in A since for edges in $G = (X \cup Y, A)$ they do not share an endvertex i or j. Secondly, if $(i,j) \in A \ \ M$, then by the definition of a stable matching there either exists $(i,j') \in M$ with $j' > j$ or $(i',j) \in M$ with $i' > i$, which for $\vec{S}_n$ means $(i,j) \to (i,j') \in M$ or $(i,j) \to (i',j) \in M$, and the proof is complete. □

Chapter 39

Five-coloring plane graphs

Theorem 39.1. *All planar graphs G can be 5-colored:*

$$\chi_\ell(G) \leq 5.$$

Proof. TODO □

Chapter 40

How to guard a museum

Theorem 40.1. *For any museum with n walls, $\lfloor \frac{n}{3} \rfloor$ guards suffice.*

Proof. First of all, let us draw $n-3$ noncrossing diagonals between corners of the walls until the interior is triangulated. For example, we can draw 9 diagonals in the museum depicted in the margin to produce a triangulation. It does not matter which triangulation we choose, any one will do. Now think of the new figure as a plane graph with the corners as vertices and the walls and diagonals as edges.

Claim. *This graph is 3-colorable.*

For $n = 3$ there is nothing to prove. Now for $n > 3$ pick any two vertices u and v which are connected by a diagonal. This diagonal will split the graph into two smaller triangulated graphs both containing the edge uv. By induction we may color each part with 3 colors where we may choose color 1 for u and color 2 for v in each coloring. Pasting the colorings together yields a 3-coloring of the whole graph.

The rest is easy. Since there are n vertices, at least one of the color classes, say the vertices colored 1, contains at most $\lfloor \frac{n}{3} \rfloor$ vertices, and this is where we place the guards. Since every triangle contains a vertex of color 1 we infer that every triangle is guarded, and hence so is the whole museum.

□

Chapter 41

Turán's graph theorem

Theorem 41.1 (First Proof)**.** *If a graph $G = (V, E)$ on n vertices has no p-clique, $p \geq 2$, then*

$$|E| \leq \left(1 - \frac{1}{p-1}\right)\frac{n^2}{2}. \tag{1}$$

Proof. We use induction on n. One easily computes that (1) is true for $n < p$. Let G be a graph on $V = \{v_1, \dots, v_n\}$ without p-cliques with a maximal number of edges, where $n \geq p$. G certainly contains $(p-1)$-cliques, since otherwise we could add edges. Let A be a $(p-1)$-clique, and set $B := V\ \ A$.

A contains $\binom{p-1}{2}$ edges, and we now estimate the edge-number e_B in B and the edge-number $e_{A,B}$ between A and B. By induction, we have $e_B \leq \frac{1}{2}\left(1 - \frac{1}{p-1}\right)(n-p+1)^2$. Since G has no p-clique, every $v_j \in B$ is adjacent to at most $p-2$ vertices in A, and we obtain $e_{A,B} \leq (p-2)(n-p+1)$. Altogether, this yields

$$|E| \leq \binom{p-1}{2} + \frac{1}{2}\left(1 - \frac{1}{p-1}\right)(n-p+1)^2 + (p-2)(n-p+1),$$

which is precisely $\left(1 - \frac{1}{p-1}\right)\frac{n^2}{2}$. □

Theorem 41.2 (Second Proof)**.** *If a graph $G = (V, E)$ on n vertices has no p-clique, $p \geq 2$, then*

$$|E| \leq \left(1 - \frac{1}{p-1}\right)\frac{n^2}{2}. \tag{1}$$

Proof. This proof makes use of the structure of the Turán graphs. Let $v_m \in V$ be a vertex of maximal degree $d_m = \max_{1 \leq j \leq n} d_j$. Denote by S the set of neighbors of v_m, $|S| = d_m$, and set $T := V\ \ S$. As G contains no p-clique, and v_m is adjacent to all vertices of S, we note that S contains no $(p-1)$-clique.

