Problem Solving for Math Competitions

Harm Derksen

CHAPTER 1

Mathematical Induction

1. The induction principle

Suppose that we want to prove that

"$P(n)$ is true for every positive integer n",

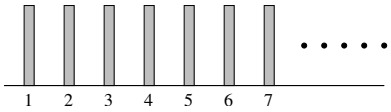
where $P(n)$ is a proposition (statement) which depends on a positive integer n. Proving $P(1)$, $P(2)$, $P(3)$, etc., would take an infinite amount of time. Instead we can use the so-called *induction principle*:

Induction Principle. Assume that k is an integer and $P(n)$ is a proposition for all $n \geq k$.

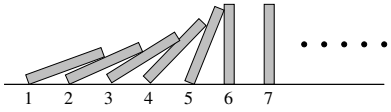
(1) Suppose that $P(k)$ is true, and
(2) for any integer $m \geq k$ for which $P(m)$ is true, $P(m+1)$ is true.

Then $P(n)$ is true for all integers $n \geq k$.

The induction principle can be compared to an infinite sequence of dominos tiles, numbered 1,2,3, etc.



If the m-th domino tile falls, it will hit the $(m+1)$-th domino tile and the $(m+1)$-th domino tile will fall as well. If the first domino tile falls, then *all* domino tiles will fall down. (Here $P(n)$ is the statement:"the n-th domino tile falls down")



Since the induction principle is intuitively clear, we will simply accept it without proof. This is why it is called an axiom. (We cannot formally prove the induction principle without making other, similar assumptions.)

A typical example of the induction principle is the following:

Example 1.1. Prove that

$$1 + 2 + 3 + \cdots + n = \frac{n(n+1)}{2}. \tag{1}$$

for every positive integer n.

Proof. We prove (1) by induction on n. For $n = 1$ we check that

$$1 = \frac{1 \cdot (1+1)}{2}.$$

Suppose that (1) is true for $n = m$. Then

$$1 + 2 + \cdots + m + (m + 1) = (1 + 2 + \cdots + m) + (m + 1) =$$

$$= \frac{m(m+1)}{2} + (m + 1) = \frac{(m + 1)(m + 2)}{2}.$$

so (1) is true for $n = m + 1$. Now (1) is true for all positive integers n by the induction principle. □

REMARK 1.2. When the German mathematician Carl Friedrich Gauss (1777–1855) was 10 years old, his school teacher gave the class an assignment to add all the numbers from 1 to 100. Gauss gave the answer almost immediately: 5050. This is how (we think) he did it: Write the numbers from 1 to 100 from left to right. Write under that the numbers from 1 to 100 in reverse order.

$$\begin{array}{ccccc} 1 & 2 & 3 & \cdots & 100 \\ 100 & 99 & 98 & \cdots & 1 \\ \hline \underbrace{101} & 101 & 101 & \cdots & 101 \end{array}$$
$$100$$

Each of the 100 column sums is 101. This shows that

$$2 \cdot (1 + 2 + \cdots + 100) = 100 \cdot 101$$

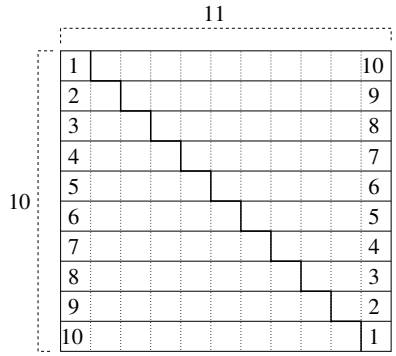
and

$$1 + 2 + \cdots + 100 = \frac{100 \cdot 101}{2} = 50 \cdot 101 = 5050.$$

This easily generalizes to a proof of (1). Gauss' proof can be graphically presented. For example, to see that

$$2 \cdot (1 + 2 + \cdots + 10) = 10 \cdot 11,$$

look at the following picture:



A formula similar to (1) exists for the sums of squares, namely

$$1^2 + 2^2 + \cdots + n^2 = \frac{n(n + 1)(2n + 1)}{6}. \tag{2}$$

EXAMPLE 1.3. Give and prove a formula for

$$1^3 + 2^3 + \cdots + n^3$$

We have seen similar examples, namely (1) and (2). We can also add the formula

$$1^0 + 2^0 + 3^0 + \cdots + n^0 = n.$$

Let

$$p_k(n) = 1^k + 2^k + 3^k + \cdots + n^k$$

where $k \in \mathbb{N}$. The examples so far suggest that $p_k(n)$ is a polynomial of degree $k+1$ (and that the leading coefficient is $\frac{1}{k+1}$). Let us *assume* that $p_3(n)$ is a polynomial of degree 4. Since $p_3(0)$ is an empty sum, we have that $p_3(0) = 0$. We can write $p_3(n) = an^4 + bn^3 + cn^2 + dn$. for certain real numbers a, b, c, d. We have

(3)

$$\begin{aligned} n^3 = p_3(n) - p_3(n-1) = a(n^4 - (n-1)^4) + b(n^3 - (n-1)^3) + c(n^2 - (n-1)^2) + d(n - (n-1)) = \\ = a(4n^3 - 6n^2 + 4n - 1) + b(3n^2 - 3n + 1) + c(2n - 1) + d = \\ = n^3(4a) + n^2(-6a + 3b) + n(4a - 3b + 2c) + (-a + b - c + d) \end{aligned}$$

Comparing coefficients in (3) gives us the linear equations:

$$1 = 4a \tag{4}$$

$$0 = -6a + 3b \tag{5}$$

$$0 = 4a - 3b + 2c \tag{6}$$

$$0 = -a + b - c + d \tag{7}$$

We solve the system of equations and find $a = \frac{1}{4}$, $b = \frac{1}{2}$, $c = \frac{1}{4}$ and $d = 0$. We now should conjecture the following formula:

$$1^3 + 2^3 + \cdots + n^3 = \tfrac{1}{4}n^4 + \tfrac{1}{2}n^3 + \tfrac{1}{4}n^2.$$

Finding this formula was the hard part. It is now not so hard to prove this formula by induction:

PROOF. We will prove that

$$1^3 + 2^3 + \cdots + n^3 = \tfrac{1}{4}n^4 + \tfrac{1}{2}n^3 + \tfrac{1}{4}n^2. \tag{8}$$

by induction on n. The case $n = 0$ is clear, because both sides of the equation are equal to 0. If (8) is true for $n = m - 1$, then

$$1^3 + 2^3 + \cdots + (m-1)^3 = \tfrac{1}{4}(m-1)^4 + \tfrac{1}{2}(m-1)^3 + \tfrac{1}{4}(m-1)^2.$$

From this follows that

$$\begin{aligned} 1^3 + 2^3 + \cdots + (m-1)^3 + m^3 = \tfrac{1}{4}(m-1)^4 + \tfrac{1}{2}(m-1)^3 + \tfrac{1}{4}(m-1)^2 + m^3 = \\ = \tfrac{1}{4}(m^4 - 4m^3 + 6m^2 - 4m + 1) + \tfrac{1}{2}(m^3 - 3m^2 + 3m - 1) + \tfrac{1}{4}(m^2 - 2m + 1) + m^3 = \\ = \tfrac{1}{4}m^4 + \tfrac{1}{2}m^3 + \tfrac{1}{4}m^2, \end{aligned}$$

so (8) is true for $n = m$. By induction follows that (8) is true for all $n \in \mathbb{N}$. □

Notice that

$$\tfrac{1}{4}m^4 + \tfrac{1}{2}m^3 + \tfrac{1}{4}m^2 = (\tfrac{1}{2}n(n+1))^2$$

which leads to the following aesthetic formula:

$$1^3 + 2^3 + \cdots + n^3 = (1 + 2 + \cdots + n)^2.$$

EXAMPLE 1.4. What is the value of

$$\frac{1}{1\cdot 2}+\frac{1}{2\cdot 3}+\frac{1}{3\cdot 4}+\cdots?$$

Let us compute the partial sums. Perhaps we will find a pattern.

$$\frac{1}{1\cdot 2}+\frac{1}{2\cdot 3}=\frac{2}{6}+\frac{4}{6}=\frac{2}{3},$$

$$\frac{1}{1\cdot 2}+\frac{1}{2\cdot 3}+\frac{1}{3\cdot 4}=\frac{2}{3}+\frac{1}{12}=\frac{8}{12}+\frac{1}{12}=\frac{9}{12}=\frac{3}{4},$$

$$\frac{1}{1\cdot 2}+\frac{1}{2\cdot 3}+\frac{1}{3\cdot 4}+\frac{1}{4\cdot 5}=\frac{3}{4}+\frac{1}{20}=\frac{15}{20}+\frac{1}{20}=\frac{16}{20}=\frac{4}{5}.$$

A pattern emerges. Namely, it seems that

$$\frac{1}{1\cdot 2}+\frac{1}{2\cdot 3}+\cdots+\frac{1}{n(n+1)}=1-\frac{1}{n+1}. \tag{9}$$

PROOF. By induction on n we prove:

$$\frac{1}{1\cdot 2}+\frac{1}{2\cdot 3}+\cdots+\frac{1}{n(n+1)}=1-\frac{1}{n+1}. \tag{10}$$

For $n=1$ we check

$$\frac{1}{1\cdot 2}=1-\frac{1}{2}.$$

If (10) is true for $n=m$, then

$$\frac{1}{1\cdot 2}+\frac{1}{2\cdot 3}+\cdots+\frac{1}{m(m+1)}+\frac{1}{(m+1)(m+2)}=$$

$$=\big(1-\frac{1}{m+1}\big)+(\frac{1}{m+1}-\frac{1}{m+2})=1-\frac{1}{m+2}.$$

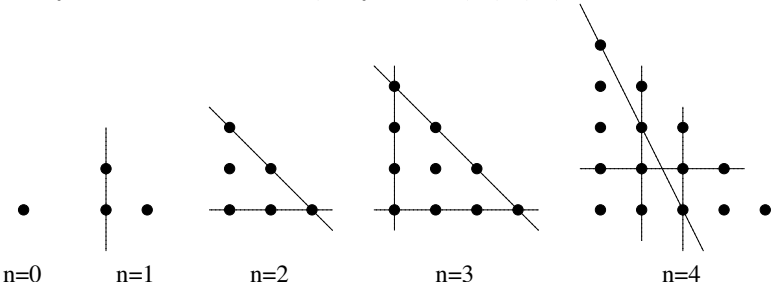
Hence (10) is true for $n=m+1$. By induction, (10) is true for all integers $n\geq 1$. We have

$$\frac{1}{1\cdot 2}+\frac{1}{2\cdot 3}+\frac{1}{3\cdot 4}+\cdots=\lim_{n\to\infty}\big(1-\frac{1}{n+1}\big)=1.$$

□

EXAMPLE 1.5 (UMUMC, 1988). Let S_n be the set of all pairs (x,y) with integral coordinates such that $x\geq 0$, $y\geq 0$ and $x+y\leq n$. Show that S_n cannot be covered by the union of n straight lines.

First we should try a few small cases, say $n=0,1,2,3,4$:



Notice that S_n is a subset of S_{n+1}. This will be helpful for our induction proof:

PROOF. We prove the statement by induction on n, the case $n = 0$ being trivial. Suppose that one needs at least $n + 1$ lines to cover S_n. Define $C_{n+1} = S_{n+1} \setminus S_n$. The set C_{n+1} consists of $n + 2$ points on the line $x + y = n + 1$. Suppose that k lines $\ell_1, \ell_2, \ldots, \ell_k$ cover S_{n+1}.

case 1: One of the lines is equal to the line $x + y = n + 1$. Without loss of generality we may assume that ℓ_k is equal to the line $x + y = n + 1$. Then $\ell_1, \ell_2, \ldots, \ell_{k-1}$ cover S_n because $\ell_k \cap S_n = \emptyset$. From the induction hypothesis follows that $k - 1 \geq n + 1$, so $k \geq n + 2$.

case 2: None of the lines are equal to the line $x + y = n + 1$. Then each of the lines intersects the line $x + y = n + 1$ in at most one point, and therefore it intersects the set C_{n+1} in at most one point. Since C_{n+1} has $n + 2$ elements, there must be at least $n + 2$ lines.

So in both cases we conclude that one needs at least $n + 2$ lines to cover S_{n+1}. □

2. Strong Induction

The following example illustrates that sometimes one has to make a statement stronger in order to be able to prove it by induction.

EXAMPLE 1.6. Prove that

$$\frac{1}{2} \cdot \frac{3}{4} \cdot \frac{5}{6} \cdots \frac{999,999}{1,000,000} < \frac{1}{1000}.$$

Since $1000 = \sqrt{1,000,000}$ one might suggest that

$$\frac{1}{2} \cdot \frac{3}{4} \cdot \frac{5}{6} \cdots \frac{2n-1}{2n} < \frac{1}{\sqrt{2n}} \tag{11}$$

for all $n \geq 1$. Let us try to prove (11). We can check (11) for small n (which gives some validity to our conjecture that this inequality holds). Suppose that (11) holds for $n = m$:

$$\frac{1}{2} \cdot \frac{3}{4} \cdot \frac{5}{6} \cdots \frac{2m-1}{2m} < \frac{1}{\sqrt{2m}} \tag{12}$$

We have to prove (11) for $n = m + 1$:

$$\frac{1}{2} \cdot \frac{3}{4} \cdot \frac{5}{6} \cdots \frac{2m+1}{2m+2} < \frac{1}{\sqrt{2m+2}}. \tag{13}$$

If we divide (13) by (12) we obtain

$$\frac{2m+1}{2m+2} \leq \sqrt{\frac{2m}{2m+2}}. \tag{14}$$

If (12) and (14) are true, then (13) is true. By squaring (14) we see that (14) is equivalent to

$$\left(\frac{2m+1}{2m+2}\right)^2 \leq \frac{2m}{2m+2}$$

and to

$$(2m+1)^2 \leq (2m+2)(2m) \tag{15}$$

So if (15) is true then our induction proof is complete. Unfortunately (15) is not true and we are stuck.

Sometimes it is easier to prove a *stronger* statement by induction:

PROOF. We prove

$$\frac{1}{2}\cdot\frac{3}{4}\cdots\frac{2n-1}{2n}<\frac{1}{\sqrt{2n+1}} \tag{16}$$

by induction on n. The case $n=1$ is clear because

$$\frac{1}{2}<\frac{1}{\sqrt{3}}.$$

Suppose that (16) is true for $n=m$:

$$\frac{1}{2}\cdot\frac{3}{4}\cdots\frac{2m-1}{2m}<\frac{1}{\sqrt{2m+1}} \tag{17}$$

Since

$$(2m+1)(2m+3)=(2m+2)^2-1<(2m+2)^2$$

we have that

$$\left(\frac{2m+1}{2m+2}\right)^2<\frac{2m+1}{2m+3}$$

and

$$\frac{2m+1}{2m+2}<\sqrt{\frac{2m+1}{2m+3}}. \tag{18}$$

Multiplying (17) by (18) yields

$$\frac{1}{2}\frac{3}{4}\cdots\frac{2m+1}{2m+2}<\frac{1}{\sqrt{2m+3}}, \tag{19}$$

so (16) is true for $n=m+1$. This shows that (16) is true for all positive integers n. In particular, for $n=500,000$ we get

$$\frac{1}{2}\cdot\frac{3}{4}\cdots\frac{999,999}{1,000,000}<\frac{1}{\sqrt{1,000,001}}<\frac{1}{1000}.$$

□

Below is a trickier proof of Example 1.6.

PROOF. Let

$$A=\frac{1\cdot 3\cdot 5\cdots 999,999}{2\cdot 4\cdot 6\cdots 1,000,000}$$

and

$$B=\frac{2\cdot 4\cdot 6\cdots 1,000,000}{3\cdot 5\cdot 7\cdots 1,000,001}.$$

Clearly $A<B$ because

$$\frac{1}{2}<\frac{2}{3},\frac{3}{4}<\frac{4}{5},\ldots,\frac{999,999}{1,000,000}<\frac{1,000,000}{1,000,001}.$$

It follows that

$$A^2<AB=\frac{1}{1,000,001}<\frac{1}{1,000,000}$$

and $A<1000^{-1}$. □

EXAMPLE 1.7. Prove that every integer $n\geq 2$ is a product of prime numbers.

PROOF. Let $Q(n)$ be the statement:

"every integer r with $2 \leq r \leq n$ is a product of prime numbers."

We use induction on n to prove that $Q(n)$ holds for all integers $n \geq 2$.

For $n = 2$ the statement is true because 2 is a prime number. Suppose that $Q(m)$ is true. We will prove $Q(m+1)$. Suppose that $2 \leq r \leq m+1$. If $r \leq m$ then r is a product of prime numbers because $Q(m)$ is true. Suppose that $r = m+1$. If $m+1$ is a prime number, then $m+1$ is a product of prime numbers and we are done. Otherwise, $m+1$ can be written as a product ab with $1 \leq a, b \leq m$. Because $Q(m)$ is true, both a and b are products of prime numbers. Hence $m+1 = ab$ is a product of prime numbers.

We have shown that $Q(n)$ holds for all $n \geq 2$. In particular, every integer $r \geq 2$ is a product of prime numbers because $Q(r)$ is true. □

3. Induction in definitions

We can also use induction in a definition. For example, the Fibonacci numbers is a sequence of numbers $F_0, F_1, F_2, \ldots$ defined by $F_0 = F_1 = 1$ and

$$F_{n+1} = F_n + F_{n-1}, \quad n \geq 1.$$

By (strong) induction on n we can prove that F_n is well-defined for all integers $n \geq 0$. The first few Fibonacci numbers are:

$$1, 1, 2, 3, 5, 8, 13, 21, 34, 55, 89, \ldots$$

The sum notation is an example of a recursive definition. Suppose that $f(n)$ is some function. If a, b are integers and $a \leq b+1$ then we define

$$\sum_{n=a}^{b} f(n)$$

as follows.

$$\sum_{n=a}^{a-1} f(n) = 0$$

and

$$\sum_{n=a}^{b} f(n) = f(b) + \sum_{n=a}^{b-1} f(n) \tag{20}$$

if $b \geq a$.

One can then formally prove by induction that

$$\sum_{n=a}^{c} f(n) = \sum_{n=a}^{b} f(n) + \sum_{n=b+1}^{c} f(n).$$

if $a, b, c \in \mathbb{Z}$ and $a - 1 \leq b \leq c$. (Induction on c. Start with $c = b$.)

Similarly we have the product notation.

$$\prod_{n=a}^{a-1} f(n) = 1$$

and

$$\prod_{n=a}^{b} f(n) = f(b) \prod_{n=a}^{b-1} f(n).$$

if $b \geq a$.

For nonnegative integers m and n with $m \leq n$ we define a binomial coefficient by

$$\binom{n}{m} = \begin{cases} 1 & \text{if } m = 0 \text{ or } m = n \\ \binom{n-1}{m-1} + \binom{n-1}{m} & \text{if } 0 < m < n \end{cases}.$$

If we arrange the binomial coefficients in a triangular shape, we get Pascal's triangle:

$$\begin{array}{ccccccccc} & & & & \binom{0}{0} & & & & \\ & & & \binom{1}{0} & & \binom{1}{1} & & & \\ & & \binom{2}{0} & & \binom{2}{1} & & \binom{2}{2} & & \\ & \binom{3}{0} & & \binom{3}{1} & & \binom{3}{2} & & \binom{3}{3} & \\ \binom{4}{0} & & \binom{4}{1} & & \binom{4}{2} & & \binom{4}{3} & & \binom{4}{4} \\ \vdots & & \vdots & & \vdots & & \vdots & & \vdots \end{array}$$

After evaluating the binomial coefficients we get:

$$\begin{array}{ccccccccc} & & & & 1 & & & & \\ & & & 1 & & 1 & & & \\ & & 1 & & 2 & & 1 & & \\ & 1 & & 3 & & 3 & & 1 & \\ 1 & & 4 & & 6 & & 4 & & 1 \\ \vdots & & \vdots & & \vdots & & \vdots & & \vdots \end{array}$$

4. Exercises

Exercise 1.1. * Prove that

$$1^2 + 2^2 + \cdots + n^2 = \frac{n(n+1)(2n+1)}{6}$$

for all positive integers n.

Exercise 1.2. * Show that

$$1 - \frac{1}{2} + \frac{1}{3} - \cdots + \frac{1}{2n-1} - \frac{1}{2n} = \frac{1}{n+1} + \frac{1}{n+2} + \cdots + \frac{1}{2n}$$

for all $n \in \mathbb{N}$.