We now construct the following graph H on V (see the figure). H corresponds to G on S and contains all edges between S and T, but no edges within T. In other words, T is an independent set in H, and we conclude that H has again no p-cliques. Let d'_j be the degree of v_j in H. If $v_j \in S$, then we certainly have $d'_j \geq d_j$ by the construction of H, and for $v_j \in T$, we see $d'_j = |S| = d_m \geq d_j$ by the choice of v_m. We infer $|E(H)| \geq |E|$, and find that among all graphs with a maximal number of edges, there must be one of the form of H. By induction, the graph induced by S has at most as many edges as a suitable graph $K_{n_1,\dots,n_{p-2}}$ on S. So $|E| \leq |E(H)| \leq E(K_{n_1,\dots,n_{p-1}})$ with $n_{p-1} = |T|$, which implies (1). □

Theorem 41.3 (Third Proof)**.** *If a graph $G = (V, E)$ on n vertices has no p-clique, $p \geq 2$, then*

$$|E| \leq \left(1 - \frac{1}{p-1}\right) \frac{n^2}{2}. \tag{1}$$

Proof. Consider a *probability distribution* $\mathbf{w} = (w_1, \dots, w_n)$ on the vertices, that is, an assignment of values $w_i \geq 0$ to the vertices with $\sum_{i=1}^{n} w_i = 1$. Our goal is to maximize the function

$$f(\mathbf{w}) = \sum_{v_i v_j \in E} w_i w_j.$$

Suppose $\mathbf{w}$ is any distribution, and let v_i and v_j be a pair of nonadjacent vertices with positive weights w_i, w_j. Let s_i be the sum of the weights of all vertices adjacent to v_i, and define s_j similarly for v_j, where we may assume that $s_i \geq s_j$. Now we move the weight from v_j to v_i, that is, the new weight of v_i is $w_i + w_j$, while the weight of v_j drops to 0. For the new distribution $\mathbf{w}'$ we find

$$f(\mathbf{w}') = f(\mathbf{w}) + w_j s_i - w_j s_j \geq f(\mathbf{w}).$$

We repeat this (reducing the number of vertices with a positive weight by one in each step) until there are no nonadjacent vertices of positive weight anymore. Thus we conclude that there is an optimal distribution whose nonzero weights are concentrated on a clique, say on a k-clique. Now if, say, $w_1 \geq w_2 > 0$, then choose $w_1' = w_1 - \varepsilon w_1 - w_2$ and change w_1 to $w_1 - \varepsilon$ and w_2 to $w_2 + \varepsilon$. The new distribution $\mathbf{w}'$ satisfies $f(\mathbf{w}') = f(\mathbf{w}) + \varepsilon(w_2 s_1 - w_1 s_2) \geq f(\mathbf{w})$, and we infer that the maximal value of $f(\mathbf{w})$ is attained for $w_i = 1/k$ on a k-clique and $w_i = 0$ otherwise. Since a k-clique contains $\binom{k}{2}$ edges, we obtain

$$f(\mathbf{w}) = \binom{k}{2} \frac{1}{k^2} = \frac{1}{2}\left(1 - \frac{1}{k}\right).$$

Since this expression is increasing in k, the best we can do is to set $k = p - 1$ (since G has no p-cliques). So we conclude

$$f(\mathbf{w}) \leq \frac{1}{2}\left(1 - \frac{1}{p-1}\right)$$

for any distribution $\mathbf{w}$. In particular, this inequality holds for the *uniform* distribution given by $w_i = \frac{1}{n}$ for all i. Thus we find

$$\frac{|E|}{n^2} = f\left(\mathbf{w} = \frac{1}{n}\right) \leq \frac{1}{2}\left(1 - \frac{1}{p-1}\right),$$

which is precisely (1). □

Theorem 41.4 (Fourth Proof)**.** *If a graph $G = (V, E)$ on n vertices has no p-clique, $p \geq 2$, then*

$$|E| \leq \left(1 - \frac{1}{p-1}\right) \frac{n^2}{2}. \tag{1}$$

Proof. This time we use some concepts from probability theory. Let G be an arbitrary graph on the vertex set $V = \{v_1, \dots, v_n\}$. Denote the degree of v_i by d_i, and write $\omega(G)$ for the number of vertices in a largest clique, called the clique number of G.

Claim. We have $\omega(G) \geq \sum_{i=1}^{n} \frac{1}{n - d_i}$.

We choose a random permutation $\pi = v_1 v_2 \dots v_n$ of the vertex set V, where each permutation is supposed to appear with the same probability $\frac{1}{n!}$, and then consider the following set C_π. We put v_i into C_π if and only if v_i is adjacent to all v_j $(j < i)$ preceding v_i. By definition, C_π is a clique in G. Let $X = |C_\pi|$ be the corresponding random variable. We have $X = \sum_{i=1}^n X_i$, where X_i is the indicator random variable of the vertex v_i, that is, $X_i = 1$ or $X_i = 0$ depending on whether $v_i \in C_\pi$ or $v_i \notin C_\pi$. Note that v_i belongs to C_π with respect to the permutation $v_1 v_2 \dots v_n$ if and only if v_i appears before all $n-1-d_i$ vertices which are not adjacent to v_i, or in other words, if v_i is the first among v_i and its $n-1-d_i$ non-neighbors. The probability that this happens is $\frac{1}{n-d_i}$, hence $EX_i = \frac{1}{n-d_i}$.