Exercise 1.3. * Prove that

$$\sum_{i=0}^{n} \binom{m+i}{m} = \binom{m+n+1}{m+1}.$$

for all nonnegative integers m and n.

Exercise 1.4. * Prove that

$$(a+b)^n = \binom{n}{0}a^n + \binom{n}{1}a^{n-1}b + \binom{n}{2}a^{n-2}b^2 + \cdots + \binom{n}{n}b^n.$$

EXERCISE 1.5. *

(a) Prove that

$$1 + x + x^2 + \cdots + x^n = \frac{x^{n+1} - 1}{x - 1}.$$

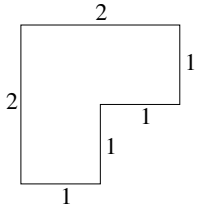
for every real number x and every positive integer n.

(b) If x is a real number with $|x| < 1$ then

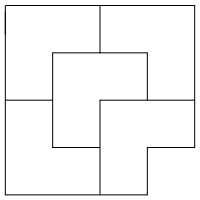
$$1 + x + x^2 + \cdots = \frac{1}{1 - x}.$$

EXERCISE 1.6. * Show that the sum of the squares of two consecutive Fibonacci numbers is again a Fibonacci number.

EXERCISE 1.7. ** Cut out a 1×1 corner of a $2^n \times 2^n$ chess board ($n \geq 1$). Show that the remainder of the chess board can be covered with L-shaped tiles (see picture).



The case $n = 2$ is shown below.



EXERCISE 1.8. ** Find and prove a formula for

$$1^4 + 2^4 + \cdots + n^4.$$

EXERCISE 1.9. ** Show that

$$\binom{n}{m} = \frac{n!}{m!\,(n-m)!}$$

as follows: Define

$$f(x) = (1 + x)^n = \binom{n}{0} + \binom{n}{1}x + \cdots + \binom{n}{n}x^n.$$

and consider $f^{(k)}(0)$ ($f^{(k)}(x)$ is the k-th derivative of $f(x)$).

EXERCISE 1.10. ** Prove that

$$\sqrt{n} < \sum_{i=1}^{n} \frac{1}{\sqrt{i}} < 2\sqrt{n}$$

for all integers $n \geq 2$.

EXERCISE 1.11. ** Define a sequence $a_1, a_2, \ldots$ by $a_1 = \frac{5}{2}$ and $a_{n+1} = a_n^2 - 2$ for $n \geq 1$. Give an explicit formula for a_n and prove it.

EXERCISE 1.12 (Division with remainder). ** Suppose that n is a nonnegative integer, and m is a positive integer. Prove that there exist integers q and r with $n = qm + r$ and $0 \leq r < m$.

EXERCISE 1.13. ** Give and prove a formula for

$$\frac{1}{1 \cdot 2 \cdot 3} + \frac{1}{2 \cdot 3 \cdot 4} + \cdots + \frac{1}{n \cdot (n+1) \cdot (n+2)}.$$

EXERCISE 1.14 (Expansion in base b). *** Suppose that n is a positive integer, and b is an integer ≥ 2. Show that there exist an nonnegative integer m, and integers $a_0, a_1, \ldots, a_m \in \{0, 1, 2, \ldots, b-1\}$ such that

$$n = a_m b^m + a_{m-1} b^{m-1} + \cdots + a_0 \tag{21}$$

and $a_m \neq 0$. Moreover, show that m and $a_0, a_1, \ldots, a_m$ are uniquely determined by n. (We will write $(a_m a_{m-1} \cdots a_0)_b$ for the right-hand side in (21)).

EXERCISE 1.15. *** Suppose that n is a positive integer. Show that we can write

$$n = F_{i_1} + F_{i_2} + \cdots + F_{i_k}$$

where k is a positive integer, $1 \leq i_1$ and $i_j \geq i_{j-1} + 2$ for $j = 2, 3, \ldots, k$. Also show that k and $i_1, \ldots, i_k$ are uniquely determined by n.

EXERCISE 1.16 (Putnam 1985, B2). *** Define polynomials $f_n(x)$ for $n \geq 0$ by $f_0(x) = 1$, $f_n(0) = 0$ for $n \geq 1$, and

$$\frac{d}{dx}(f_{n+1}(x)) = (n+1) f_n(x+1)$$

for $n \geq 0$. Find, with proof, the explicit factorization of $f_{100}(1)$ into powers of distinct primes.

EXERCISE 1.17 (Putnam 1987, B2). *** Let r, s and t be integers with $0 \leq r$, $0 \leq s$ and $r + s \leq t$. Prove that

$$\frac{\binom{s}{0}}{\binom{t}{r}} + \frac{\binom{s}{1}}{\binom{t}{r+1}} + \cdots + \frac{\binom{s}{s}}{\binom{t}{r+s}} = \frac{t+1}{(t+1-s)\binom{t-s}{r}}.$$

CHAPTER 2

Extremal Principle

It sometimes can be very useful to assume that a certain quantity is maximal. We will see various examples of this.

1. The Discrete Extremal Principle

The (discrete version) of the extremal principle can be formulated as follows:

Discrete Extremal Principle *A real valued function f on a finite set S has a maximum and a minimum.*

EXAMPLE 2.1 ($(\text{UM})^2\text{C}^{18}$ 2001 2). **** Show that the people at a party can be divided into two groups and sent to two different rooms in such a way that, for every person in either room, at least half that person's friends at the party are in the other room. (You may assume that friendship is a symmetric relation.

PROOF. Let m the the number of all pairs $\{P, Q\}$ of people such that P and Q are in different rooms and P and Q are friends. We may assume that m is maximal over all possible ways of dividing the people in two groups. Suppose some person P has a_P friends in his own room and b_P friends in the other room. If P would move to the other room then we have to add $b_P - a_P$ to m. By our maximality assumption on m, we get that $b_P \leq a_P$ for all P which is what we wanted to prove. □

2. The Continuous Extremal Principle

There is also a continuous version of the Extremal Priciple. This is not quite as obvious. It is well known in calculus.

Continuous Extremal Principle A continuous real-valued function f on a closed interval $[a, b] \subset \mathbb{R}$ has a maximum and a minimum.

THEOREM 2.2 (Rolle's Theorem). *Suppose that f is a real-valued differentiable function on an open inverval (a, b) which has a maximum (or minimum) at $c \in (a, b)$. Then $f'(c) = 0$.*

PROOF. By definition

$$f'(c) = \lim_{h \to 0} \frac{f(c+h) - f(c)}{h}$$

In particular

$$f'(c) = \lim_{h \downarrow 0} \frac{f(c+h) - f(c)}{h} \leq 0$$

because $f(c)$ is the maximal value of f. On the other hand

$$f'(c) = \lim_{h \uparrow 0} \frac{f(c+h) - f(c)}{h} \geq 0.$$

This shows $f'(c) = 0$. □

EXAMPLE 2.3. Show that

$$x^3 + \frac{3}{x} \geq 4$$

for $x > 0$.

PROOF. Let $f(x) = x^3 + 3/x$. Clearly if $0 < x < \frac{1}{2}$ and if $x > 2$, then $f(x) \geq 4$. The continuous function $f(x)$ has a minimum on the interval $[\frac{1}{2}, 2]$, say at c. If $c = \frac{1}{2}$ or $c = 2$ then $f(x) \geq f(c) \geq 4$ for all $x \in [\frac{1}{2}, 2]$. Assume now that $\frac{1}{2} < c < 2$. Then we must have

$$f'(c) = 3c^2 - \frac{3}{c^2} = 0$$

by Theorem 2.2. We easily solve this and find $c = 1$. Now we have

$$f(x) \geq f(1) \geq 4$$

for all $x \in [\frac{1}{2}, 2]$. □

An immediate consequence of the previous theorem and the Continuous Extremal Principle is the Mean Value Theorem:

THEOREM 2.4 (Mean Value Theorem). *Let f be a continuous real-valued function on the closed interval $[a, b] \subset \mathbb{R}$ which is differentiable on the open interval (a, b). Then there exists a $c \in (a, b)$ such that*

$$f'(c) = \frac{f(b) - f(a)}{b - a}.$$

PROOF. Put

$$g(x) = f(x) - f(a) - \frac{f(b) - f(a)}{b - a}(x - a).$$

Note that $g(a) = g(b) = 0$. There exists a $c \in [a, b]$ with $g(c)$ maximal. If $c = a$ or $c = b$, then $g(x) \leq 0$ for $x \in [a, b]$ and we can find a $c \in (a, b)$ such that $g(c)$ is minimal. In any case there is a $c \in (a, b)$ for which $g(c)$ is maximal or minimal. From the previous theorem follows that

$$g'(c) = f'(c) - \frac{f(b) - f(a)}{b - a} = 0.$$

□

THEOREM 2.5. *Suppose f is a differentiable function on an interval (a, b). Then f is (weakly) increasing if and only if $f'(x) \geq 0$ for all $a < x < b$. (Weakly increasing means here that $f(x_1) \leq f(x_2)$ if $a \leq x_1 < x_2 \leq b$.)*

PROOF. Suppose that $a \leq x_1 < x_2 \leq b$. By the Mean Value Theorem there exists a c in the interval (x_1, x_2) such that

$$\frac{f(x_2) - f(x_1)}{x_2 - x_1} = f'(c)$$

Since $f'(c) \geq 0$ and $x_2 > x_1$, we have $f(x_2) \geq f(x_1)$. □

EXAMPLE 2.6. * Show that $\sin(x) \leq x$ for $x \geq 0$ and $\sin(x) \geq x$ for $x \leq 0$. Also show that $\cos(x) \geq 1 - \frac{1}{2}x^2$ for all $x \in \mathbb{R}$.

PROOF. Consider $f(x) = \sin(x) - x$. Then $f'(x) = \cos(x) - 1 \leq 0$. This means that $f(x)$ is weakly decreasing on $\mathbb{R}$. Since $f(0) = 0$, we have $f(x) \leq 0$ for all $x \geq 0$ and $f(x) \geq 0$ for all $x \leq 0$. Now consider $g(x) = \cos(x) - 1 + \frac{1}{2}x^2$. we have $g'(x) = -\sin(x) + x = -f(x)$. Therefore $g'(x) \geq 0$ for $x \geq 0$ and $g'(x) \leq 0$ for $x \leq 0$. It follows that g is weakly increasing for $x \geq 0$ and g is weakly decreasing for $x \leq 0$. Since $g(0) = 0$ we have $g(x) \geq 0$ for all $x \in \mathbb{R}$. □

EXAMPLE 2.7. Suppose that $x_1, x_2, \ldots, x_n$ are real numbers such that $0 \leq x_i \leq 1$ for all i. What is the maximum possible value of

$$\sum_{i=1}^{n} \sum_{j=1}^{n} (x_i - x_j)^2.$$

PROOF. We want to maximalize the function

$$f(x_1, x_2, \ldots, x_n) = \sum_{i=1}^{n} \sum_{j=1}^{n} (x_i - x_j)^2.$$

(With some analysis one can see that f must have a maximum value, because f is a continuous function on a compact set. Don't worry if you do not understand this. Perhaps we will discuss it later, but we will not use it now.) Let us fix $x_2, x_3, \ldots, x_n$, and consider f as a function of one variable x_1. Say $f = ax_1^2 + bx_1 + c$ where $a = n^2 > 0$ and b, c are constants depending on $x_2, x_3, \ldots, x_n$. Now f could have a local extremum, but this would always be a local minimum because $a > 0$. The maximum of f is therefore at $x_1 = 0$ or at $x_1 = 1$.

From this discussion it is clear that we can replace x_1 by 0 or by 1 without decreasing the value of $f(x_1, x_2, \ldots, x_n)$. Similary, we can replace x_2 by 0 or by 1 without decreasing the value of f etc. So

$$f(x_1, x_2, \ldots, x_n) \leq f(y_1, y_2, \ldots, y_n)$$

for some choices $y_1, y_2, \ldots, y_n \in \{0, 1\}$.

So we are looking for the maximum value of

$$f(y_1, y_2, \ldots, y_n)$$

where $y_1, y_2, \ldots, y_n \in \{0, 1\}$. By symmetry we may assume that $y_1 = y_2 = \cdots = y_k = 0$ and $y_{k+1} = y_{k+2} = \cdots = y_n = 1$. In that case, the value of $f(y_1, \ldots, y_n)$ is $k(n-k) + (n-k)k = 2k(n-k)$. The function $2k(n-k)$ is again a parabola with the maximum at $k = \frac{n}{2}$. But k has to be an integer. It follows that the maximum value of $f(x_1, x_2, \ldots, x_n)$ is

$$2\frac{n}{2}(n - \frac{n}{2}) = \frac{n^2}{2}$$

if n is even and

$$2\frac{n-1}{2}(n - \frac{n-1}{2}) = \frac{n^2 - 1}{2}$$

if n is odd.

Exercises

EXERCISE 2.1. *** There are n people standing in a field, each carrying a gun. Every person shoots the person nearest to him (all people shoot at the same time, all distances are distinct). Show that at least one person survives if n is odd.

EXERCISE 2.2. ** Let $f : \mathbb{Z} \to \mathbb{Z}$ be an integer-valued function on $\mathbb{Z}$ with

$$2f(n) < f(n-1) + f(n+1)$$

for all $n \in \mathbb{Z}$. Prove that f has arbitrary large values.

EXERCISE 2.3. **** Let S be a measurable subset of $\mathbb{R}^2$ with area A. Show that one can choose a set $T \subset S$ of at least A/π points in S such that all pairs of distinct points in T have distance at least 1. (*Hint:* Suppose that S is maximal. Consider balls of radius 1 around each point. What can you say now?)

The following result is actually useful in *coding theory* and is known as the *Gilbert-Varshamov bound*.

EXERCISE 2.4. **** Let $S = \{0,1\}^n$ (this means that S is the set of all sequences with just zeroes and ones of length n). For $a = (a_1, a_2, \ldots, a_n)$ and $b = (b_1, b_2, \ldots, b_n)$ we define the *Hamming distance* by

$$d(a,b) = \#\{i \mid a_i \neq b_i\}$$

i.e., the number of indices for which $a_i \neq b_i$. Prove that for every positive integer k there exists a subset T of S with at least

$$\frac{2^n}{\binom{n}{0} + \binom{n}{1} + \binom{n}{2} + \cdots + \binom{n}{k-1}}.$$

elements such that $d(a,b) \geq k$ for all distinct $a, b \in T$. (The solution to this problem is similar to the solution of Problem 2.3.)

EXERCISE 2.5. *** Suppose that $a_1, a_2, \ldots, a_n, b_1, b_2, \ldots, b_n$ are real numbers such that $a_1 \leq a_2 \leq \cdots \leq a_n$ and $b_1 \leq b_2 \leq \cdots \leq b_n$. Let $c_1, c_2, \ldots, c_n$ be a permutation of $b_1, b_2, \ldots, b_n$. Show that

$$a_1 b_n + a_2 b_{n-1} + \cdots + a_n b_1 \leq a_1 c_1 + a_2 c_2 + \cdots + a_n c_n \leq a_1 b_1 + a_1 b_2 + \cdots + a_n b_n.$$

(*Hint: Choose a permutation $c_1, \ldots, c_n$ such that $a_1 c_1 + \cdots + a_n c_n$ is maximal. Prove that $c_1 \leq \cdots \leq c_n$.*)

EXERCISE 2.6. *** Suppose that $a_1 \leq a_2 \leq \cdots \leq a_n$ and $b_1 \leq b_2 \leq \cdots \leq b_n$. Prove the following *Chebychev inequality*:

$$\frac{a_1 + a_2 + \cdots + a_n}{n} \cdot \frac{b_1 + b_2 + \cdots + b_n}{n} \leq \frac{a_1 b_1 + a_2 b_2 + \cdots + a_n b_n}{n}.$$

(*Hint:* Use the previous problem.)

EXERCISE 2.7. ** For every integer n, prove that there exists a subset S of $\{1, 2, \ldots, n^2\}$ with n elements ,so that the difference of any two distinct elements of S is not a square.

EXERCISE 2.8. ******* Suppose that there are n lines in the Euclidean plane $\mathbb{R}^2$ such that

(a) Every two lines intersect;
(b) Through any intersection point of two lines there goes at least one other line.

Prove that all lines go through one point. (*Hint: Choose a line ℓ and an intersection point P, not on ℓ, such that the distance of P to ℓ is minimal. Deduce a contradiction.*)

EXERCISE 2.9. ***** Suppose that in the plane $\mathbb{R}^2$, there are n blue points and n red points (all of them distinct). No four points are on a line. Show that you can label the blue points with $B_1, B_2, \ldots, B_n$ and the red points with $R_1, R_2, \ldots, R_n$ such that the line segments B_iR_i do not intersect each other. (*Hint: Choose a labeling with $\sum_{i=1}^{n} |B_iR_i|$ minimal, where $|B_iR_i|$ is the distance from B_i to R_i.*)

EXERCISE 2.10. *** Suppose that f is a differentiable function on the interval $[0, 2]$. Prove that there exists an element $x \in [0, 2]$ with

$$f''(x) = f(0) - 2f(1) + f(2).$$

EXERCISE 2.11. ** Find the maximum value of

$$x^{\frac{1}{x}}$$

for $x > 0$.

EXERCISE 2.12. * Show that

$$e^x \geq x + 1$$

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

EXERCISE 2.13. * Show that

$$\log(x) \leq x - 1$$

for all $x > 0$ (here $\log(x)$ is the natural logarithm).

EXERCISE 2.14. ** Suppose that f is a differentiable function on $[0, \infty)$ such that $f(0) = 1$ and $f'(x) \geq f(x)$ for all $x > 0$. Prove that $f(x) \geq e^x$ for all $x > 0$.

EXERCISE 2.15. ** Suppose that $f(x)$ is a continuous function on $\mathbb{R}$ which can be differentiated twice, and $f''(x) > 0$ for all $x \in \mathbb{R}$. Show that $f(x)$ is positive for some $x \in \mathbb{R}$.

EXERCISE 2.16 (Putnam 1985). *** Let T be an acute triangle. Inscribe a rectangle R in T with one side along a side of T. Then inscribe a rectangle S in the triangle formed by the side of R opposite the side of the boundary of T and the two othert sides of T, with one side along the side of R. For any polygon X, let $A(X)$ denote the area of X. Find the maximum value, or show that no maximum exists, of

$$\frac{A(R) + A(S)}{A(T)}$$

where T ranges over all trinagles and R, S over all rectangles as above.

CHAPTER 3

Inequalities

1. Elementary inequalities

Perhaps the most fundamental inequality for real numbers is

$$x^2 \geq 0, \quad x \in \mathbb{R}.$$

Using this inequality one can deduce many more inequalities. For example, if we take $x = a - b$ with $a, b \in \mathbb{R}$ we obtain:

$$a^2 - 2ab + b^2 = (a - b)^2 \geq 0.$$

It follows that

$$\frac{a^2 + b^2}{2} \geq ab.$$

This inequality is interesting by itself. If we now substitute $a = \sqrt{y}$ and $b = \sqrt{z}$ we obtain

$$\frac{y + z}{2} \geq \sqrt{yz}.$$

whenever y, z are nonnegative real numbers. Substitution is a very useful method for proving inequalities.

EXAMPLE 3.1. Prove that

$$a^2 + b^2 + c^2 \geq ab + ac + bc$$

for all $a, b, c \in \mathbb{R}$. Also prove that equality holds if and only if $a = b = c$.

PROOF. We have

$$a^2 + b^2 + c^2 - ab - ac - bc = \tfrac{1}{2}((a - b)^2 + (b - c)^2 + (c - a)^2) \geq 0$$

and it is now obvious that equality holds if and only if $a = b = c = 0$. □

Another obvious but important inequality is:

$$xy \geq 0, \quad \text{if } x, y \in \mathbb{R} \text{ and } x \geq 0 \text{ and } y \geq 0.$$

This can be used in many ways. For example if $0 \leq x \leq 1$ then

$$x \geq x^2$$

because

$$x - x^2 = x(1 - x) \geq 0$$

and both x and $1 - x$ are nonnegative.

EXAMPLE 3.2. Suppose that $x_1, x_2, \ldots, x_n$ are real numbers such that $0 \leq x_i \leq 1$ for all i. Prove that

$$x_1 + x_2 + \cdots + x_n \geq x_1x_2 + x_2x_3 + x_3x_4 + \cdots + x_nx_1.$$

When do we have equality?

PROOF. The inequality is obvious because it is equivalent to

$$x_1(1 - x_2) + x_2(1 - x_3) + \cdots + x_n(1 - x_1) \geq 0.$$

If we have equality then

$$x_1 = 0 \text{ or } x_2 = 1, \quad x_2 = 0 \text{ or } x_3 = 1, \ldots \quad , x_n = 0 \text{ or } x_1 = 1.$$

If $x_1 \neq 0$ then $x_2 = 1$ and in particular $x_2 \neq 0$. From this it follows that $x_3 = 1$. But then $x_3 \neq 0$, so $x_4 = 1$, etc. This way we see that $x_2 = x_3 = x_4 = \cdots = x_n = x_1 = 1$. In a similar way we see that if $x_i \neq 0$ for some i, then $x_1 = x_2 = x_3 = \cdots = x_n = 1$. The only other case where equality holds is when $x_1 = x_2 = \cdots = x_n = 0$. □

Making the right substitutions can be very helpful as the following example shows.

EXAMPLE 3.3. Suppose that $a_1, a_2, \ldots, a_n$ are real numbers such that $a_i \geq 1$ for all i. Prove the inequality

$$(1 + a_1)(1 + a_2) \cdots (1 + a_n) \geq \frac{2^n}{n+1}(1 + a_1 + a_2 + \cdots + a_n).$$

Let us write $a_i = x_i + 1$. Then $x_i \geq 0$ for all i. It is easier to deal with the inequality $x_i \geq 0$ than with the inequality $a_i \geq 1$. The inequality transforms to

$$(2 + x_1)(2 + x_2) \cdots (2 + x_n) \geq \frac{2^n}{n+1}(x_1 + x_2 + \cdots + x_n + (n + 1)) =$$

$$= 2^n + \frac{2^n}{n+1}(x_1 + x_2 + \cdots + x_n).$$

This inequality follows already if we only look at the constant and linear part of the left-handside:

$$(2 + x_1)(2 + x_2) \cdots (2 + x_n) \geq 2^n + 2^{n-1}(x_1 + x_2 + \cdots + x_n) \geq 2^n + \frac{2^n}{n+1}(x_1 + \cdots + x_n).$$

because

$$2^{n-1} \geq \frac{2}{n+1}2^{n-1} = \frac{2^n}{n+1}.$$

2. Convexity

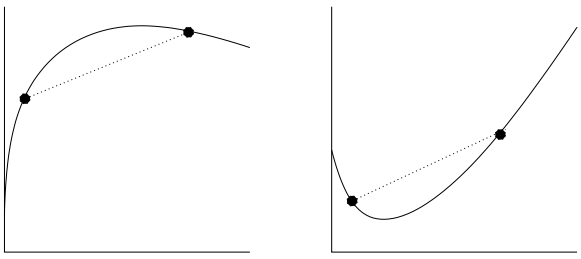
Let f be a real-valued function on an interval $I \subseteq \mathbb{R}$. Now f is said to be *convex* if

$$f(ta + (1 - t)b) \leq tf(a) + (1 - t)f(b)$$

for all $t \in [0, 1]$ and all $a, b \in I$ (the chord between $(a, f(a))$ and $(b, f(b))$ lies above the graph of f). The function f is said to be *concave* if

$$f(ta + (1 - t)b) \geq tf(a) + (1 - t)f(b)$$

for all $t \in [0, 1]$ and all $a, b \in I$ (the chord between $(a, f(a))$ and $(b, f(b))$ lies below the graph of f).



concave convex

(You may well be used to a different terminology, for example "concave up" and "concave down" instead of "convex" and "concave".)

THEOREM 3.4. *Suppose that f is a real-valued function on $I \subseteq \mathbb{R}$, $x_1, x_2, \ldots, x_n \in I$, and $t_1, t_2, \ldots, t_n \in [0,1]$ with $t_1 + t_2 + \cdots + t_n = 1$. If f is convex, then*

$$f(t_1x_1 + t_2x_2 + \cdots + t_nx_n) \leq t_1f(x_1) + t_2f(x_2) + \cdots + t_nf(x_n). \tag{22}$$

If f is concave, then

$$f(t_1x_1 + t_2x_2 + \cdots + t_nx_n) \geq t_1f(x_1) + t_2f(x_2) + \cdots + t_nf(x_n). \tag{23}$$

PROOF. Suppose that f is convex. We will prove the statement by induction on n, the case $n = 1$ being trivial. Suppose that we already have proven that

$$f(t_1x_1 + t_2x_2 + \cdots + t_nx_n) \leq t_1f(x_1) + t_2f(x_2) + \cdots + t_nf(x_n).$$

for all $x_1, x_2, \ldots, x_n \in I$ and all $t_1, t_2, \ldots, t_n \in [0,1]$ with $t_1 + t_2 + \cdots + t_n = 1$.

Suppose now that $x_1, x_2, \ldots, x_{n+1} \in I$ and $t_1, \ldots, t_{n+1} \in [0,1]$ with $t_1+t_2+\cdots+t_{n+1} = 1$. Define $s_i = t_i/(1 - t_{n+1})$ for $i = 1, 2, \ldots, n$. Note that $s_1 + s_2 + \cdots + s_n = 1$. Take $a = s_1x_1 + s_2x_2 + \cdots + s_nx_n$, $b = x_{n+1}$ and $t = 1 - t_{n+1}$. From the definition of convexity and the induction hypothesis follows that

$$\begin{aligned} f(t_1x_1 + \cdots + t_{n+1}x_{n+1}) = f(ta + (1-t)b) \leq tf(a) + (1-t)f(b) = \\ = (1 - t_{n+1})f(s_1x_1 + \cdots + s_nx_n) + t_{n+1}f(x_{n+1}) \leq \\ \leq (1 - t_{n+1})(s_1f(x_1) + s_2f(x_2) + \cdots + s_nf(x_n)) + t_{n+1}f(x_{n+1}) = \\ = t_1f(x_1) + \cdots + t_{n+1}f(x_{n+1}). \end{aligned}$$

To prove the second statement, observe that f is concave if and only if $-f$ is convex. Then apply the first statement to $-f$. □

In particular the case $t_1 = t_2 = \cdots = t_n = 1/n$ is interesting.

COROLLARY 3.5. *If f is convex on I, then*

$$f\Big(\frac{x_1 + x_2 + \cdots + x_n}{n}\Big) \leq \frac{f(x_1) + \cdots + f(x_n)}{n}$$

for all $x_1, \ldots, x_n \in I$.

If f is concave on I, then

$$f\Big(\frac{x_1 + x_2 + \cdots + x_n}{n}\Big) \geq \frac{f(x_1) + \cdots + f(x_n)}{n}$$

for all $x_1, \ldots, x_n \in I$.

THEOREM 3.6. *Suppose that f is a real-valued function on an interval $I \subseteq \mathbb{R}$ with a second derivative. If $f''(x) \geq 0$ for all $x \in I$, then f is convex. If $f''(x) \leq 0$ for all $x \in I$, then f is concave. (The converse of these statements are also true).*

PROOF. If $f''(x) \geq 0$ for all $x \in I$ then $f'(x)$ is weakly increasing on the interval I. Suppose that $a, b \in I$ and $t \in [0, 1]$. Define $c = ta + (1-t)b$. By the Mean Value Theorem, there exist $\alpha \in (a, c)$ and $\beta \in (c, b)$ such that

$$f'(\alpha) = \frac{f(c) - f(a)}{c - a} \text{ and } f'(\beta) = \frac{f(b) - f(c)}{b - c}.$$

Since $\alpha < \beta$ and f' is weakly increasing, we have

$$\frac{f(ta + (1-t)b) - f(a)}{(1-t)(b-a)} = \frac{f(c) - f(a)}{c - a} = f'(\alpha) \leq$$

$$\leq f'(\beta) = \frac{f(b) - f(c)}{b - c} = \frac{f(b) - f(ta + (1-t)b)}{t(b-a)}$$

Multiplying out gives

$$f(ta + (1-t)b) \leq tf(a) + (1-t)f(b).$$

This shows that f is convex.

The second statement follows from the first statement, applied to $-f$. □

EXAMPLE 3.7. Suppose that α, β, γ are the angles of a triangle. Prove that

$$\sin(\alpha) + \sin(\beta) + \sin(\gamma) \leq \frac{3\sqrt{3}}{2}$$

PROOF. The function $\sin(x)$ is concave on the interval $[0, \pi]$, because its second derivative is $-\sin(x) \leq 0$. Thus we have

$$\frac{\sin(\alpha) + \sin(\beta) + \sin(\gamma)}{3} \leq \sin\left(\frac{\alpha + \beta + \gamma}{\pi}\right) = \sin(\tfrac{1}{3}\pi) = \frac{\sqrt{3}}{2}.$$

□

3. Arithmetics, Geometric and Harmonic mean

THEOREM 3.8. *Let $x_1, x_2, x_3, \ldots, x_n > 0$. We define the Arithmetic Mean by*

$$A(x_1, x_2, \ldots, x_n) = \frac{x_1 + x_2 + \cdots + x_n}{n},$$

the Geometric Mean by

$$G(x_1, x_2, \ldots, x_n) = \sqrt[n]{x_1 x_2 \cdots x_n}$$

and the Harmonic Mean by

$$H(x_1, x_2, \ldots, x_n) = \frac{n}{\frac{1}{x_1} + \frac{1}{x_2} + \cdots + \frac{1}{x_n}}.$$

Then we have

$$H(x_1, \ldots, x_n) \leq G(x_1, \ldots, x_n) \leq A(x_1, \ldots, x_n).$$

PROOF. Let $f(x) = \log(x)$. Then $f''(x) = -1/x^2 < 0$ for $x > 0$ so f is concave on the interval $(0, \infty)$. It follows that

$$\log\big(\frac{x_1 + x_2 + \cdots + x_n}{n}\big) \geq \frac{\log(x_1) + \log(x_2) + \cdots + \log(x_n)}{n}.$$

Applying the exponential function (which is an increasing function) to both sides yields

$$\frac{x_1 + x_2 + \cdots + x_n}{n} \geq \sqrt[n]{x_1 x_2 \cdots x_n}.$$

If we now take $y_i = \frac{1}{x_i}$ then we get

$$\frac{\frac{1}{y_1} + \frac{1}{y_2} + \cdots + \frac{1}{y_n}}{n} \geq \frac{1}{\sqrt[n]{y_1 y_2 \cdots y_n}}.$$

Taking the reciprocal yields

$$\frac{n}{\frac{1}{y_1} + \frac{1}{y_2} + \cdots + \frac{1}{y_n}} \leq \sqrt[n]{y_1 y_2 \cdots y_n}.$$

□

EXAMPLE 3.9. Suppose that $x_1, x_2, \ldots, x_n$ are positive real numbers. Prove that

$$\frac{x_1}{x_2} + \frac{x_2}{x_3} + \cdots + \frac{x_{n-1}}{x_n} + \frac{x_n}{x_1} \geq n.$$

PROOF. Put $y_i = x_i/x_{i+1}$ for all i. We assume that the index is cyclic, so that $x_{n+1} = x_1$. Comparing the arithmetic and geometric average gives:

$$\frac{y_1 + y_2 + \cdots + y_n}{n} \geq \sqrt[n]{y_1 y_2 \cdots y_n} = 1.$$

□

4. The Schwarz Inequality

Another important inequality is the Schwarz inequality. For vectors $x = (x_1, \ldots, x_n)$ and $y = (y_1, \ldots, y_n)$ in $\mathbb{R}^n$ one defines

$$x \cdot y = x_1 y_1 + \cdots + x_n y_n.$$

Note that $x \cdot y = y \cdot x$, $(x+y) \cdot z = x \cdot z + y \cdot z$ and $(tx) \cdot y = t(x \cdot y)$ for $t \in \mathbb{R}$ and $x, y, z \in \mathbb{R}^n$.

The norm of the vector x is defined by

$$\|x\| = \sqrt{x \cdot x} = \sqrt{x_1^2 + \cdots + x_n^2}.$$

THEOREM 3.10. *Suppose that $x = (x_1, x_2, \ldots, x_n)$, $y = (y_1, y_2, \ldots, y_n) \in \mathbb{R}^n$, then*

$$|x_1 y_1 + \cdots + x_n y_n| \leq \sqrt{x_1^2 + \cdots + x_n^2}\sqrt{y_1^2 + \cdots + y_n^2}$$

or in short form:

$$|x \cdot y| \leq \|x\|\|y\|.$$

PROOF. For any vector $a \cdot a \geq 0$. In particular, if we take $a = x + ty$ we get

$$(x + ty) \cdot (x + ty) = x \cdot x + 2t(x \cdot y) + t^2(y \cdot y) \geq 0$$

for all $t \geq 0$. Viewed as a quadratic polynomial in t, this polynomial has a nonpositive discriminant. The discriminant is

$$4(x \cdot y)^2 - 4(x \cdot x)(y \cdot y) \leq 0$$

In particular we have

$$(x \cdot y)^2 \leq (x \cdot x)(y \cdot y)$$

and taking square roots gives us

$$|x \cdot y| \leq \sqrt{x \cdot x}\sqrt{y \cdot y} = \|x\|\|y\|.$$

□

The Schwarz inequality is important in Euclidean geometry in dimension $2, 3$ or higher. In particular, one often defines the angle ϕ between two vectors x, y by

$$\cos(\varphi) = \frac{x \cdot y}{|x||y|}, \quad 0 \leq \varphi \leq \pi.$$

The Schwarz inequality tells us that this definition makes sense, since the righthand side has absolute value at most 1.

5. The triangle inequality

Another famous geometric inequality is the triangle inequality. If a, b, c are the lengths of the sides of a triangle, then $a + b \geq c$ (and also $a + c \geq b$ and $b + c \geq a$).

6. One more useful inequality

THEOREM 3.11. *Suppose that $x_1, x_2, \ldots, x_n, y_1, y_2, \ldots, y_n$ are real numbers such that $x_1 \leq x_2 \leq \cdots \leq x_n$ and $y_1 \leq y_2 \leq \cdots \leq y_n$. Suppose that $z_1, z_2, \ldots, z_n$ are the same as $y_1, y_2, \ldots, y_n$, but possibly in a different order. Then we have*

$$x_1y_n + x_2y_{n-1} + \cdots + x_ny_n \leq x_1z_1 + x_2z_2 + \cdots + x_nz_n \leq x_1y_1 + x_2y_2 + \cdots + x_ny_n.$$

PROOF. Suppose that $z_1, z_2, \ldots, z_n$ is a rearrangement of $y_1, y_2, \ldots, y_n$. Let m be the number of displacements of the sequence $z_1, z_2, \ldots, z_n$, so m is the number of pairs (i, j) with $i < j$ and $z_i > z_j$. We prove the right inequality by induction on m. If $m = 0$ then $z_i = y_i$ for all i and we have inequality. Suppose $m > 0$. Then $z_i > z_{i+1}$ for some i. Note that the sequence

$$z_1, z_2, \ldots, z_{i-1}, z_{i+1}, z_i, z_{i+2}, \ldots, z_n$$

(exchange z_i and z_{i+1}) has only $m - 1$ displacements, so by induction

$$x_1z_1 + x_2z_2 + \cdots x_iz_{i+1} + x_{i+1}z_i + \cdots + x_nz_n \geq x_1y_1 + x_2y_2 + \cdots + x_nz_n.$$

We have

$$(x_{i+1} - x_i)(z_i - z_{i+1}) \geq 0,$$

so

$$x_iz_i + x_{i+1}z_{i+1} \geq x_iz_{i+1} + x_{i+1}z_i$$

and

$$x_1z_1 + x_2z_2 + \cdots + x_iz_i + x_{i+1}z_{i+1} + \cdots + x_nz_n \geq$$

$$\geq x_1z_1 + x_2z_2 + \cdots + x_iz_{i+1} + x_{i+1}z_i + \cdots + x_nz_n \geq x_1y_1 + x_2y_2 + \cdots + x_ny_n.$$

The left inequality in the Theorem follows from the right inequality. Note that $-y_n \leq -y_{n-1} + \cdots \leq -y_1$ and that $-z_1, -z_2, \ldots, -z_n$ is a rearrangement of $-y_1, -y_2, \ldots, -y_n$. So we have

$$x_1(-z_1) + x_2(-z_2) + \cdots + x_n(-z_n) \leq x_1(-y_n) + x_2(-y_{n-1}) + \cdots + x_n(-y_1).$$

□

7. Exercises

EXERCISE 3.1. ** Use the inequality $\frac{x+y}{2} \geq \sqrt{xy}$ repeatedly to prove

$$\frac{x+y+z+w}{4} \geq \sqrt[4]{xyzw}$$

for all $x, y, z, w \geq 0$.

EXERCISE 3.2. ** Prove that

$$x_1^2 + x_2^2 + \cdots + x_n^2 \geq \frac{2}{n-1} \sum_{1 \leq i < j \leq n} x_i x_j$$

for all positive integers n.

EXERCISE 3.3. * If $x \leq y \leq z$ and $y > 0$, prove that

$$x + z - y \geq \frac{xz}{y}$$

EXERCISE 3.4. ** For nonnegative real $u_1, \ldots, u_n$, prove that

$$(\sum_{i=1}^{n} u_i)^3 \leq n^2 \sum_{i=1}^{n} u_i^3.$$

(use that x^3 is convex for $x \geq 0$).

EXERCISE 3.5. *** Suppose that $p_1, p_2, \ldots, p_n$ are nonnegative real numbers such that $\sum_{i=1}^{n} p_i = 1$. Prove that

$$\sum_{i=1}^{n} -p_i \log p_i \leq \log n.$$

(This inequality comes from *information theory.*)

EXERCISE 3.6. ** For positive real a, b, c prove that

$$b^3c^3 + c^3a^3 + a^3b^3 \geq 3a^2b^2c^2.$$

EXERCISE 3.7. *** Let

$$s_n = 1 + \frac{1}{2} + \frac{1}{3} + \cdots + \frac{1}{n}.$$

Prove that

$$n((n+1)^{\frac{1}{n}} - 1) \leq s_n \leq n - \frac{n-1}{n^{1/(n-1)}}.$$

(Hint: use the geometric and arithmetic mean for $1+1, 1+\frac{1}{2}, \cdots, 1+\frac{1}{n}$ and for $1-\frac{1}{2}, 1-\frac{1}{3}, \cdots, 1-\frac{1}{n}$.)

EXERCISE 3.8. **** Prove the Hölder inequality: If $1/p + 1/q = 1$ and $x, y \in \mathbb{R}^n$ then

$$|x \cdot y| \leq \|x\|_p \|y\|_q$$

where $\|x\|_p = (|x_1|^p + |x_2|^p + \cdots + |x_n|^p)^{1/p}$. (Hint: Use that $\log(x)$ is convex and prove $x_i y_i \leq x_i^p/p + y_i^q/q$. Then prove the inequality in the special case that $\|x\|_p = \|y\|_q = 1$. Reduce the general case to this special case.)

EXERCISE 3.9. * Let Q be a convex quadrilateral (i.e., the diagonals lie inside the figure). Let S be the sum of the lengths of the diagonals and let P be the perimeter. Prove

$$\frac{1}{2}P < S < P.$$

EXERCISE 3.10. ** Suppose that we have an triangle with sides a, b, c such that for every positive integer n there exists a triangle with sides a^n, b^n and c^n. Prove that the triangle must be equilateral.

EXERCISE 3.11. ** Suppose that $x_1, x_2, \ldots, x_n$ are positive real numbers. Prove that

$$\frac{x_1^2}{x_2} + \frac{x_2^2}{x_3} + \cdots + \frac{x_{n-1}^2}{x_n} + \frac{x_n^2}{x_1} \geq x_1 + x_2 + \cdots + x_n.$$

EXERCISE 3.12. *** Prove that

$$a^a b^b c^c \geq a^b b^c c^a$$

for all positive real numbers a, b, c.

EXERCISE 3.13. * Prove that

$$\frac{x_1}{x_1 + x_2} + \frac{x_2}{x_2 + x_3} + \cdots + \frac{x_{n-1}}{x_{n-1} + x_n} + \frac{x_n}{x_n + x_1} \geq 1$$

EXERCISE 3.14. **** Prove or disprove: If x and y are real numbers with $y \geq 0$ and $y(y+1) \leq (x+1)^2$, then $y(y-1) \leq x^2$.