Thus by linearity of expectation (see ?) we obtain

$$E(|C_\pi|) = EX = \sum_{i=1}^n EX_i = \sum_{i=1}^n \frac{1}{n-d_i}.$$

Consequently, there must be a clique of at least that size, and this was our claim. To deduce Turán's theorem from the claim we use the Cauchy–Schwarz inequality from Chapter 20,

$$\left(\sum_{i=1}^n a_i b_i\right)^2 \leq \left(\sum_{i=1}^n a_i^2\right)\left(\sum_{i=1}^n b_i^2\right).$$

Set $a_i = \sqrt{n-d_i}$, $b_i = \frac{1}{\sqrt{n-d_i}}$, then $a_i b_i = 1$, and so

$$n^2 \leq \left(\sum_{i=1}^n (n-d_i)\right)\left(\sum_{i=1}^n \frac{1}{n-d_i}\right) \leq \omega(G)\sum_{i=1}^n (n-d_i). \tag{2}$$

At this point we apply the hypothesis $\omega(G) \leq p-1$ of Turán's theorem. Using also $\sum_{i=1}^n d_i = 2|E|$ from the chapter on double counting, inequality (2) leads to

$$n^2 \leq (p-1)(n^2 - 2|E|),$$

and this is equivalent to Turán's inequality. □

Theorem 41.5 (Fifth Proof)**.** *If a graph $G = (V, E)$ on n vertices has no p-clique, $p \geq 2$, then*

$$|E| \leq \left(1 - \frac{1}{p-1}\right)\frac{n^2}{2}. \tag{1}$$

Proof. Let G be a graph on n vertices without a p-clique and with a maximal number of edges.

Claim. *G does not contain three vertices u, v, w such that $vw \in E$, but $uv \notin E$, $uw \notin E$.*

Suppose otherwise, and consider the following cases.

Case 1: $d(u) < d(v)$ or $d(u) < d(w)$. We may suppose that $d(u) < d(v)$. Then we duplicate v, that is, we create a new vertex v' which has exactly the same neighbors as v (but v' is not an edge), delete u, and keep the rest unchanged. The new graph G' has again no p-clique, and for the number of edges we find

$$|E(G')| = |E(G)| + d(v) - d(u) > |E(G)|,$$

a contradiction.

Case 2: $d(u) \geq d(v)$ and $d(u) \geq d(w)$. Duplicate u twice and delete v and w (as illustrated in the margin). Again, the new graph G' has no p-clique, and we compute (the -1 results from the edge vw):

$$|E(G')| = |E(G)| + 2d(u) - (d(v) + d(w) - 1) > |E(G)|.$$

So we have a contradiction once more. A moment's thought shows that the claim we have proved is equivalent to the statement that

$$u \sim v :\iff uv \notin E(G)$$

defines an equivalence relation. Thus G is a complete multipartite graph, $G = K_{n_1,\ldots,n_{p-1}}$, and we are finished. □

Theorem 41.6 (Five proofs of Turán's graph theorem)**.** *Collecting the proofs from the chapter...*

Proof. □

Chapter 42

Communicating without errors

Theorem 42.1. *Whenever* $T = \{v^{(1)}, \ldots, v^{(m)}\}$ *is an orthonormal representation of* G *with constant* σ_T*, then*

$$\Theta(G) \leq \frac{1}{\sigma_T}.$$

Proof. TODO □

Chapter 43

The chromatic number of Kneser graphs

Theorem 43.1 (Lyusternik–Shnirel'man)**.** *If the d-sphere S^d is covered by $d+1$ sets,*

$$S^d = U_1 \cup \cdots \cup U_d \cup U_{d+1},$$

such that each of the first d sets $U_1, \ldots, U_d$ is either open or closed, then one of the $d+1$ sets contains a pair of antipodal points $x^*, -x^*$.