EXERCISE 3.15. **** Let a, b, c be positive real numbers such that $abc = 1$. Prove that

$$= \frac{1}{a^3(b+c)} + \frac{1}{b^3(c+a)} + \frac{1}{c^3(a+b)} \geq \frac{3}{2}.$$

EXERCISE 3.16. **** Let $p_1, p_2, \ldots, p_n$ be any n points on the sphere

$$\{(x, y, z) \mid x^2 + y^2 + z^2 = 1\}.$$

Prove that the sum of the squares of the distances between them is at most n^2.

EXERCISE 3.17 (USSR Mathematics Olympiad). ****** Suppose that $x_1, x_2, \ldots, x_n$ are positive real numbers. Prove that

$$\frac{x_1}{x_2 + x_3} + \frac{x_2}{x_3 + x_4} + \cdots + \frac{x_n}{x_1 + x_2} \geq \frac{n}{4}$$

(indices go cyclic).

CHAPTER 4

Number Theory

1. The greatest common divisor

If d and n are integers, then we say that d divides n if and only if there exists an integer q such that $n = qd$. Notice that if d divides n and m, then d also divides $n + m$ and $n - m$ and $an + bm$ for all integers a, b.

THEOREM 4.1. *If n and m are integers and $m \neq 0$, then there exists an integer q such that*

$$n = qm + r$$

where $0 \leq r < |m|$.

PROOF. First reduce to the case that $n \geq 0$. Then use induction on n. (Exercise.) □

A useful variation is the following result.

THEOREM 4.2. *If n and m are integers and $m \neq 0$, then there exists an integer q such that*

$$n = qm + r$$

where $-|m|/2 \leq r < |m|/2$.

Suppose that n and m are integers, not both equal to 0. The greatest common divisor of n and m is the largest *positive* integer d such that d divides both n and m. We denote the greatest common divisor of n and m by $\gcd(n, m)$. We will also use the convention that $\gcd(0, 0) = 0$. The following observation will be useful.

LEMMA 4.3. *If $n, m, q \in \mathbb{Z}$, then We have $\gcd(n, m) = \gcd(m, n - qm)$.*

PROOF. The case $n = m = 0$ is clear. Assume that at least one of n and m is nonzero. Now $\gcd(n, m)$ divides n, m and $n - qm$, hence

$$\gcd(n, m) \leq \gcd(m, n - qm).$$

On the other hand, $\gcd(m, n - qm)$ divides m, $n - qm$ and $n = (n - qm) + qm$. so

$$\gcd(m, n - qm) \leq \gcd(n, m).$$

□

EXAMPLE 4.4. Suppose we have two large integers, say 9081 and 3270. How do we find their greatest common divisor? We do division with remainder:

$$9081 = 3 \cdot 3270 - 729.. \tag{24}$$

Now $\gcd(9081, 3270) = \gcd(3270, 729)$. We have simplified our problem! Now we can play this game again:

$$3270 = 4 \cdot 729 + 354. \tag{25}$$

so $\gcd(3270, 729) = \gcd(729, 354)$.

$$729 = 2 \cdot 354 + 21 \tag{26}$$

so $\gcd(729, 354) = \gcd(354, 21)$.

$$354 = 17 \cdot 21 - 3 \tag{27}$$

so $\gcd(354, 21) = \gcd(21, 3) = 3$ because $21 = 7 \cdot 3$. We have found that $\gcd(9081, 3270) = 3$. This method of computing the gcd is called Euclid's algorithm.

ALGORITHM 4.5 (Euclid's Algorithm). Suppose that $r_0, r_1 \in \mathbb{Z}$ are nonzero integers. Define $q_1, q_2, \cdots \in \mathbb{Z}$ and $r_2, r_3, \cdots \in \mathbb{Z}$ inductively as follows. If r_{i-1} and r_i are already defined, then we define q_i and r_{i+1} by

$$r_{i-1} = q_i r_i + r_{i+1}$$

where $0 \leq r_{i+1} < |r_i|$ as in Theorem 4.1 (or $-|r_i|/2 \leq r_{i+1} < |r_i|/2$ as in Theorem 4.2). (Note r_{i+1} and q_i are well defined as long as $r_i \neq 0$).

Since $|r_1| > |r_2| > \cdots$ we have that $r_{k+1} = 0$ for some positive integer k. Suppose that $r_{k+1} = 0$ and that $r_i \neq 0$ for $i \leq k$. Then $\gcd(r_0, r_1) = r_k$.

If one uses Theorem 4.2 then it is clear that Euclid's algorithm is very fast. The number of divisions with remainder one has to do is roughly $\log_2 |r_1|$. (A similar bound also holds if one uses Theorem 4.1 though).

PROOF. It is not hard to show that Euclid's algorithm works. Note that $\gcd(r_{i-1}, r_i) = \gcd(r_i, r_{i+1})$ for all i. By induction on i one shows that $\gcd(r_0, r_1) = \gcd(r_i, r_{i+1})$ for all i. In particular,

$$\gcd(r_0, r_1) = \gcd(r_k, r_{k+1}) = \gcd(r_k, 0) = r_k.$$

□

EXAMPLE 4.6. Euclid's algorithm can be used to find integers x and y such that $\gcd(n, m) = xn + ym$. It works as follows. First use Euclid's algorithm to compute $\gcd(n, m)$ and then work back. For example, we already saw that $\gcd(9081, 3270) = 3$. We would like to find x and y such that

$$3 = 9081x + 3270y.$$

Now we work back in the computation of $\gcd(9081, 3270)$. From (27) follows that

$$3 = (-1) \cdot 354 + 17 \cdot 21.$$

From (26) follows that

$$3 = (-1) \cdot 354 + 17 \cdot (729 - 2 \cdot 354) = 17 \cdot 729 + (-1 - 17 \cdot 2) \cdot 354 = 17 \cdot 729 - 35 \cdot 354.$$

From (25) follows that

$$3 = 17 \cdot 729 - 35 \cdot (3270 - 4 \cdot 729) =$$
$$= -35 \cdot 3270 + (17 + 35 \cdot 4) \cdot 729 = -35 \cdot 3270 + 157 \cdot 729.$$

and finally, from (24) follows that

$$3 = -35 \cdot 3270 + 157 \cdot (-9081 + 3 \cdot 3270) =$$
$$= -157 \cdot 9081 + (-35 + 3 \cdot 157) \cdot 3270 = -157 \cdot 9081 + 436 \cdot 3270.$$

This method is sometimes called the *extended Euclid's algorithm.*

ALGORITHM 4.7. (Extended Euclid's Algorithm) Let $r_0, r_1, \ldots, r_k, r_{k+1} = 0$ and $q_0, q_1, \ldots, q_k$ as in Algorithm 4.5.

Define $x_k = 0$ and $x_{k+1} = 1$. For $i \geq 1$, define x_{k-i} by induction by

$$x_{k-i-1} = x_{k-i+1} - q_{k-i}x_{k-i}.$$

Then we have that

$$\gcd(r_0, r_1) = x_{i+1}r_i + x_i r_{i+1}$$

for $i = 0, 1, \ldots, k$. In particular,

$$\gcd(r_0, r_1) = x_1 r_0 + x_0 r_1.$$

PROOF. Let $i = k - j$. We prove by induction on j that

$$\gcd(r_0, r_1) = x_{k-j+1}r_{k-j} + x_{k-j}r_{k-j+1}.$$

For $j = 0$ we have to prove that

$$\gcd(r_0, r_1) = 1 \cdot r_k + 0 \cdot r_{k+1} = r_k$$

but this follows from Algorithm 4.5.

Suppose that

$$\gcd(r_0, r_1) = x_{k-j+1}r_{k-j} + x_{k-j}r_{k-j+1}.$$

If we substitute, $r_{k-j+1} = r_{k-j-1} - q_{k-j}r_{k-j}$ we obtain

$$\gcd(r_0, r_1) = x_{k-j+1}r_{k-j} + x_{k-j}(r_{k-j-1} - q_{k-j}r_{k-j}) =$$
$$= x_{k-j}r_{k-j-1} + (x_{k-j+1} - q_{k-j}x_{k-j})r_{k-j} = x_{k-j}r_{k-j-1} + x_{k-j-1}r_{k-j}.$$

□

THEOREM 4.8. *Suppose that n and m are integers. There exist integers x and y such that*

$$\gcd(n, m) = xn + ym.$$

PROOF. This follows from the extended Euclid's Algorithm (Algorithm 4.7). □

If n and m are integers with $\gcd(n, m) = 1$ then we say that m and n are *relatively prime.*

COROLLARY 4.9. *If a, n, m are integers and a divides both n and m then a also divides* $\gcd(n, m)$.

PROOF. This follows immediately from the previous Theorem 4.8. □

EXAMPLE 4.10 (Putnam 2000). Prove that the expression

$$\frac{\gcd(m, n)}{n}\binom{n}{m}$$

is an integer.

Given our previous discussion, it seems natural to write

$$\gcd(m,n) = xm + yn$$

where x, y are integers. The solution then follows quickly.

PROOF. We can write

$$\gcd(m,n) = xm + yn$$

where $x, y \in \mathbb{Z}$. Then

$$\frac{\gcd(m,n)}{n}\binom{n}{m} = x\binom{n}{m} + y\frac{m}{n}\binom{n}{m}.$$

Now

$$\frac{m}{n}\binom{n}{m} = \frac{m}{n}\frac{n!}{m!(n-m)!} = \frac{(n-1)!}{(m-1)!(n-m)!} = \binom{n-1}{m}$$

is an integer. It follows that

$$\frac{\gcd(m,n)}{n}\binom{n}{m}$$

is an integer. □

LEMMA 4.11. *Suppose that n, m, r are integers such that $\gcd(m,n) = 1$. If m divides nr then m divides r.*

PROOF. We can write $1 = xm + yn$ for certain $x, y \in \mathbb{Z}$. Clearly m divides xmr and ynr, so m divides

$$r = r \cdot 1 = r \cdot (xm + yn) = xmr + ynr.$$

□

If n and m are nonzero integers then the least common multiple $\operatorname{lcm}(m,n)$ of n and m is defined as the smallest positive integer that is divisible by both m and n. Moreover we define $\operatorname{lcm}(m,0) = 0$ for all integers m.

LEMMA 4.12. *If n and m are positive integers and a is an integer divisible by both n and m, then a is divible by $\operatorname{lcm}(m,n)$.*

PROOF. We can write $a = q\operatorname{lcm}(m,n) + r$ with $0 \leq r < \operatorname{lcm}(m,n)$. NOw r is also divisible by m and n. We must have that $r = 0$ otherwise we get a contradiction with the definition of $\operatorname{lcm}(m,n)$. This proves that a is divisible by $\operatorname{lcm}(m,n)$. □

LEMMA 4.13. *If n and m are positive integers then*

$$\gcd(m,n)\operatorname{lcm}(m,n) = mn$$

PROOF. The positive integer $mn/\gcd(m,n)$ is divisible by m and n, so

$$\frac{mn}{\gcd(m,n)} \geq \operatorname{lcm}(m,n).$$

The positive integer $mn/\operatorname{lcm}(m,n)$ divides both m and n.So we have

$$\frac{mn}{\operatorname{lcm}(m,n)} \leq \gcd(m,n).$$

□

EXAMPLE 4.14. In the strange country Oz, the only official coins are the 7-cents coin and the 13-cents coin. What is the largest amount that cannot be paid with these coins if a shop has no change at all?

We can first make a list of amounts that we can make:

$$7, 13, 14, 20, 21, 26, 27, 28, 33, 34, 35, 39, 40, 41, 42, 46, 48, 48, 49, 52, 53, 54, 55, 56,$$

$$59, 60, 61, 62, 63, 65, 66, 67, 68, 69, 70, 72, 73, 74, 75, 76, 77, 78, 79, \ldots$$

The largest amount that cannot be made seems to be 71. It is easy to check that 71 is not a nonnegative combination of 7 and 13.

Let us try to understand why all the amounts of ≥ 72 can be made by using the two types of coins. Suppose that $m \geq 72$. We would like to find nonnegative integers x and y such that

$$m = 13x + 7y$$

If x and y are not necessarily nonnegative then this is certainly possible. We can write

$$1 = 13 \cdot (-1) + 7 \cdot 2$$

and

$$m = 13 \cdot (-m) + 7 \cdot 2m.$$

Using this solution we find many other solutions. If k is an integer then

$$m = 13 \cdot (-m + 7k) + 7 \cdot (2m - 13k).$$

For a suitable k, we might have that both $-m+7k$ and $2m-13k$ are nonnegative. Consider the smallest k for which $-m + 7k$ is nonnegative. Then we have $0 \leq -m + 7k < 7$. Now

$$7 \cdot (2m - 13k) \geq m - 13 \cdot (-m + 7k) \geq 72 - 13 \cdot 6 = -6.$$

It follows that $2m - 13k > -1$, so $2m - 13k$ is nonnegative.

Now we would like to prove that if

$$71 = 13x + 7y \tag{28}$$

with $x, y \in \mathbb{Z}$, then at least one of the integers x, y is negative. We already saw one solution, namely

$$71 = 13 \cdot (-71) + 7 \cdot (142). \tag{29}$$

Combining (28) and (29) yields:

$$13 \cdot (x + 71) = 7 \cdot (142 - y).$$

Since $\gcd(13, 7) = 1$, we have that 7 divides $x + 71$. Say $x + 71 = 7k$. Then we alsy have that $142 - y = 13k$. From $x + 71 = 7k$ and $x \geq 0$ follows that $k \geq 11$. But then $y = 142 - 13k \leq -1$.

2. Prime Numbers

Recall that a prime number is a positive integer with exactly 2 positive divisors, namely 1 and itself.

LEMMA 4.15. *If p is a prime number dividing mn where m and n are integers, then p divides m or p divides n.*

PROOF. If p divides m then were are done. Otherwise $\gcd(p, m) = 1$, so p divides n by Lemma 4.11. □

THEOREM 4.16. *(Euclid) Every positive integer can uniquely be written as a product of prime numbers.*

PROOF. We already have seen in problem set 1 that every positive integer is a product of prime numbers. We still have to prove the uniqueness. Suppose that $p_1 < p_2 < \cdots < p_k$ are distinct prime numbers such that

$$p_1^{a_1} p_2^{a_2} \cdots p_k^{a_k} = p_1^{b_1} p_2^{b_2} \cdots p_k^{a_k}.$$

Suppose that $a_1 > b_1$. Then

$$p_1^{a_1 - b_1} p_2^{a_2} \cdots p_k^{a_k} = p_2^{b_2} \cdots p_k^{a_k}$$

and p_1 divides $p_2^{b_2} \cdots p_k^{a_k}$. This implies that p_1 divides p_i for some $i \geq 2$. This is impossible because the only divisors of p_i are 1 and p_i itself. Constradiction. Therefore $a_1 \leq b_1$. Similarly we see that $a_1 \geq b_1$ and therefore $a_1 = b_1$. Similarly we can prove that $a_i = b_i$ for $i = 2, 3, \ldots k$. □

Many properties can be expressed in terms of the prime factorization. Suppose that

$$A = p_1^{a_1} p_2^{a_2} \cdots p_k^{a_k}$$

and

$$B = p_1^{b_1} p_2^{b_2} \cdots p_k^{b_k}$$

are positive integers with their factorizations into prime numbers. Then A divides B if and only if $a_i \leq b_i$ for all $i = 1, 2, \ldots, k$. We also have that

$$\gcd(A, B) = p_1^{c_1} p_2^{c_2} \cdots p_k^{c_k}$$

where $c_i = \min(a_i, b_i)$ for all i.

THEOREM 4.17. *(Euclid) There are infinitely many prime numbers.*

PROOF. Suppose that there are finitely many distinct prime numbers, say $p_1, p_2, \ldots, p_k$. Let $N = p_1 p_2 \cdots p_k + 1$. Now N is a product of prime numbers. In particular there exists a prime numper q such that q divides N. Now $q = p_i$ for some i with $1 \leq i \leq k$. Since p_i divides N, we have that p_i divides

$$N - p_1 p_2 \cdots p_k = 1$$

which leads to a contradiction. □

EXAMPLE 4.18. The number $\sqrt{2}$ is irrational.

PROOF. Suppose taht $\sqrt{2}$ is rational, say $\sqrt{2} = p/q$ where p, q are positive integers. Squaring gives $p^2 = 2q^2$. The prime number 2 appears an even number of time in the prime factorization of p^2. On the other hand, 2 appears an odd number of times in the prime factorization of $2q^2$. Wet get a contradiction, so $\sqrt{2}$ has to be irrational. □

The distribution of prime numbers is quite mysterious. One of the most famous/notorious open problems in mathematics is the Riemann Hypothesis. This conjecture is closely related to the distribution of prime numbers. The following result is well-known but not so elementary:

THEOREM 4.19 (Dirichlet). *Suppose that a and b are positive integers that are relatively prime. Then there are infinitely prime numbers of the form $a + nb$ where n is a positive integer.*

3. Exercises

EXERCISE 4.1. ** Let $F_0, F_1, F_2, \ldots$ be the Fibonacci numbers: $F_0 = F_1 = 1$ and $F_{n+1} = F_n + F_{n-1}$ for all $n \geq 1$. Prove that the greatest common divisor of two consecutive Fibonnaci numbers is always equal to 1.

EXERCISE 4.2. *** Define $T_0, T_1, T_2, \ldots$ by $T_1 = 2$ and $T_{n+1} = T_n^2 - T_n + 1$ for $n \geq 0$. Prove that $\gcd(T_i, T_j) = 1$ for all $i \neq j$.

EXERCISE 4.3. **** Let $m \geq 2$ be an integer and suppose that a and b are positive integers. Prove that

$$\gcd(m^a - 1, m^b - 1) = m^{\gcd(a,b)} - 1.$$

EXERCISE 4.4. ** We have two drinking glasses. One glass can contain exactly 21oz. The other glass can contain exactly 13oz. Is it possible to measure exactly 1oz. of water using the two glasses?

EXERCISE 4.5. ** Suppose that

$$A = p_1^{a_1} p_2^{a_2} \cdots p_k^{a_k}$$

is an integer, $p_1 < p_2 < \cdots < p_k$ are distinct primes and $a_1, \ldots, a_k$ are nonnegative integers. Give a formula for the number of divisors of A.

EXERCISE 4.6. *** We start with a deck of 52 cards. We put all the cards in one row, face down. In the first round we turn all the cards around. In the second round we turn every second card around. In the third round we turn every third card around. We keep doing this until we complete round 52. Which cards will be faced up in the end?

EXERCISE 4.7. *** Suppose that $P(x) = a_n x^n + a_{n-1} x^{n-1} + \cdots + a_0$ is a nonconstant polynomial with integer coefficients. Prove that there exists a positive integer m such that $|P(m)|$ is not a prime number.

EXERCISE 4.8. ** Show that there are infinitely many prime numbers of the form $4k - 1$ where k is a positive integer (without using Dirichlet's Theorem).

EXERCISE 4.9. * Find all prime numbers p for which $p + 2$ and $p + 4$ are also prime numbers.

EXERCISE 4.10. **** Find all integers n for which $\phi(n)$ divides n.

EXERCISE 4.11. * Use Euclid's Algorithm to find $\gcd(1029, 791)$.

CHAPTER 5

Modular Arithmetic

1. The Chinese Remainder Theorem

Suppose that m is an integer. We say that a is congruent to b modulo m if m divides the difference $a - b$. The notation we use is

$$a \equiv b (\text{mod } m).$$

Notice that if $a_1 \equiv b_1 (\text{mod } m)$ and $a_2 \equiv b_2 (\text{mod } m)$ then

$$a_1 + a_2 \equiv b_1 + b_2 (\text{mod } m)$$

and

$$a_1 a_2 \equiv b_1 b_2 (\text{mod } m).$$

THEOREM 5.1 (Chinese Remainder Theorem). *Suppose that m and n are positive integers such that $\gcd(m, n) = 1$. Suppose that a and b are integers. Then there is a unique integer c with $0 \leq c < mn$ such that*

$$c \equiv a (\text{mod } m)$$

and

$$c \equiv b (\text{mod } n)$$

PROOF. We find can find integers $x, y \in \mathbb{Z}$ such that $xm + yn = 1$. Note that $xm \equiv 1 (\text{mod } n)$ and $yn \equiv 1 (\text{mod } m)$. Consider $d = bxm + ayn$. We can write $d = qmn + c$ with $0 \leq c < mn$. Then

$$c \equiv d \equiv ayn \equiv a (\text{mod } m)$$

and

$$c \equiv d \equiv bxm \equiv b (\text{mod } n).$$

This shows the existance of c. Suppose that c' is another integer with $c' \equiv a (\text{mod} m)$, $c \equiv b (\text{mod} n)$ and $0 \leq c' < mn$. Then $c - c'$ is divisible by m and by n. Because $\gcd(m, n) = 1$, $c - c'$ is divisible by mn. Since $|c - c'| < mn$ we must have that $c = c'$. □

The previous theorem easily can be generalized as follows.

THEOREM 5.2. *Suppose that $m_1, m_2, \ldots, m_k$ are pairwise relatively prime positive integers (so $\gcd(m_i, m_j) = 1$ for $i \neq j$). Suppose that $a_1, a_2, \ldots, a_k$ are integers. Then there is a unique integer c with $0 \leq c < m_1 m_2 \cdots m_k$ such that*

$$c \equiv a_i (\text{mod } m_i)$$

for $i = 1, 2, \ldots, k$.

EXAMPLE 5.3. Show that the difference of two consecutive prime numbers can be arbitrarily large.

We want to show that for every m there exists an n such that $n+1, n+2, \ldots, n+m$ are not prime. Let us assume that $n+1$ is divisible by 2 and that $n > 2$. Then $n+1$ is not a prime number. Now $n+2$ is not divisible by 2. However, we could assume that $n+2$ is divisible by 3 and $n+2 > 3$. Then $n+2$ is certainly not a prime either. Similarly we could assume that $n+3$ is divisible by 5 and $n+3 > 5$. The Chinese Remainder Theorem comes to the rescue.

PROOF. Let $p_1, p_2, \ldots, p_m$ be the first m prime numbers. Using the Chinese Remainder theorem we can find an integer c such that

$$n \equiv -i (\mathrm{mod} p_i)$$

for $i = 1, 2, \ldots, m$. Without loss of generality we may assume that $n > p_i$ for all i (otherwise we may add a multiple of $p_1 p_2 \cdots p_m$ to n). For every i in $\{1, 2, \ldots, m\}$ we see that p_i divides $n+i$ but $c+i > p_i$. This shows that $c+i$ is not a prime number. □

A slightly easier proof is the following.

PROOF. For every n, consider the numbers

$$n! + 2, n! + 3, \cdots, n! + n.$$

all these numbers are not prime numbers because $n! + i$ is divisible by i. □

2. Euler's function

For an integer n we define $\phi(n)$ as the number of elements in the set

$$\{a \in \mathbb{Z} \mid 1 \leq a \leq n,\ \gcd(a, n) = 1\}$$

of all positive integers a which are relatively prime to n.

LEMMA 5.4. *If m and n are positive integers then $\phi(mn) = \phi(m)\phi(n)$.*

PROOF. Given $c \in \{1, 2, \ldots, mn\}$ we can find unque $a \in \{1, 2, \ldots, n\}$ and $b \in \{1, 2, \ldots, m\}$ such that

$$c \equiv a (\mathrm{mod}\ n) \tag{30}$$

and

$$c \equiv b (\mathrm{mod}\ m). \tag{31}$$

Conversely, given $a \in \{1, 2 \ldots, n\}$ and $b \in \{1, 2, \ldots, m\}$ there exists a unique $c \in \{1, 2, \ldots, mn\}$ such that (30) and (31) hold by the Chinese remainder theorem. We have

$$\gcd(c, mn) = \gcd(c, m) \gcd(c, n) = \gcd(a, n) \gcd(b, m).$$

So $\gcd(c, mn) = 1$ if and only if $\gcd(a, n) = \gcd(b, m) = 1$. There are $\phi(n)$ choices for a such that $\gcd(a, n) = 1$. There are $\phi(m)$ choices for b such that $\gcd(a, m) = 1$. Therefore, there are $\phi(n)\phi(m)$ choices for a and b such that $\gcd(a, n) = \gcd(b, m) = 1$. So there are $\phi(m)\phi(n)$ choices for c such that $\gcd(c, nm) = 1$. This shows that $\phi(mn) = \phi(m)\phi(n)$. □

LEMMA 5.5. *If p is a prime number and k is a positive integer then*

$$\phi(p^k) = (p-1)p^{k-1}.$$

PROOF. The elements of

$$\{1, 2, 3, \ldots, p^k\}$$

that are not relatively prime to p^k are exactly the p^{k-1} multiples of p. This shows that

$$\phi(p^k) = p^k - p^{k-1} = (p-1)p^{k-1}.$$

□

In general if $n = p_1^{a_1} p_2^{a_2} \cdots p_k^{a_k}$ is the prime factorization of n, where $p_1 < p_2 < \cdots < p_k$ are distinct prime numbers and $a_1, a_2, \ldots, a_k$ are positive integers, then

$$\phi(n) = (p_1 - 1)p_1^{a_1-1}(p_2 - 1)p_2^{a_2-1} \cdots (p_k - 1)p_k^{a_k-1}.$$

3. Exercises

EXERCISE 5.1 (Gardner, M., *The Monkey and the Coconuts*, Ch. 9 in The Second Scientific American Book of Puzzles & Diversions: A New Selection. New York: Simon and Schuster, pp. 104-111, 1961.). *** Five sailors survive a shipwreck and swim to a tiny island where there is nothing but a coconut tree and a monkey. The sailors gather all the coconuts and put them in a big pile under the tree. Exhausted, they agree to go to wait until the next morning to divide up the coconuts.

At one o'clock in the morning, the first sailor wakes. He realizes that he can't trust the others, and decides to take his share now. He divides the coconuts into five equal piles, but there is one left over. He gives that coconut to the monkey, buries his coconuts, and puts the rest of the coconuts back under the tree.

At two o'clock, the second sailor wakes up. Not realizing that the first sailor has already taken his share, he too divides the coconuts up into five piles, leaving one over which he gives to the monkey. He then hides his share, and piles the remainder back under the tree.

At three, four and five o'clock in the morning, the third, fourth and fifth sailors each wake up and carry out the same actions.

In the morning, all the sailors wake up, and try to look innocent. No one makes a remark about the diminished pile of coconuts, and no one decides to be honest and admit that they've already taken their share. Instead, they divide the pile up into five piles, for the sixth time, and find that there is yet again one coconut left over, which they give to the monkey.

How many coconuts were there originally? (Find the smallest number of coconuts that is consistent with this story.)

EXERCISE 5.2. * Use the Extended Euclid's Algorithm to find integers $x, y \in \mathbb{Z}$ such that $268x + 421y = 1$.

EXERCISE 5.3. ** Find a multiple of 2003 that ends with the digits 9999.

EXERCISE 5.4. ** Find an integer x such that $x^2 + 1$ is divisible by 130.

CHAPTER 6

Polynomials

1. Introduction

In this problem set we will consider polynomials with coefficients in K, where K is the real numbers $\mathbb{R}$, the complex numbers $\mathbb{C}$, the rational numbers $\mathbb{Q}$ or any other *field*. (A field is a number system satisfying certain axioms, but if you have not heard about this before, just think of the examples we just mentioned.) A polynomial in the variable x with coefficients in K is an expression

$$f(x) = a_n x^n + a_{n-1}x^{n-1} + \cdots + a_1 x + a_0$$

with $a_0, a_1, a_2, \ldots, a_n \in K$. If $a_n \neq 0$ then f is said to have degree n. We may denote this by $\deg(f(x)) = n$. For convenience, we also define the degree of the zero polynomial 0 by $\deg(0) = -\infty$. The polynomial is called *monic* if $a_n = 1$. Now $K[x]$ denotes the set of all polynomials in the variable x with coefficients in K.

In many ways, polynomials behave similar to $\mathbb{Z}$ (this is because $K[x]$ and $\mathbb{Z}$ are both so-called *principal ideal domains*). As for the integers $\mathbb{Z}$, we can define gcd and lcm for polynomials. There also exists an Euclidean algorithm To prove these results for polynomials, one could simply copy the proofs for the same results for the integers.

Suppose that $f(x), g(x) \in K[x]$. First, we say that a polynomial g divides a polynomial f if $f(x) = g(x)h(x)$ for some polynomial $h \in K[x]$. A monic polynomial f is called *irreducible* if it has exactly 2 monic divisors (namely 1 and itself).

For example, $x^2+1 \in \mathbb{R}[x]$ is irreducible. Indeed if x^2+1 is a product of two polynomials of degree 1, then $x^2 + 1 = (x + a)(x + b)$ and $-a \in \mathbb{R}$ would be a zero of $x^2 + 1$ which is impossible. Seen as a polynomial with complex coefficients $x^2+1 \in \mathbb{C}[x]$ is reducible, namely $x^2 + 1 = (x + i)(x - i)$. The polynomial $x^2 - 2 \in \mathbb{Q}[x]$ is irreducible by a similar reasoning because $\sqrt{2}$ is irrational.

These monic irreducible polynomials play the role of prime numbers. For example every monic polynomial is a unique product of monic irreducible polynomials (as we will see).

Sometimes we will also consider polynomials in several variables. For example $K[x, y]$ denotes the polynomials in x and y with coefficients in K. These can be seen as polynomials in y with coefficients in $K[x]$, or polynomials in x with coefficients in $K[y]$.

2. Division with remainder

All polynomials considered have coefficients in K. We will develop a theory similar to the theory of integers.

THEOREM 6.1. *If $f(x), g(x)$ are polynomials and $g(x) \neq 0$, then there are unique polynomials $q(x)$ and $r(x)$ such that*

$$f(x) = q(x)g(x) + r(x)$$

with $\deg(r(x)) < \deg(g(x))$.

We will call $q(x)$ the *quotient* and $r(x)$ the remainder. Theorem 6.1 can be done explicitly using a long division just like you would do for integers. For example, let us divide $x^5 + 3x^3 + 2x - 1$ by $x^2 - x + 2$:

$$\begin{array}{llllllll} x^2-x+2/ & x^5 & & +3x^3 & & +2x & -1 & \backslash x^3+x^2+2x \\ & x^5 & -x^4 & +2x^3 & & & & \\ \hline & & x^4 & +x^3 & & & & \\ & & x^4 & -x^3 & +2x^2 & & & \\ \hline & & & 2x^3 & -2x^2 & +2x & & \\ & & & 2x^3 & -2x^2 & +4x & & \\ \hline & & & & & -2x & -1 & \end{array}$$

Therefore the quotient is $x^3 + x^2 + 2x$ and the remainder is $-2x - 1$ (You may have learned the long division slightly different. For example, it is a cultural thing where you put the quotient. Also, the horizontal bars weren't meant to be quite this long but I didn't figure it out how to do this in TEX properly.)

THEOREM 6.2. *Suppose that $f(x), g(x)$ are nonzero polynomials, and let $h(x)$ be a nonzero monic polynomial of smallest degree such that both $f(x)$ and $g(x)$ divide $h(x)$. This polynomial $h(x)$ is unique and we call it* $\operatorname{lcm}(f(x), g(x))$. *Moreover if $u(x)$ is any common multiple of $f(x)$ and $g(x)$ then* $\operatorname{lcm}(f(x), g(x))$ *divides $u(x)$.*

PROOF. If $u(x)$ is a common multiple of $f(x)$ and $g(x)$ then we can write $u(x) = q(x)h(x) + r(x)$ with $\deg(r(x)) < \deg(h(x))$ and $r(x)$ is a common multiple of $f(x)$ and $g(x)$. Now $r(x)$ cannot be nonzero by minimality of $\deg(h(x))$. Therefore $r(x) = 0$ and $h(x)$ divides $u(x)$. We now prove uniqueness of $h(x)$. If $v(x)$ were another nonzero monic polynomial with minimal degree such that $f(x)$ and $g(x)$ divide $v(x)$, then $h(x)$ must divide $v(x)$ and $v(x)$ must divide $h(x)$. Since both polynomials are monic, we get $h(x) = v(x)$. □

THEOREM 6.3. *If $f(x), g(x)$ are nonzero polynomials, then there is a nonzero monic polynomial $h(x)$ of largest degree such that $h(x)$ divides both $f(x)$ and $g(x)$. The polynomial $h(x)$ is unique and we call it* $\gcd(f(x), g(x))$. *Moreover, if $u(x)$ is any polynomial dividing both $f(x)$ and $g(x)$ then $u(x)$ divides* $\gcd(f(x), g(x))$.

PROOF. Define $h(x)$ as a nonzero polynomial of smallest possible degree such that it is of the form

$$a(x)f(x) + b(x)g(x)$$

for some polynomials $a(x)$ and $b(x)$. We may assume that $h(x)$ is monic by multiplying with a constant. Using division with remainder, we find $q(x)$ and $r(x)$ such that

$$f(x) = q(x)h(x) + r(x)$$

with $\deg(r(x)) < \deg(h(x))$. Now

$$r(x) = f(x) - q(x)(a(x)f(x) + b(x)g(x)) = (1 - q(x)a(x))f(x) + (-q(x)b(x))g(x).$$

Because of the minimality of the degree of $h(x)$, we must have $r(x) = 0$. This shows that $h(x)$ divides $f(x)$. In a similar way one can prove that $h(x)$ divides $g(x)$. If $u(x)$ is any polynomial dividing both $f(x)$ and $g(x)$ then $u(x)$ also divides $h(x) = a(x)f(x) + b(x)g(x)$. This also

shows immediately that $h(x)$ is a common divisor of $f(x)$ and $g(x)$ of largest possible degree. If $u(x)$ is another monic common divisor of $f(x)$ and $g(x)$ then $u(x)$ divides $h(x)$ and since both are monic of the same degree we get $u(x) = h(x)$. This shows the uniqueness. □

The previous proof shows in particular that for nonzero polynomials $f(x)$ and $g(x)$, there always exists polynomials $a(x)$ and $b(x)$ such that

$$\gcd(f(x), g(x)) = a(x)f(x) + b(x)g(x).$$

One could also define $\operatorname{lcm}(f(x), 0) = \operatorname{lcm}(0, f(x)) = 0$ and $\gcd(f(x), 0) = \gcd(0, f(x)) = f(x)$ for any polynomial $f(x)$.

3. Euclid's Algorithm

We can also compute the greatest common divisor of two nonzero polynomials $f(x)$ and $g(x)$ using the Euclidean algorithm. Let us assume that $\deg(f(x)) \geq \deg(g(x))$. Put $r_0(x) = f(x)$ and $r_1(x) = f(x)$. If $r_i(x) \neq 0$ then we define $r_{i+1}(x)$ and $q_i(x)$ inductively by

$$r_{i-1}(x) = q_i(x)r_i(x) + r_{i+1}(x)$$

where $q_i(x), r_{i+1}(x) \in K[x]$ and $\deg(r_{i+1}(x)) < \deg(r_i(x))$. Since $\deg(r_0(x)) > \deg(r_1(x)) > \cdots$ we must have $r_{k+1}(x) = 0$ for some k. So we have

$$\begin{aligned} r_0(x) &= q_1(x)r_1(x) + r_2(x) \\ r_1(x) &= q_2(x)r_2(x) + r_3(x) \\ \vdots &= \vdots \\ r_{k-2}(x) &= q_{k-1}(x)r_{k-1}(x) + r_k(x) \\ r_{k-1}(x) &= q_k(x)r_k(x) \end{aligned}$$

Up to a constant $r_k(x)$ is equal to $\gcd(f(x), g(x))$. All proofs are similar to the GCD algorithm for integers.

4. Chinese Remainder Theorem

Definition 6.4. If $a(x), b(x), f(x) \in K[x]$ are polynomials then we write

$$a(x) \equiv b(x) \bmod f(x)$$

if $f(x)$ divides the $a(x) - b(x)$.

We now can formulate a Chinese Remainder Theorem for polynomials.

Theorem 6.5 (Chinese Remainder Theorem). *If $f(x)$ and $g(x)$ are polynomials with $\gcd(f(x), g(x)) = 1$ and $a(x), b(x) \in K[x]$ are polynomials, then there exists a polynomial $c(x) \in K[x]$ with $\deg(c(x)) < \deg(f(x)) + \deg(g(x))$ such that*

$$c(x) \equiv a(x) \bmod f(x)$$

and

$$c(x) \equiv b(x) \bmod g(x)$$

5. Unique Factorization

Just as for the unique factorization into prime numbers, every polynomial has a unique factorization into irreducible polynomials.

THEOREM 6.6. *Every monic polynomial in $K[x]$ can be uniquely (up to permutation) written as a product of monic irreducible polynomials.*

6. The Fundamental Theorem of Algebra

THEOREM 6.7 (Fundamental Theorem of Algebra). *If $P(z) = z^n + a_{n-1}z^{n-1} + \cdots + a_1 z + a_0$ is a polynomial with complex coefficients $a_0, a_1, \ldots, a_{n-1}$, then*

$$P(z) = (z - x_1)(z - x_2)\cdots(z - x_n)$$

for some complex numbers $x_1, x_2, \ldots, x_n$. Here $x_1, x_2, \ldots, x_n$ are exactly the zeroes of $P(z)$, (some zeroes may appear several times, we call them multiple zeroes).

The fundamental theorem of algebra implies that the only irreducible monic polynomials over the complex numbers are of the form $z - a$, with $a \in \mathbb{C}$.

COROLLARY 6.8. *If $P(z) = z^n + a_{n-1}z^{n-1} + \cdots + a_1 z + a_0$ is a polynomial with real coefficients $a_0, a_1, \ldots, a_{n-1}$, then we can write*

$$P(z) = Q_1(z)Q_2(z)\cdots Q_r(z)$$

where $Q_i(z)$ is a monic polynomial of degree 1 or 2 for every i.

PROOF. It suffices to show that irreducible polynomials over $\mathbb{R}$ have degree 1 or 2. Suppose that $P(z)$ is an monic irreducible noncosntant polynomial. According the the previous theorem, there exists a complex root $a \in \mathbb{C}$. If a is real, then $P(z)$ is divisible by $z - a$ and we must have $P(z) = z - a$ because $P(z)$ is irreducible. If a is not real, then $P(\overline{a}) = 0$ as well, where $\overline{a}$ is the complex conjugate of a. Let $Q(z) = (z - a)(z - \overline{a}) = z^2 - (a + \overline{a})z + a\overline{a}$. The polynomial $Q(z)$ divides $P(z)$ and $Q(z)$ has real coefficients. Because $P(z)$ is irreducible, we have that $P(z) = Q(z)$. □

Suppose that $P(z)$ is a monic polynomial of degree n with zeroes $x_1, x_2, \cdots, x_n$. Then we have

$$P(z) = (z - x_1)(z - x_2)\cdots(z - x_n).$$

If we multiply this out we get

$$P(z) = z^n - e_1 z^{n-1} + e_2 z^{n-2} - \cdots + (-1)^n e_n$$

where

$$e_k = \sum_{1 \le i_1 < i_2 < \cdots < i_k \le n} x_{i_1} x_{i_2} \cdots x_{i_k}.$$

are called the *elementary symmetric polynomials*. In particular we have

$$e_1 = x_1 + x_2 + \cdots + x_n$$

which is the sum of all zeroes,

$$e_2 = x_1x_2 + x_1x_3 + \cdots + x_1x_n + x_2x_3 + x_2x_4 + \cdots + x_2x_n + \cdots + x_{n-1}x_n.$$

which is the sum of all products of distinct variables, and

$$e_n = x_1 x_2 \cdots x_n$$

which is just the product of all variables. You probably know the case $n = 2$. In that case we get $P(z) = (z - x_1)(z - x_2) = z^2 - (x_1 + x_2)z + x_1 x_2$, so $s_1 = x_1 + x_2$ and $s_2 = x_1 x_2$.

A polynomial $Q(x_1, x_2, \ldots, x_n)$ in the variables $x_1, x_2, \ldots, x_n$ is called *symmetric* if

$$Q(x_1, \ldots, x_n) = Q(x_{\sigma(1)}, \ldots, x_{\sigma(2)})$$

if $\sigma(1), \sigma(2), \ldots, \sigma(n)$ is a permutation of $1, 2, \ldots, n$. The *elementary symmetric polynomials* are of course symmetric. Other important symmetric polynomials are the power sums:

$$p_k = x_1^k + x_2^k + \cdots + x_n^k.$$

7. Exercises

EXERCISE 6.1. ** Show that

$$p_{n+k} - e_1 p_{n+k-1} + e_2 p_{n+k-2} - \cdots + (-1)^n e_n p_k = 0.$$

EXERCISE 6.2. * Show that $e_2 = (p_1^2 - p_2)/2$, and $e_3 = (p_1^3 - 3p_1 p_2 + 2p_3)/6$.