Proof. Let a covering $S^d = U_1 \cup \cdots \cup U_d \cup U_{d+1}$ be given as specified, and assume that there are no antipodal points in any of the sets U_i. We define a map $f : S^d \to \mathbb{R}^d$ by

$$f(x) := (\delta(x, U_1), \delta(x, U_2), \ldots, \delta(x, U_d)).$$

Here $\delta(x, U_i)$ denotes the distance of x from U_i. Since this is a continuous function in x, the map f is continuous. Thus the Borsuk–Ulam theorem tells us that there are antipodal points $x^*, -x^*$ with $f(x^*) = f(-x^*)$. Since U_{d+1} does not contain antipodes, we get that at least one of x^* and $-x^*$ must be contained in one of the sets U_i, say in U_k $(k \leq d)$. After exchanging x^* with $-x^*$ if necessary, we may assume that $x^* \in U_k$. In particular this yields $\delta(x^*, U_k) = 0$, and from $f(x^*) = f(-x^*)$ we get that $\delta(-x^*, U_k) = 0$ as well.

If U_k is closed, then $\delta(-x^*, U_k) = 0$ implies that $-x^* \in U_k$, and we arrive at the contradiction that U_k contains a pair of antipodal points.

If U_k is open, then $\delta(-x^*, U_k) = 0$ implies that $-x^*$ lies in $\overline{U_k}$, the closure of U_k. The set U_k, in turn, is contained in $S^d\ \ (\overline{U_k})$, since this is a closed subset of S^d that contains U_k. But this means that $-x^*$ lies in $S^d\ \ (\overline{U_k})$, so it cannot lie in $-U_k$, and x^* cannot lie in U_k, a contradiction. □

Theorem 43.2 (Gale's theorem)**.** *There is an arrangement of $2k+d$ points on S^d such that every open hemisphere contains at least k of these points.*

Proof. □

Theorem 43.3 (Kneser's conjecture)**.** *We have*

$$\chi(K(2k+d, k)) = d+2.$$

Proof. For our ground set let us take $2k+d$ points in general position on the sphere S^{d+1}. Suppose the set $V(n,k)$ of all k-subsets of this set is partitioned into $d+1$ classes, $V(n,k) = V_1 \dot\cup \dots \dot\cup V_{d+1}$. We have to find a pair of disjoint k-sets A and B that belong to the same class V_i.

For $i = 1, \dots, d+1$ we set

$$O_i = \{x \in S^{d+1} : \text{the open hemisphere } H_x \text{ with pole } x \text{ contains a } k\text{-set from } V_i\}.$$

Clearly, each O_i is an open set. Together, the open sets O_i and the closed set $C = S^{d+1} \;\; (O_1 \cup \dots \cup O_{d+1})$ cover S^{d+1}. Invoking Lyusternik–Shnirel'man (43.1) we know that one of these sets contains antipodal points x^* and $-x^*$. This set cannot be C! Indeed, if $x^*, -x^* \in C$, then by the definition of the O_i's, the hemispheres H_{x^*} and H_{-x^*} would contain fewer than k points. This means that at least $d+2$ points would be on the equator $H_{x^*} \cap H_{-x^*}$ with respect to the north pole x^*, that is, on a hyperplane through the origin. But this cannot be since the points are in general position. Hence some O_i contains a pair $x^*, -x^*$, so there exist k-sets A and B both in class V_i, with $A \subset H_{x^*}$ and $B \subset H_{-x^*}$.

But since we are talking about open hemispheres, H_{x^*} and H_{-x^*} are disjoint, hence A and B are disjoint, and this is the whole proof. □

43.1 Appendix: A proof sketch for the Borsuk–Ulam theorem

Theorem 43.4. *For every continuous map $f : S^d \to \mathbb{R}^d$ from d-sphere to d-space, there are antipodal points x^*, $-x^*$ that are mapped to the same point $f(x^*) = f(-x^*)$.*

Proof. TODO □

Chapter 44

Of friends and politicians

Theorem 44.1. *Suppose that G is a finite graph in which any two vertices have precisely one common neighbor. Then there is a vertex which is adjacent to all other vertices.*

Proof. Suppose the assertion is false, and G is a counterexample, that is, no vertex of G is adjacent to all other vertices. To derive a contradiction, we proceed in two steps. The first part is combinatorics, and the second part is linear algebra.

(1) We claim that G is a regular graph, that is, $d(u) = d(v)$ for any $u, v \in V$.