EXERCISE 6.3. ** Suppose that $P(z) = z^n + a_{n-1} z^{n-1} + \cdots + a_0$ is a polynomial with n distinct real zeroes, $x_1, x_2, \cdots, x_n$. Express

$$\frac{1}{x_1} + \frac{1}{x_2} + \cdots + \frac{1}{x_n}$$

in terms of $a_0, a_1, \ldots, a_{n-1}$.

EXERCISE 6.4. *** Suppose that x_1, x_2, x_3 are complex numbers with

$$x_1 + x_2 + x_3 = x_1^2 + x_2^2 + x_3^2 = x_1^3 + x_2^3 + x_3^3 = 10.$$

What is $x_1^4 + x_2^4 + x_3^4$? (*Hint:* Use problem 6.1 and problem 6.2.)

EXERCISE 6.5. **** Show that we have equality of *formal* power series

$$\sum_{k=1}^{\infty} \frac{(e_1 z - e_2 z^2 + e_3 z^3 - \cdots + (-1)^{n-1} e_n z^n)^k}{k} = p_1 z + \frac{p_2}{2} z^2 + \frac{p_3}{3} z^3 + \cdots .$$

EXERCISE 6.6. *** Suppose that $|z| < 1$. Show that

$$\prod_{n=1}^{\infty} \frac{1}{(1 - z^{2n-1})} = \prod_{n=1}^{\infty} (1 + z^n).$$

EXERCISE 6.7. (Polya's Theorem)***** If $P(z) = z^n + a_{n-1} z^{n-1} + \cdots + a_0$ is a polynomial with real coefficients, such that $P(z) > 0$ for $z > 0$. Prove that $(1+z)^n P(z)$ has nonnegative coefficients. (For example, $1 - 3z + 3z^2 > 0$ for all $z > 0$, and

$$(1+z)^{13}(1 - 3z + 3z^2) = 1 + 10z + 42z^2 + 91z^3 + 91z^4 +$$

$$+1287z^8 + 429z^7 + 2002z^9 + 2002z^{10} + 1365z^{11} + 637z^{12} + 196z^{13} + 36z^{14} + 3z^{15}$$

has nonnegative coefficients. By the way, 13 was the smallest power with this property here. *Hint:* Use the fundamental theorem of algebra for polynomials with real coefficients.)

EXERCISE 6.8. *** A polynomial $P(z)$ with real coefficients of degree n starts with

$$az^n + bz^{n-1} + cz^{n-2} + \cdots$$

Show that if $P(z)$ cannot have n real zeroes if $b^2 - 2ac < 0$. Also show that there exists a polynomial $P(z)$ with n real zeroes for which $b^2 - 4ac < 0$.

EXERCISE 6.9. * A polynomial $P(z) = a_n z^n + a_{n-1} z^{n-1} + \cdots + a_1 z + a_0$ is called symmetric if $a_i = a_{n-i}$ for all i. (Assume that $a_n \neq 0$.) Prove that for a symmetric polynomial $P(z)$ we have that x is a zero of $P(z)$ if and only if $1/x$ is a zero of $P(z)$.

EXERCISE 6.10. ** Find all zeroes of the (symmetric) polynomial

$$P(z) = z^4 + 10z^3 + 23z^2 + 10z + 1.$$

(*Hint:* first prove that there exists a factorization $P(z) = (z^2 + az + 1)(z^2 + bz + 1)$ using the previous problem.)

EXERCISE 6.11. **

(a) Prove Theorem 6.1 (for example by induction with respect to $\deg(f(x))$).
(b) Suppose that $f(x)$ is a polynomial with coefficients in K and $f(a) = 0$ for some $a \in K$. Prove that you can write $f(x) = (x - a)q(x)$ for some polynomial $q(x) \in K[x]$.
(c) Use this to show that a nonzero polynomial of degree n has at most n zeroes.

EXERCISE 6.12. *** Find all polynomials (with real coefficients) $f(x)$ such that

$$f(x^2) = (f(x))^2.$$

EXERCISE 6.13. ** If $f(x)$ is a polynomial, prove that we can write

$$f(x) - f(y) = a(x, y)(x - y)$$

where $a(x, y)$ is a polynomial in two variables. (*Hint: Reduce to the case* $f(x) = x^n$.)

EXERCISE 6.14. * Suppose that $f(x)$ is a polynomial with integer coefficients, and that a, b are integers. Show that $f(a) - f(b)$ is divisible by $a - b$. In particular, if $a \equiv b \bmod n$ for some integer n, then $f(a) \equiv f(b) \bmod n$.

EXERCISE 6.15. *** Let $P(x)$ be a polynomial with integer coefficients. Prove: There do not exist three distinct integers a, b, c such that $P(a) = b$, $P(b) = c$ and $P(c) = a$.

EXERCISE 6.16. *** Find a polynomial $P(x, y, z, t)$ (with real coefficients) such that $P(2, 0, 0, 1) = 2001$, but $P(a, b, c, d) = 0$ for all other quadruples of integers with $0 \leq a, b, c, d \leq 9$.

EXERCISE 6.17. ***

(a) Prove the identity

$$\cos(nx) = 2\cos(x)\cos((n-1)x) - \cos((n-2)x)$$

for natural numbers n and $x \in \mathbb{R}$.
(b) Prove that for every natural number n there exists a polynomial $T_n(x)$ of degree n such that $T_n(\cos(x)) = \cos(nx)$. (These polynomials $T_n(x)$ are called *Chebychev Polynomials*).

(c) Prove that $|T_n(x)| \leq 1$ for $|x| \leq 1$ and that the leading coefficient of $T_n(x)$ is 2^{n-1} (i.e., $T_n(x) = 2^{n-1}x^n + \dots$).

EXERCISE 6.18. ***** Suppose that $P(x) = a_n x^n + a_{n-1}x^{n-1} + \cdots + a_0$ is a polynomial of degree n and $|P(x)| \leq 1$ for $|x| \leq 1$. Prove that $|a_n| \leq 2^{n-1}$. (*Hint: You may use the results of the previous problem. If $|a_n| > 2^{n-1}$, then show that $T_n(x) - \frac{2^{n-1}}{a_n}P(x)$ is a polynomial of degree $n-1$ with at least n zeroes.*)

EXERCISE 6.19. ***** Suppose

$$f(x) - f(y) = a(x,y)(g(x) - g(y))$$

for some polynomials $f(x)$ and $g(x)$ and a polynomial $a(x,y)$ in two variables. Prove that there exists a polynomial h such that $f(x) = h(g(x))$.

EXERCISE 6.20 (Putnam 1986, A6). ***** Let $a_1, a_2, \dots, a_n$ be real numbers, and let $b_1, b_2, \dots, b_n$ be distinct positive integers. Suppose that there is a polynomial $f(x)$ satisfying the identity

$$(1-x)^n f(x) = 1 + \sum_{i=1}^{n} a_i x^{b_i}.$$

Find a simple expression (not involving any sums) for $f(1)$ in terms of $b_1, b_2, \dots, b_n$ and n (but independent of $a_1, a_2, \dots, a_n$.)

EXERCISE 6.21 (Putnam). ***** Let $f(x)$ be a polynomial with integer coefficients. Define a sequence $a_0, a_1, \dots$ of integers such that $a_0 = 0$ and $a_{n+1} = f(a_n)$ for all $n \geq 0$. Prove that if there exists a positive integer m for which $a_m = 0$, then either $a_1 = 0$ or $a_2 = 0$.

EXERCISE 6.22. *****(Gauss' Lemma)

(1) If $f(x) = a_n x^n + a_{n-1}x^{n-1} + \cdots + a_0$ is a polynomial with integer coefficients, then the *content* $c(f(x))$ of $f(x)$ is defined as $\gcd(a_n, a_{n-1}, \dots, a_0)$. Prove that $c(f(x)g(x)) = c(f(x))c(g(x))$ if $f(x)$ and $g(x)$ are polynomials with integer coefficients. (*Hint: Reduce to the case that $c(f(x)) = c(g(x)) = 1$. Then reduce the polynomials modulo some prime numbers and see what happens.*)
(2) If $f(x)$ is a polynomial with integer coefficients and $f(x) = a(x)b(x)$ with $a(x)$ and $b(x)$ nonconstant polynomials with rational coefficients, then one can find polynomials $\widetilde{a}(x)$ and $\widetilde{b}(x)$ with *integer* coefficients such that $f(x) = \widetilde{a}(x)\widetilde{b}(x)$. (In other words, $f(x)$ is reducible over $\mathbb{Q}$ if and only if $f(x)$ is reducible of $\mathbb{Z}$.)

EXERCISE 6.23. ***(Interpolation) Suppose that $a_1, a_2, \dots, a_n \in \mathbb{R}$ are distinct and that $b_1, b_2, \dots, b_n \in \mathbb{R}$. Prove that there exists a polynomial $f(x)$ with real coefficients such that $f(a_i) = b_i$ and f has degree at most $n-1$. (*Hint: For $i = 1, 2, 3, \dots, n$ define a polynomial f_i such that $f_i(a_j) = 0$ for all $j \neq i$ and $f_i(a_i) = b_i$. Then define $f = \sum_i f_i$.*)

EXERCISE 6.24. ***** Prove the Eisenstein criterion. If $f(x) = a_n x^n + a_{n-1}x^{n-1} + \cdots + a_1 x + a_0$ is a polynomial with integer coefficients, and p is a prime number such that p divides $a_1, a_2, \dots, a_{n-1}$, p does not divide a_n and p^2 does not divide a_0. Then $f(x)$ is irreducible over $\mathbb{Q}$ (it suffices to show, using the previous problem, that it is impossible to write $f(x)$ as a product of two nonconstant polynomials with integer coefficients).

EXERCISE 6.25 (Putnam 1985, B2). *** Let k be the smallest positive integer for which there exist distinct integers m_1, m_2, m_3, m_4, m_5 such that the polynomial

$$p(x) = (x - m_1)(x - m_2)(x - m_3)(x - m_4)(x - m_5)$$

has exactly k nonzero coefficients. Find, with proof, a set of integers m_1, m_2, m_3, m_4, m_5 for which this minimum k is achieved.

EXERCISE 6.26 (Putnam 1985, A4). **** Define a sequence $\{a_i\}$ by $a_1 = 3$ and $a_{i+1} = 3^{a_i}$ for $i \geq 1$. Which itnegers between 00 and 99 inclusive occur as the last two digits in the decimal expansion of infinitely many a_i?

EXERCISE 6.27. * What are the quotient and the remainder of division of $x^7 + x^5 - x^4 + 2x^3 + 4x^2 - 1$ by $x^3 + x^2 - x + 1$?

CHAPTER 7

Pigeonhole Principle

The pigeonhole principle is the following observation:

THEOREM 7.1. *Suppose that $> kn$ marbles are distributed over n jars, then one jar will contain at least $\geq k+1$ marbles.*

(It can also be formulated in terms of pigeons and pigeonholes, hence the name.) The proof of this pigeonhole principle is easy. It is more difficult to know when to apply it. There are many surprising applications of the pigeonhole principle. The pigeonhole principle was first explicitly formulated by the mathematician Dirichlet (1805–1859).

The pigeonhole principle says for example that at least two people in New York City will have the same number of hairs on their head. This is because humans have $< 1,000,000$ hairs and there are $> 1,000,000$ people in NYC.

The pigeonhole principle is particularly powerful in existence proofs which are not constructive. For example in the previous example we proved the existence of two people with the same number of hairs without specifically identifying these two individuals.

EXAMPLE 7.2. How many bishops can one put on an 8×8 chessboard such that no two bishops can hit each other.

It seems like a good idea to put 8 bishops in one row at the edge of the board. If we put 6 bishops on these positions then we see that still no two bishops can hit each other. So we see that at least 14 bishops can be put on the chessboard. We conjecture that this number is maximal.

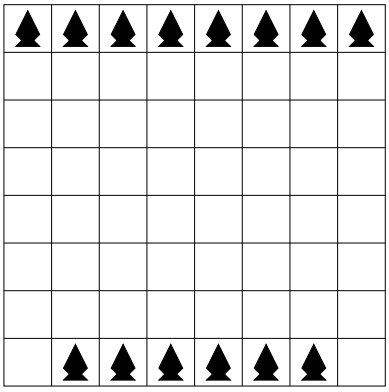
How can we prove that 14 is the maximal number of bishops? We can use the pigeonhole principle. We need to partition the $8 \times 8 = 64$ fields into 14 sets such that whenever two bishops are on fields which lie in the same set, then they can hit each other.

Note that a bishop on a black field only can move to other black fields. A bishop on a white field can only move to other white fields. To prove that 14 is the maximal number of bishops, we could prove that there at most 7 "black" bishops and at most 7 "white" bishops. We try to partition the 32 black fields into 7 sets such that if two bishops are on fields in the same set, then they can hit each other. We see that the following configuration works:

	1		2		3		4
1		2		3		4	
	2		3		4		5
2		3		4		5	
	3		4		5		6
3		4		5		6	
	4		5		6		7
4		5		6		7	

A similar configuration works for the white fields. (Take the mirror image.) In the proof that we are going to write down, we do not need to distinguish between "black" and "white" bishops. We can combine the partition of black fields and the partition of the white fields to get a partition of the set of all 64 fields into 14 subsets.

PROOF. The answer is 14. Place 14 bishops on the chessboard as follows:



Then no two bishops can hit each other.
Let us label the fields on the chessboard as follows:

11	1	10	2	9	3	8	4
1	11	2	10	3	9	4	8
12	2	11	3	10	4	9	5
2	12	3	11	4	10	5	9
13	3	12	4	11	5	10	6
3	13	4	12	5	11	6	10
14	4	13	5	12	6	11	7
4	14	5	13	6	12	7	11

Whenever two bishops are placed on the chessboard with the same number, they can hit each other. If a number of bishops are placed on fields of the chessboard such that no

two can hit each other, then all the numbers of the fields are distinct. This shows that the number of bishops is at most 14. □

EXAMPLE 7.3. (Putnam 1958) Let S be a subset of $\{1, 2, 3, \ldots, 2n\}$ with $n+1$ elements. Show that one can choose distinct elements $a, b \in S$ such that a divides b.

Is the $n+1$ in the problem sharp? Suppose that S has the property that for every pair of distinct $a, b \in S$, a does not divide b and b does not divide a. How many elements can S have?

If S contains 1 then it could not contain any other element. If S contains 2 then all other even numbers are excluded. In order to get S as large as possible, it seems that one should choose large elements. If we take the n largest elements, $S = \{n+1, n+2, \ldots, 2n\}$ then clearly no two distinct elements divide each other. Any positive integer a with $a \leq n$ divides an element of S. This shows that S is maximal with the desired property.

The problem has somewhat of a pigeonhole flavor: We are asked to prove the existence of certain elements $a, b \in S$ but it seems unlikely that we can explicitly construct these elements.

How can we apply the pigeon hole principle? Since we have $n+1$ elements we partition $\{1, 2, \ldots, 2n\}$ into n sets $T_1, T_2, \ldots, T_n$. The pigeonhole principle says that $S \cap T_i$ contains at least two elements for some i. This then should be useful to conclude that there exist $a, b \in S$ such that a divides b. So we would like T_i to have the following property: Whenever $a, b \in T_i$ with $a < b$ then a divides b. So T_i should be of the form

$$\{a_1, a_2, a_3, \ldots, a_k\}$$

with $a_1 \mid a_2 \mid a_3 \mid \cdots \mid a_k$. The largest such set is

$$\{1, 2, 2^2, 2^3, \ldots\}.$$

Let us define T_1 to be this set. The smallest element not in T_1 is 3. So let us define

$$T_2 = \{3, 3 \cdot 2, 3 \cdot 2^2, 3 \cdot 2^3, \ldots\}.$$

The smallest element, not in T_1 and T_2 is 5. so let us define

$$T_3 = \{5, 5 \cdot 2, 5 \cdot 2^2, 5 \cdot 2^3, \ldots\}.$$

Let us define more generally

$$T_k = \{(2k-1), (2k-1) \cdot 2, (2k-1) \cdot 2^2, (2k-1) \cdot 2^3, \ldots\}$$

for $k = 1, 2, \ldots, n$. It is easy to see that the union of $T_1, T_2, \ldots, T_n$ contains. $\{1, 2, \ldots, 2n\}$. We are now ready to write down the proof, using the pigeonhole principle.

PROOF. Let us define

$$T_k = \{1, 2, \ldots, 2n\} \cap \{(2k-1), (2k-1) \cdot 2, (2k-1) \cdot 2^2, (2k-1) \cdot 2^3, \ldots\}$$

for all $k = 1, 2, \ldots, n$. Every $c \in \{1, 2, \ldots, 2n\}$ can uniquely be written as $c = 2^j(2i-1)$ with $j \in \mathbb{N}$ and $i \in \{1, 2, \ldots, n\}$. This shows $T_1, T_2, \ldots, T_n$ is a partition of $\{1, 2, \ldots, 2n\}$. By the pigeon hole principle, $S \cap T_i$ contains at least two distinct elements for some i, say $\{a, b\} \subset S \cap T_i$ with $a < b$. then $a = 2^j(2i-1)$ and $b = 2^k(2i-1)$ for some $j, k \in \mathbb{N}$ with $j < k$ and it is clear that $a \mid b$. □

EXAMPLE 7.4. Suppose that S is a set of n integers. Show that one can choose a nonempty subset T of S such that the sum of all elements of T is divisible by n.

One can try to attack this problem using the pigeonhole principle but it is not immediately clear how we can apply it. What are the "pigeonholes" here? Since our goal is to prove that something is divisible by n, it is natural to take the congruence classes modulo n as pigeonholes. The pigeonhole principle says: "Given $n+1$ integers, one can choose two of them such that their difference is divisible by n." How can we apply this here? We can apply it if we have integers $a_1, a_2, \ldots, a_{n+1}$ such that $a_j - a_i$ is a sum of distinct elements of S for all $i < j$. We can indeed achieve this. Suppose that $S = \{b_1, b_2, \ldots, b_n\}$. Take $a_1 = 0$, $a_2 = b_1$, $a_3 = b_1 + b_2$, $a_4 = b_1 + b_2 + b_3$, etc. We can write down our proof:

PROOF. Suppose that $S = \{b_1, b_2, \ldots, b_n\}$. Define

$$c_i = b_1 + b_2 + \cdots + b_i$$

for all $i = 0, 1, \ldots, n$ ($c_0 = 0$). Of the $n + 1$ numbers $c_0, c_1, \ldots, c_n$, at least 2 must lie in the same congruence class module n by the pigeonhole principle. Assume that we have $c_i \equiv c_j (\mathrm{mod} n)$ for $i < j$. Then we get that

$$c_j - c_i = b_{i+1} + b_{i+2} + \cdots + b_j$$

is divisible by n. □

EXAMPLE 7.5. Suppose that we are given a sequence of $nm + 1$ distinct real numbers. Prove that there is an increasing subsequence of length $n+1$ or a decreasing subsequence of length $m + 1$.

To get an idea, let us do a random example with $n = m = 3$:

$$55, 63, 57, 60, 74, 85, 16, 61, 7, 49. \tag{32}$$

What is the longest increasing subsequence and what is the longest decreasing subsequence? How can we efficiently find these without checking all possible subsequences?

For a longest decreasing sequence in (32) there are two cases. Either such a sequence ends with 49 or it does not. If the sequence does not contain 49, then a longest decreasing sequence of (32) is a longest decreasing subsequence of the shortened sequence

$$55, 63, 57, 60, 74, 85, 16, 61, 7. \tag{33}$$

If 49 appears in a longest decreasing subsequence, then we may wonder what the previous element in that subsequence is. Is it 55,63,57,60,74,85 or 61? (Clearly 16 and 7 are out of the question because the subsequence is decreasing.) It would now be useful to know for each x in $\{55, 63, 57, 60, 74, 85, 61\}$ what the longest decreasing subsequence is of (33) that ends with x. We then could take the longest decreasing subsequence of (33) ending with some x in $\{55, 63, 57, 60, 74, 85, 61\}$ and add 49 at the end to obtain a longest decreasing subsequence of (32).

So to find the longest decreasing subsequence of (32) we need to find the longest decreasing subsequence of (32) ending with x for $x = 55, 63, \ldots, 49$ (in that order).

x	a longest decreasing subsequence ending with x
55	55
63	63
57	63, 57
60	63, 60
74	74
85	85
16	63, 60, 16
61	85, 61
7	63, 60, 16, 7
49	85, 61, 49

We have found that the longest decreasing subsequence has length 4. Namely the subsequence 63,60,16,7 is decreasing. So the statement we want to prove works out in this example. Let us determine the longest increasing sequence:

x	a longest decreasing subsequence ending with x
55	55
63	55, 63
57	55, 57
60	55, 57, 60
74	55, 57, 60, 74
85	55, 57, 60, 74, 85
16	16
61	55, 57, 60, 61
7	7
49	7, 49

We see that there even is an increasing sequence of length 5.

We checked one (small) example and it seems that we are still far from a solution (but this is actually not the case).

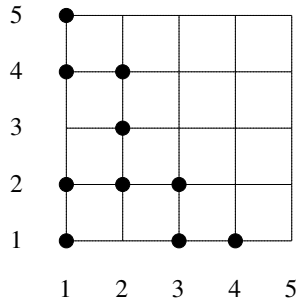
We are interested in the lengths of maximal increasing/decreasing sequences. So let us make a table containing the length of a longest increasing sequence ending in x and the

length of a longest decreasing sequence ending in x for all x.

x	decreasing	increasing
55	1	1
63	1	2
57	2	2
60	2	3
74	1	4
85	1	5
16	3	1
61	2	4
7	4	1
49	3	2

Let us plot the last two columns against each other. We get 10 *distinct* points

$$(1,1),(1,2),(2,2),(2,3),(1,4),(1,5),(3,1),(2,4),(4,1),(3,2).$$



If there were no increasing or decreasing sequence of length 4, then all points would fit in a 3×3 box and two of the points would have to coincide by the pigeonhole principle. This leads to a contradiction as the following proof shows.

PROOF. Suppose that

$$x_1, x_2, \ldots, x_{mn+1}$$

is a sequence of distinct real numbers. Let a_i be the length of the longest decreasing subsequence ending with x_i. Let b_i be the length of the longest increasing subsequence ending with x_i. We claim that if $i \neq j$, then that $(a_i, b_i) \neq (a_j, b_j)$.

Indeed, if $x_j < x_j$ then we can take a longest decreasing subsequence ending with x_i and add x_j at the end. This way we obtain a decreasing subsequence ending with x_j of length $a_i + 1$. This shows that $a_j > a_i$ and $(a_i, b_i) \neq (a_j, b_j)$.

If $x_j > x_i$ then we can take a longest increasing subsequence ending with x_i and add x_j at the end. This shows that $b_j > b_i$ and $(a_i, b_i) \neq (a_j, b_j)$.

There are only nm pairs (a, b) with $a, b \in \mathbb{Z}$ and $1 \leq a \leq m$ and $1 \leq b \leq n$. We must have $a_i > m$ or $b_i > n$ for some i. □

1. Diophantine Approximation

EXAMPLE 7.6. Suppose that α is a real number and that N is a positive integer. Show that one of the numbers $\alpha, 2\alpha, 3\alpha, \ldots, N\alpha$ differs at most $\frac{1}{N}$ from an integer.

It is not so clear a priori how one can use the pigeonhole priciple in this problem. Since we are only interested in the value $i\alpha$ modulo the integers, we define $\beta_i = i\alpha - \lfloor i\alpha \rfloor$. ($\lfloor x \rfloor$ is the largest integer $\leq x$.) We observe that $0 \leq \beta_i < 1$ for all i. We want to show that $\beta_i \leq \frac{1}{N}$ or $\beta_i \geq 1 - \frac{1}{N}$ for some i.

An important observation is that $\beta_{i+j} - \beta_i$ is the same as α_j up to an integer for all i. So if β_{i+j} is very close to β_i then α_j is very close to an integer. We want to show that one can choose two of the $N+1$ numbers $\beta_0 = 0, \beta_1, \beta_2, \ldots, \beta_n$ that are at most of distance $\frac{1}{N}$ of each other.

Here is where the pigeonhole principle might come in. We need to partition the interval $[0,1\rangle$ into N sets, such that every two elements in the same set are at most $\frac{1}{N}$ apart. This is possible. We can take $S_k = [\frac{k-1}{N}, \frac{k}{N}\rangle$ for $k = 1, 2, \ldots, N$. By the pigeon hole principle at least two of the numbers in $\beta_0, \beta_1, \ldots, \beta_N$ lie in the same set S_k. Let us write down a more formal proof.

PROOF. Define

$$\beta_i = i\alpha - \lfloor i\alpha \rfloor$$

for $i = 0, 1, 2, \ldots, N$. Then $0 \leq \beta_i < 1$ for all i. Define $S_k = [\frac{k-1}{N}, \frac{k}{N}\rangle$ for $k = 1, 2, \ldots, N$. The interval $[0,1\rangle$ is the union of intervals $S_1, S_2, \ldots, S_N$. By the pigeon hole principle, at least two of the numbers $\beta_0, \beta_1, \ldots, \beta_N$ lie in the same interval S_k for some k. Say $\beta_i, \beta_j \in S_k$ for some i, j with $0 \leq i < j \leq N$. But then

$$-\frac{1}{N} \leq \beta_j - \beta_i = (j-i)\alpha - (\lfloor j\alpha \rfloor - \lfloor i\alpha \rfloor) \leq \frac{1}{N}.$$

We are done because $1 \leq j - i \leq N$ and $\lfloor j\alpha \rfloor - \lfloor i\alpha \rfloor$ is an integer. □

diophantine approximation is an area of number theory where one likes to approximate irrational numbers by rational number. The previous example allows us to characterize irrational numbers!

THEOREM 7.7. *A real number α is irrational if and only if there exists a sequences of integers $p_1, p_2, \ldots$ and $q_1, q_2, \ldots$ such that*

$$\lim_{n\to\infty} q_n\alpha - p_n = 0$$

and $q_n\alpha - p_n \neq 0$ for all n.

PROOF. Suppose that α is irrational. For every n, we can find integers p_n, q_n with $1 \leq q_n \leq n$ such that $|q_n\alpha - p_n| < \frac{1}{n}$. It follows that

$$\lim_{n\to\infty} q_n\alpha - p_n = 0.$$

Obviously $q_n\alpha - p_n \neq 0$ for all n because α is irrational.

Conversely, suppose that $q_n\alpha - p_n \neq 0$ for all n and $\lim_{n\to\infty} q_n\alpha - p_n = 0$. Assume that α is rational, say $\alpha = \frac{a}{b}$ with $a, b \in \mathbb{Z}$ and $b > 0$. Now we have

$$|q_n\alpha - p_n| = \left| \frac{q_n a - p_n b}{b} \right| \geq \frac{1}{b}$$

because $q_n\alpha - p_n \neq 0$. This leads to a contradiction with $\lim_{n\to\infty} q_n\alpha - p_n = 0$. □

We can apply this:

THEOREM 7.8. *The number $\sqrt{2}$ is irrational.*

PROOF. Expanding $(\sqrt{2}-1)^n$ and using $(\sqrt{2})^2 = 2$ we get

$$(\sqrt{2}-1)^n = q_n\sqrt{2} - p_n$$

for some integers p_n and q_n. We have

$$\lim_{n\to\infty} q_n\sqrt{2} - p_n = \lim_{n\to\infty} (\sqrt{2}-1)^n = 0$$

because $|\sqrt{2}-1| < 1$. Also

$$q_n\sqrt{2} - p_n = (\sqrt{2}-1)^n \neq 0$$

for all n because $\sqrt{2} \neq 1$. This proves that $\sqrt{2}$ is irrational. □

2. balls

For a finite set S we denote the number of elements of S by $|S|$. The pigeonhole principle can be reformulated as:

THEOREM 7.9. *If $S_1, S_2, \ldots, S_n$ are subsets of a finite set T and*

$$|S_1| + |S_2| + \cdots + |S_n| > k|T|$$

then there exists an element $x \in T$ that lies in at least $k+1$ of the sets $S_1, S_2, \ldots, S_n$.

If S is a measurable set in $\mathbb{R}^3$, let $\mu(S)$ be its volume. We have the following variation of the previous theorem.

THEOREM 7.10. *If $S_1, S_2, \ldots, S_n$ are measurable subsets of a measurable set T, and*

$$\mu(S_1) + \mu(S_2) + \cdots \mu(S_n) > k\mu(T).$$

then there exists an element $x \in T$ that lies in at least $k+1$ of the sets $S_1, S_2, \ldots, S_n$.

EXAMPLE 7.11. Let S be a set of points in the cube $[0,1] \times [0,1] \times [0,1]$ (in $\mathbb{R}^3$). Such that the distance between every two distinct elements $x, y \in S$ is at least 0.1. Give an upper bound for the number of elements of S.

We could use the pigeonhole principle as follows. Partition the cube into small regions, such that in each region the maximal distance between two points in this region is < 0.1. For example, we could partition the cube into $N \times N \times N$ little cubes of sidelength $\frac{1}{N}$. The maximum distance between two points in this little cube is $\sqrt{3}/N$, the length of its diagonal. We need that $\sqrt{3}/N < 0.1$, so $N > 10\sqrt{3} \approx 17.32$. (Without a calculator we see that $10\sqrt{3} < 18$ because $18^2 = 324 > 300 = (10\sqrt{3})^2$.) So let us take $N = 18$. Each of the $N \times N \times N$ cubes can contain at most 1 element of S. Therefore, the cardinality of S is at most $18^3 = 324 \cdot 18 = 5832$.

There is another way of looking at this problem. Instead of saying that two points x and y have distance at least 0.1, we could say that the balls with radius 0.05 around x and around y are disjoint. Note that all balls lie within the cube $[-0.05, 1.05] \times [-0.05, 1.05] \times [-0.05, 1.05]$ with volume $1.1^3 = 1.331$. We can reformulate the problem as the problem of packing oranges of diameter 0.1 into a (cube-shaped) box of sidelength 1.1. The volume of a ball with radius

0.05 is $\frac{4}{3}\pi(0.05)^3 \approx 0.00523599$ (we are using a calculator now). The number of oranges is at most

$$\frac{(1.1)^3}{\frac{4}{3}\pi(0.05)^3} = \frac{3 \cdot 22^3}{4\pi} = \frac{7986}{\pi} \approx 2542.02.$$

This means that S has at most 2542 points. This is quite an improvement.

Johannes Kepler (1571–1630) conjectured in 1611 that the densest way of packing balls in $\mathbb{R}^3$ is the cubic or hexagonal packing (well-known to people selling oranges). These packing give a density of

$$\frac{\pi}{3\sqrt{2}} \approx 74.048\%.$$

Kepler's conjecture was proven by Thomas Hales (U of M!) in 1998.

Using this result, we see that S can have at most

$$\frac{\pi}{3\sqrt{2}} \frac{7986}{\pi} = 1331\sqrt{2} \approx 1882.3183.$$

So S can have at most 1882 elements. (We do not claim here that this number is sharp.)

EXAMPLE 7.12. A binary word of length n is a sequence of 0's and 1's of length n. The set $\{0,1\}^n$ is the set of all binary words of length n. Let S be a subset of $\{0,1\}^n$ with the following property: for every pair of distinct elements $x = x_1x_2\cdots x_n$ and $y = y_1y_2\cdots y_n$ we have that x and y differ in at least 3 positions. Show that S has at most

$$\frac{2^n}{n+1}$$

elements.

PROOF. We can use the ideas in the previous example. The *distance* $d(x,y)$ between two words $x = x_1x_2\cdots x_n$ and $y = y_1y_2\cdots y_n$ is the number of positions where they differ. For any binary word $x \in \{0,1\}^n$, let $B(x)$ be the *ball with radius 1*, so

$$B(x) = \{z \in \{0,1\}^n \mid d(x,z) \leq 1\}.$$

In other words $B(x)$ is the set of all binary words of length n which differ from x in at most 1 position. The number of elements of $B(x)$ is $n+1$ (namely x itself and all words obtained by changing x at on position). Notice now that $d(x,y) \geq 3$ is equivalent with $B(x)$ and $B(y)$ are disjoint. So all balls

$$B(x), \quad x \in S.$$

are disjoint. The disjoint union of all balls

$$\bigcup_{x \in S} B(x)$$

has exactly $|S|(n+1)$ elements. On the other hand, this union is a subset of $\{0,1\}^n$ which has 2^n elements. We obtain the inequality

$$|S|(n+1) \leq 2^n$$

□

The previous example is known as the *Hamming bound for* 1*-error correcing binary codes.* The mathematician Richard Hamming (1915–1998) also studied examples where equality holds (and these are known as Hamming codes).

3. Exercises

EXERCISE 7.1. * What is the maximum number of rooks that one place on an 8×8 chessboard such that no two rooks can hit each other? Prove your answer.

EXERCISE 7.2. *
What is the maximum number of queens that one can place on an 8×8 chessboard such that no two Queens can hit each other?

EXERCISE 7.3. **** What is the maximum number of queens that one can place on an 8×8 chessboard such that no two Queens can hit each other?

EXERCISE 7.4. ****[Dutch Mathematics Olympiad] A set S of positive integers is called *square-free* if for all distinct $a, b \in S$ we have that the product ab is not a square. What is the maximum cardinality of a square free subset $S \subseteq \{1, 2, 3, \ldots, 25\}$?

EXERCISE 7.5. * Show that $(a-b)(a-c)(b-c)$ is always even if a, b, c are integers.

EXERCISE 7.6. **** Prove that for every integer $n \geq 2$ there exists an integer m such that $k^3 - k + m$ is not divisible by n for all integers k.

EXERCISE 7.7. *** Show that, given a 7-digit number, you can cross out some digits at the beginning and at the end such that the remaining number is divisible by 7. For example, if we take the number 1234589, then we can cross out 1 at the beginning and 89 at the end to get the number $2345 = 7 \times 335$.

EXERCISE 7.8. **** Improve the statement in Example 7.6: Suppose that α is a real number and that N is a positive integer. Show that one of the numbers $\alpha, 2\alpha, 3\alpha, \cdots, N\alpha$ differs at most $\frac{1}{N+1}$ from an integer.

EXERCISE 7.9. *** Prove that the Euler number

$$e = \frac{1}{0!} + \frac{1}{1!} + \frac{1}{2!} + \frac{1}{3!} + \cdots$$

is irrational.

EXERCISE 7.10. ****
Let $x_1, x_2, \ldots, x_n \in \mathbb{R}$ with $|x_i| \leq 1$ for $i = 1, 2, \ldots, n$. Show that there exist $a_1, a_2, \ldots, a_n \in \{-1, 0, 1\}$, not all equal to 0, such that

$$|a_1 x_1 + a_2 x_2 + \cdots + a_n x_n| \leq \frac{n}{2^n - 1}$$

EXERCISE 7.11. ***** [IMO 1987] Let $x_1, x_2, \ldots, x_n$ be real numbers satisfying $x_1^2 + x_2^2 + \cdots + x_n^2 = 1$. Prove that for every integer $k \geq 2$ there are integers $a_1, a_2, \ldots, a_n$, not all 0, such that $|a_i| \leq k - 1$ for all i and

$$|a_1 x_1 + a_2 x_2 + \cdots + a_n x_n| \leq \frac{(k-1)\sqrt{n}}{k^n - 1}.$$

EXERCISE 7.12. ***** [Dutch Mathematical Olympiad] Suppose that S is a subset of $\{1, 2, 3, \ldots, 30\}$ with at least 11 elements. Show that one can choose a nonempty subset T of S such that the product of all elements of T is a square.

EXERCISE 7.13. *** Suppose that $a_0, a_1, a_2, \ldots, a_n \in \mathbb{Z}$ are integers. Show that the product

$$\prod_{0 \le i < j \le n} (a_j - a_i)$$

is divisible by $n!$.

EXERCISE 7.14. **** Let $a_1, a_2, \ldots, a_{10}$ be distinct integers from $\{1, 2, \ldots, 99\}$. Show that $\{a_1, a_2, \ldots, a_{10}\}$ contains two disjoint non-empty subsets with the sum of the numbers from the first equal to the sum of the elements from the second subset.

EXERCISE 7.15. ***** The set M consists of 2001 distinct positive integers, none of which is divisible by any prime $p > 23$. Prove that there are distinct x, y, z, t in M such that $xyzt = u^4$ for some integer u.

EXERCISE 7.16 (Putnam 1989). **** Let m be a positive integer and let $\mathcal{G}$ be a regular $(2m+1)$-gon inscribed in the unit circle. Show that there is a postive constant A, independent of m, with the following property. For any point p inside $\mathcal{G}$ there are two distinct vertices v_1 and v_2 of $\mathcal{G}$ such that

$$||p - v_1| - |p - v_2|| < \frac{1}{m} - \frac{A}{m^2}.$$

Here $|s - t|$ denotes the distance between the points s and t.

EXERCISE 7.17. *** Show that

$$\sum_p \frac{1}{2^p}$$

where p runs over all prime numbers, is an irrational number.

EXERCISE 7.18 (Putnam 2000). Let a_j, b_j, c_j be integers $1 \le j \le N$. Assume for each j, at least one of a_j, b_j, c_j is odd. Show that there exist integers r, s, t such that $ra_j + sb_j + tc_j$ is odd for at least $4N/7$ values of j, $1 \le j \le N$.

CHAPTER 8

Sequences and Series

DEFINITION 8.1. A sequence of real numbers $x_1, x_2, x_3, \ldots$ converges to a real number x if for every $\delta > 0$ there exists a positive integer N such that for all $n \geq N$ we have

$$|x_n - x| < \delta.$$

We will write $\lim_{n\to\infty} x_n = x$ and say that x is the limit of $x_1, x_2, x_3, \ldots$ as n tends to infinity.

DEFINITION 8.2. We say

$$\lim_{n\to\infty} x_n = \infty$$

if for every positive real number C, there exists a positive integer N such that $x_n \geq C$ for all $n \geq N$. Similarly, one can define what is meant by

$$\lim_{n\to\infty} x_n = -\infty.$$

EXAMPLE 8.3.

$$\lim_{n\to\infty} \frac{1}{n} = 0.$$

PROOF. Given $\delta > 0$, we can choose $N > 1/\delta$. Then for all $n \geq N$ we have

$$\left|\frac{1}{n} - 0\right| \leq \frac{1}{N} < \delta.$$

□

EXAMPLE 8.4. If $|x| < 1$, then

$$\lim_{n\to\infty} x^n = 0.$$

PROOF. Put $\varepsilon = 1 - |x|$. Then

$$|x^n| = (1-\varepsilon)^n \leq \frac{1}{(1+\varepsilon)^n} \leq \frac{1}{1+\varepsilon n}.$$

If we now take $N > (\delta\varepsilon)^{-1}$, then for all $n \geq N$ we have

$$|x^n| < \frac{1}{\varepsilon n} \leq \delta.$$

This shows that $\lim_{n\to\infty} x^n = 0$. □

There are various well-known rules for limits, such as:

LEMMA 8.5. *If* $\lim_{n\to\infty} x_n = x$ *and* $\lim_{n\to\infty} y_n = y$ *then* $\lim_{n\to\infty}(x_n + y_n) = x + y$ *and* $\lim_{n\to\infty} x_n y_n = xy$.

There are also some more abstract theorems for showing convergence, such as:

THEOREM 8.6. *If C is a real number, and*

$$x_1 \leq x_2 \leq x_3 \leq x_4 \leq \dots$$

is a weakly increasing sequence with $x_i \leq C$ for all i, then $x_1, x_2, x_3, \dots$ converges.

THEOREM 8.7. *If $x_1, x_2, x_3, \dots$ is a sequence such that for every $\delta > 0$, there exists an n such that $|x_n - x_m| \leq \delta$ for all $m \geq n$. Then $x_1, x_2, x_3, \dots$ converges. Such a sequence $x_1, x_2, x_3, \dots$ is called a Cauchy sequence.*

1. Series

We will discuss convergence of series.

DEFINITION 8.8. If $x_1, x_2, x_3, \dots$ is a sequence of real numbers, then we say that the series

$$\sum_{i=1}^{\infty} x_i$$

converges with value y if the sequence $y_1, y_2, y_3, \dots$ with y_n defined by

$$y_n = \sum_{i=1}^{n} x_i$$

converges to y.