Note first that the condition of the theorem implies that there are no cycles of length 4 in G. Let us call this the *C_4-condition.*

We first prove that any two *nonadjacent* vertices u and v have equal degree $d(u) = d(v)$. Suppose $d(u) = k$, where $w_1, \ldots, w_k$ are the neighbors of u. Exactly one of the w_i, say w_2, is adjacent to v, and w_2 is adjacent to exactly one of the other w_i's, say w_1, so that we have the situation of the figure to the left. The vertex v has with w_1 the common neighbor w_2, and with w_i $(i \geq 2)$ a common neighbor z_i $(i \geq 2)$. By the C_4-condition, all these z_i must be distinct. We conclude $d(v) \geq k = d(u)$, and thus $d(u) = d(v) = k$ by symmetry.

To finish the proof of (1), observe that any vertex different from w_2 is not adjacent to either u or v, and hence has degree k, by what we already proved. But since w_2 also has a non-neighbor, it has degree k as well, and thus G is k-regular.

Summing over the degrees of the k neighbors of u we get k^2. Since every vertex (except u) has exactly one common neighbor with u, we have counted every vertex once, except for u, which was counted k times. So the total number of vertices of G is

$$n = k^2 - k + 1.$$

(2) The rest of the proof is a beautiful application of some standard results of linear algebra. Note first that k must be greater than 2, since for $k \leq 2$ only $G = K_1$ and $G = K_3$ are possible by (1), both of which are trivial windmill graphs. Consider the adjacency matrix $A = (a_{ij})$, as defined on page 282. By part (1), any row has exactly k 1's, and by the condition of the theorem, for any two rows there is exactly one column where they both have a 1. Note further that the main diagonal consists of 0's. Hence we have

$$A^2 = \begin{pmatrix} k & 1 & \ldots & 1 \\ 1 & k & 1 & \\ \vdots & \ddots & \ddots & \vdots \\ 1 & \ldots & 1 & k \end{pmatrix} = (k-1)I + J,$$

where I is the identity matrix, and J the matrix of all 1's. It is immediately checked that J has the eigenvalues n (of multiplicity 1) and 0 (of multiplicity $n-1$). It follows that A^2 has the eigenvalues $k-1+n=k^2$ (of multiplicity 1) and $k-1$ (of multiplicity $n-1$).

Since A is symmetric and hence diagonalizable, we conclude that A has the eigenvalues k (of multiplicity 1) and $\pm\sqrt{k-1}$. Suppose r of the eigenvalues are equal to $\sqrt{k-1}$ and s of them are equal to $-\sqrt{k-1}$, with $r+s=n-1$. Now we are almost home. Since the sum of the eigenvalues of A equals the trace (which is 0), we find

$$k+r\sqrt{k-1}-s\sqrt{k-1}=0,$$

and, in particular, $r \neq s$, and

$$\sqrt{k-1}=\frac{k}{s-r}.$$

Now if the square root $\sqrt{m}$ of a natural number m is rational, then it is an integer! An elegant proof for this was presented by Dedekind in 1858: Let n_0 be the smallest natural number with $n_0\sqrt{m} \in \mathbb{N}$. If $\sqrt{m} \notin \mathbb{N}$, then there exists $\ell \in \mathbb{N}$ with $0 < \sqrt{m}-\ell < 1$. Setting $n_1 := n_0(\sqrt{m}-\ell)$, we find $n_1 \in \mathbb{N}$ and $n_1\sqrt{m} = n_0(\sqrt{m}-\ell)\sqrt{m} = n_0 m - \ell(n_0\sqrt{m}) \in \mathbb{N}$. With $n_1 < n_0$ this yields a contradiction to the choice of n_0.

Returning to our equation, let us set $h=\sqrt{k-1} \in \mathbb{N}$, then

$$h(s-r)=k=h^2+1.$$

Since h divides h^2+1 and h^2, we find that h must be equal to 1, and thus $k=2$, which we have already excluded. So we have arrived at a contradiction, and the proof is complete. □

Chapter 45

Probability makes counting (sometimes) easy

Theorem 45.1. *Every family of at most 2^{d-1} d-sets is 2-colorable, that is, $m(d) > 2^{d-1}$.*

Proof. TODO □

Theorem 45.2. *Every family of at most 2^{d-1} d-sets is 2-colorable, that is, $m(d) > 2^{d-1}$.*

Proof. TODO □

Theorem 45.3. *For every $k \geq 2$, there exists a graph G with chromatic number $\chi(G) > k$ and girth $\gamma(G) > k$.*

Proof. TODO □

Theorem 45.4. *Let G be a simple graph with n vertices and m edges, where $m \geq 4n$. Then*

$$\operatorname{cr}(G) \geq \frac{1}{64}\frac{m^3}{n^2}.$$

Proof. TODO □