EXAMPLE 8.9.

$$\sum_{n=1}^{\infty} \frac{1}{n} = \infty$$

PROOF. Note that

$$\sum_{n=1}^{2^k} \frac{1}{n} = 1 + \sum_{j=1}^{k-1} \sum_{l=2^j+1}^{2^{j+1}} \frac{1}{l} \geq 1 + \sum_{j=1}^{k-1} \sum_{l=2^j+1}^{2^{j+1}} \frac{1}{2^{j+1}} =$$

$$= 1 + \sum_{j=1}^{k-1} \frac{2^j}{2^{j+1}} = 1 + (k-1)\frac{1}{2} > \frac{k}{2}.$$

Given a positive integer C, then for $m \geq 2^{2C}$ we have

$$\sum_{n=1}^{m} \frac{1}{n} \geq \sum_{n=1}^{2^{2C}} \frac{1}{n} > 2C\frac{1}{2} = C.$$

An alternative proof uses the fact that

$$\frac{1}{n} \geq \int_n^{n+1} \frac{1}{x}\, dx$$

Therefore

$$\sum_{n=1}^{m} \frac{1}{n} \geq \sum_{n=1}^{m} \int_n^{n+1} \frac{1}{x}\, dx = \int_1^{m+1} \frac{1}{x}\, dx = \log(m+1).$$

and $\lim_{m\to\infty} \log(m+1) = \infty$. □

EXAMPLE 8.10. If $|x| < 1$ then

$$\sum_{n=0}^{\infty} x^n = \frac{1}{1-x}.$$

PROOF. We have

$$(1-x)(1+x+x^2+\cdots+x^n) = (1-x)+(x-x^2)+\cdots+(x^n-x^{n+1}) =$$
$$= 1+(-x+x)+(-x^2+x^2)+\cdots+(-x^n+x^n)-x^{n+1} = 1-x^{n+1},$$

(telescope sum) and therefore

$$\sum_{n=0}^{m} x^n = \frac{1-x^{m+1}}{1-x}.$$

If we take the limit $m \to \infty$ we get

$$\sum_{n=0}^{\infty} x^n = \lim_{m\to\infty} \sum_{n=0}^{m} x^n = \lim_{m\to\infty} \frac{1-x^{m+1}}{1-x} = \frac{1}{1-x}.$$

since $\lim_{m\to\infty} x^m = 0$ as we have seen before. □

2. Exercises

EXERCISE 8.1. ** Let x be a real number with $|x| < 1$. Find and prove a formula for

$$1 + 2x + 3x^2 + 4x^3 + \cdots .$$

EXERCISE 8.2. ** Suppose that $a_1, a_2, a_3, \ldots$ are real numbers such that

$$a_1 + a_2 + a_3 + \cdots$$

converges.

(a) Does $a_1^2 + a_2^2 + a_3^2 + \cdots$ necessarily converge?
(b) Assume also that $a_1, a_2, a_3, \ldots$ are all nonnegative. Does $a_1^2+a_2^2+a_3^2+\cdots$ necessarily converge?

EXERCISE 8.3. **

(a) Show that (using comparison with an integral for example), that for $a > 1$,

$$\sum_{n=1}^{\infty} \frac{1}{n^a}$$

converges.
(b) Show that

$$\sum_{n=1}^{\infty} \frac{1}{n\log(n)}$$

diverges.
(c) Show that for $a > 1$,

$$\sum_{n=2}^{\infty} \frac{1}{n\log^a(n)}$$

converges.

(d) Show that

$$\sum_{n=2}^{\infty} \frac{1}{n \log(n) \log(\log(n))}$$

diverges (watch out for $n = 2$).

EXERCISE 8.4. * Evaluate

$$\frac{1}{1 \cdot 2} + \frac{1}{2 \cdot 3} + \frac{1}{3 \cdot 4} + \cdots$$

(*Hint:* $\frac{1}{n(n+1)} = \frac{1}{n} - \frac{1}{n+1}$, *telescope sum!*)

EXERCISE 8.5. ** Show

$$\sum_{n} \frac{1}{n}$$

converges where the sum is taken over all positive integers n which don't have any 9 if they are written in the decimal system.

EXERCISE 8.6 (Putnam). ***** Let $a_1 < a_2 < a_3 < \cdots$ be an increasing sequence of positive integers. Let the series

$$\sum_{m=1}^{\infty} \frac{1}{a_n}$$

be convergent. For any number x, let $k(x)$ be the number of the a_n's which do not exceed x. Show that $\lim_{x \to \infty} k(x)/x = 0$.

EXERCISE 8.7. *** Show that

$$\sum_{n=1}^{\infty} \frac{1}{p_n} = \infty$$

where p_n is the n-th prime number. (*Hint: Use the fact that every natural number has a unique prime factorization, and show that*

$$\sum_{n=1}^{m} \frac{1}{n} \leq (1 + p_1^{-1} + \cdots + p_1^{-m})(1 + p_2^{-1} + \cdots + p_2^{-m}) \cdots (1 + p_m + \cdots + p_m^{-m}) \leq$$

$$\leq \frac{1}{1 - p_1^{-1}} \frac{1}{1 - p_2^{-1}} \cdots \frac{1}{1 - p_m^{-1}}.)$$

EXERCISE 8.8. ***** Construct real numbers $a_1, a_2, a_3, \ldots$ such that $\sum_{n=1}^{\infty} a_n$ converges, and $\sum_{n=1}^{\infty} a_n^3$ diverges.

EXERCISE 8.9. *** Let $a_1, a_2, \ldots$ be real numbers such that $\sum_n a_n/n$ converges. Show that $\lim_{N \to \infty} \frac{1}{N} \sum_{n=1}^{N} a_n = 0$.

EXERCISE 8.10. *** Evaluate

$$\prod_{n=2}^{\infty} \frac{n^3 - 1}{n^3 + 1}.$$

EXERCISE 8.11 (Putnam 1985). Let d be a real number. For each integer $m \geq 0$, define a sequence $\{a_m(j)\}$, $j = 0, 1, 2, \ldots$ by the condition

$$a_m(0) = d/2^m, \quad \text{and} \quad a_m(j+1) = (a_m(j))^2 + 2a_m(j), \quad j \geq 0.$$

Evaluate $\lim_{n\to\infty} a_n(n)$.

EXERCISE 8.12 (Putnam 1990). Let

$$T_0 = 2, T_1 = 3, T_2 = 6,$$

and for $n \geq 3$,

$$T_n = (n+4)T_{n-1} - 4nT_{n-2} + (4n-8)T_{n-3}.$$

The first few terms are,

$$2, 3, 6, 14, 40, 152, 784, 5168, 40576.$$

Find, with proof, a formula for T_n of the form $T_n = A_n + B_n$, where $\{A_n\}$ and $\{B_n\}$ are well-known sequences.

EXERCISE 8.13 (Putnam 1993). Let $\{x_n\}_{n\geq 0}$ be a sequence of nonzero real numbers such that $x_n^2 - x_{n-1}x_{n+1} = 1$ for $n = 1, 2, 3, \ldots$. Prove that there exists a real number a such that $x_{n+1} = ax_n - x_{n-1}$ for all $n \geq 1$.

EXERCISE 8.14. Suppose that $A_1, A_2, A_3, \ldots$ is a sequence of positive integers such that $A_1 = 1$ and $A_i < A_{i+1} \leq 2A_i$ for all positive integers i. Prove that every positive integer n can be written as a sum of distinct A_i's.

EXERCISE 8.15. ****[Putnam 1985, B3] Let

$$\begin{array}{cccc} a_{1,1} & a_{1,2} & a_{1,3} & \cdots \\ a_{2,1} & a_{2,2} & a_{2,3} & \cdots \\ a_{3,1} & a_{3,2} & a_{3,3} & \cdots \\ \vdots & \vdots & \vdots & \ddots \end{array}$$

be a doubly infinite array of positive integers, and suppose each positive integer appears exactly eight times in the array. Prove that $a_{m,n} > mn$ for some pair of positive integers (m, n).

EXERCISE 8.16. Suppose that we have n lines in the plane such that (i) no two lines are parallel and, (ii) no three lines go through 1 point. In how many regions do these lines divide the plane? Prove your formula.

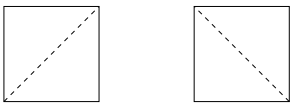
CHAPTER 9

Generating Functions

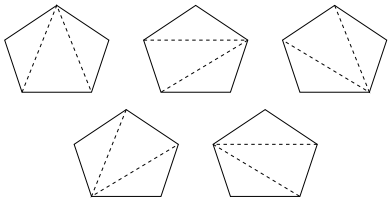
EXAMPLE 9.1. A triangulation of a convex n-gon is a partition of the area of the n-gon into triangles such that the vertices of each triangle is a vertex of the n-gon. How many distinct triangulations does a convex 10-gon have?

Let A_n be the number of triangulations of an n-gon. Let us find the value of A_n for small n.

We have $A_3 = 1$ and $A_4 = 2$:

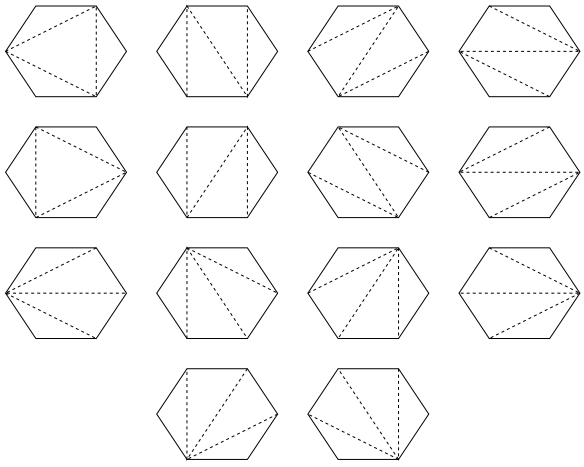


$A_5 = 5$:



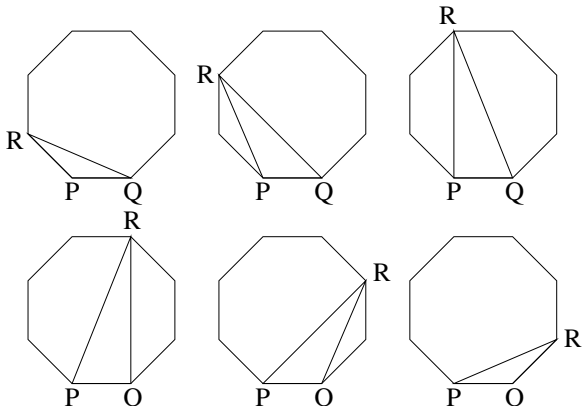
I

$A_6 = 14$:



It becomes more and more clear that it may not be feasible to write down all triangulations of an 10-gon. As n gets larger, we need a more systematic way of counting the possibilities to make sure that we are not forgetting any case.

Let P and Q be two fixed adjacent vertices of the n-gon. For each triangulation, there is a unique vertex R of the n-gon ($R \neq P, Q$) such that PQR is a triangle in the triangulation. For example, for $n = 8$ there are the following cases:



For fixed R, the complement of the triangle PQR within the n-gon is a union of an m-gon and a $(n+1-m)$-gon. The m-gon has A_m triangulations, and the $(n+1-m)$-gon has A_{n+1-m} triangulations. This gives $A_m A_{n+1-m}$ triangulations for this particular choice of R. From this we see the equation:

$$A_n = A_2 A_{n-1} + A_3 A_{n-2} + \cdots + A_{n-1} A_2.$$

where we define $A_2 = 1$. In particular,

$$\begin{aligned}
A_7 &= 1 \cdot 14 + 1 \cdot 5 + 2 \cdot 2 + 5 \cdot 1 + 14 \cdot 1 = 42 \\
A_8 &= 1 \cdot 42 + 1 \cdot 14 + 2 \cdot 5 + 5 \cdot 2 + 14 \cdot 1 + 42 \cdot 1 = 132 \\
A_9 &= 1 \cdot 132 + 1 \cdot 42 + 2 \cdot 14 + 5 \cdot 5 + 14 \cdot 2 + 42 \cdot 1 + 132 \cdot 1 = 429 \\
A_{10} &= 1 \cdot 429 + 1 \cdot 132 + 2 \cdot 42 + 5 \cdot 14 + 14 \cdot 5 + 42 \cdot 2 + 132 \cdot 1 + 429 \cdot 1 = 1430.
\end{aligned}$$

By the way, if one defines $C_n = A_{n+2}$ for all $n \geq 2$, then C_n are the so-called *Catalan numbers*. The Catalan numbers have many interesting interpretations (which we will not discuss now). It is known that

$$C_n = \frac{\binom{2n}{n}}{n+1}.$$

So for example $A_{10} = C_8 = \binom{16}{8}/9 = 1430$.

CHAPTER 10

Probability

1. Discrete Probability

Discrete probability deals with discrete random variables. For an event A we denote the probability that this event occurs by $P(A)$. If A and B are two events, then the probability that both A and B occur will be denoted by $P(A, B)$ or by $P(A \text{ and } B)$. The probability that A or B occurs will be denoted by $P(A \text{ or } B)$, etc.

The probability that event A occurs, *given* that B occurs is denoted by $P(A|B)$. This is called a *conditional probability*. The formula for $P(A|B)$ is

$$P(A|B) = \frac{P(A, B)}{P(B)}.$$

Suppose that we throw two dice. Let A be the event that the first die is 5. Let B be the event that the sum of the two dice is ≥ 10. Now we have $P(A) = \frac{1}{6}$. We have $P(B) = \frac{5}{36}$ because there are 5 possibilities to get a sum ≥ 10, namely $(4, 6)$, $(5, 6)$, $(6, 6)$, $(5, 5)$,$(6, 4)$. Similarly the probability $P(A, B)$ is equal to $\frac{2}{36}$ because there are two possibilities for the first die to be 5 and the sum to be ≥ 10, namely $(5, 5)$ and $(5, 6)$.

The probability that the first die is 5, given the fact that the sum of the dice is ≥ 10 is equal to

$$P(A|B) = \frac{P(A, B)}{P(B)} = \frac{\frac{2}{36}}{\frac{5}{36}} = \frac{2}{5}.$$

Suppose that X is a random event that has finitely many outcomes, namely $\{x_1, x_2, \ldots, x_n\}$. Each event $X = x_i$ has a certain probability, denoted by $p_i = P(X = x_i)$. We have $0 \leq p_i \leq 1$ for all i and

$$p_1 + p_2 + \cdots + p_n = 1.$$

If X is real-valued, then the expected value of X is

$$EX = p_1 x_1 + p_2 x_2 + \cdots + p_n x_n.$$

Example 10.1 (The Monty Hall Problem). This problem was inspired from the gameshow "Let's Make A deal", hosted by Monty Hall. It is now mathematical folklore.

A TV host shows you three numbered doors (all three equally likely), one hiding a car and the other two hiding goats. You get to pick a door, winning whatever is behind it. Regardless of the door you choose, the host, who knows where the car is, then opens one of the other two doors to reveal a goat, and invites you to switch your choice if you so wish. Does switching increases your chances of winning the car?

The answer is YES! If the host always opens one of the two other doors, you should switch. Notice that 1/3 of the time you choose the right door (i.e. the one with the car) and switching is wrong, while 2/3 of the time you choose the wrong door and switching gets

you the car. Thus the expected return of switching is 2/3 which improves over your original expected gain of 1/3.

Some experiments have an infinite number of outcomes as in the following example.

EXAMPLE 10.2. Suppose that we throw a coin. If the outcome is heads, then we throw again. We repeat this until the outcome is tails. Let X be the number of throws needed. Let p be the probability that the a coin gives tails. What is the expected number of throws needed?

The range of X is $\{1, 2, 3, \dots\}$. The probability $P(X = i)$ is equal to $(1-p)^{i-1}p$. If $|x| < 1$ then

$$\frac{1}{1-x} = 1 + x + x^2 + \cdots .$$

If we apply this here we see that indeed

$$\sum_{i=1}^{\infty}(1-p)^{i-1}p = p\frac{1}{1-(1-p)} = 1.$$

The expected value of X is

$$\sum_{i=1}^{\infty} i(1-p)^{i-1}p.$$

If $|x| < 1$ then we have the formula

$$\frac{1}{(1-x)^2} = 1 + 2x + 3x^2 + \cdots$$

From this follows that the expected number of throws EX is equal to

$$p\frac{1}{(1-(1-p))^2} = \frac{1}{p}.$$

2. Inclusion-Exclusion

For the following example we need to introduce the *inclusion-exclusion* principle (although it is not really part of combinatorics rather than probability theory). If A_1, A_2 are finite sets, then

$$|A_1 \cup A_2| = |A_1| + |A_2| - |A_1 \cup A_2|$$

(If X is a finite set then $|X|$ denotes its cardinality). If A_1, A_2, A_3 are finite sets, then

$$|A_1 \cup A_2 \cup A_3| = |A_1| + |A_2| + |A_3| - |A_1 \cap A_2| - |A_1 \cap A_3| - |A_2 \cap A_3| + |A_1 \cap A_2 \cap A_3|.$$

These formulas generalize to an arbitrary number of sets. In general one has

$$|A_1 \cup A_2 \cup \cdots \cup A_n| = c_1 - c_2 + c_3 - c_4 + \cdots + (-1)^{n-1}c_n. \tag{34}$$

where

$$c_r = \sum_{1 \le i_1 < i_2 < \cdots < i_r \le n} |A_{i_1} \cap A_{i_2} \cap \cdots \cap A_{i_r}|.$$

EXAMPLE 10.3. Suppose each person of a group of n people write their name on a piece of paper. The papers with the names are put in a random. Each person pulls (without looking) a name out of the hat at random. (This is common practice when people want to prepare presents for each other on holidays.) Let p_n be the probability that someone drew his own name. What is $\lim_{n\to\infty} p_n$?

Let A_i be the set of all permutations σ of $\{1, 2, 3, \ldots, n\}$ for which $\sigma(i) = i$. (A permutation σ of $\{1, 2, \ldots, n\}$ is a bijective (onto and 1–1) map from $\{1, 2, \ldots, n\}$ to itself. There are $n!$ possible permutations.) Now $A_1 \cup A_2 \cup \cdots \cup A_n$ is the set of all permutations σ for which $\sigma(i) = i$ for *some* i. The probability that someone draws his/her own name is:

$$p_n = \frac{|A_1 \cup A_2 \cup \cdots \cup A_n|}{n!}.$$

To find $|A_1 \cup A_2 \cup \cdots \cup A_n|$ we can use the inclusion-exclusion principle. If $1 \leq i_1 < i_2 < \cdots < i_r \leq n$ then

$$A_{i_1} \cap A_{i_2} \cap \cdots \cap A_{i_r}$$

is exactly the set of all permutations σ which fix $i_1, i_2, \ldots, i_r$. Such a σ can freely permute

$$\{1, 2, \ldots, n\} \setminus \{i_1, \ldots, i_r\}.$$

It follows that

$$|A_{i_1} \cap A_{i_2} \cap \cdots \cap A_{i_r}| = (n - r)!$$

Since there are $\binom{n}{r}$ possible choices of $i_1, i_2, \ldots, i_r$ we get that

$$c_r = \binom{n}{r}(n - r)! = \frac{n!}{r!}.$$

From the inclusion-exclusion principle follows that

$$|A_1 \cup A_2 \cup \cdots \cup A_n| = \frac{n!}{1!} - \frac{n!}{2!} + \frac{n!}{3!} - \cdots + (-1)^{n-1}\frac{n!}{n!}$$

and

$$p_n = \frac{1}{1!} - \frac{1}{2!} + \cdots + (-1)^{n-1}\frac{1}{n!}.$$

We now have that $\lim_{n\to\infty} p_n = 1 - 1/e$ where e is the Euler number, because

$$\frac{1}{e} = e^{-1} = \frac{1}{0!} - \frac{1}{1!} + \frac{1}{2!} - \frac{1}{3!} + \cdots .$$

3. continuous probability

A continuous random variable X has some values inside some infinite set S. On S we have some measure (integral). For example X may be a random point on in the square $[0, 1] \times [0, 1]$. If $U \subseteq [0, 1] \times [0, 1]$, then the probability $P(X \in U)$ is equal the area of U. This is an example of a *uniform distribution*.

EXAMPLE 10.4. On a piece of paper there are parallel lines drawn every 1 inch. We throw a needle on the piece of paper. What is the probability that the needle does not touch one of the lines?

PROOF. Mark one end of the needle with the letter P and the other end with the letter Q. Suppose that that lines are $\ldots, y = -1, y = 0, y = 1, \ldots$. Let Y be the random variable with values in $[0, 1)$ defined as the y-coordinate P modulo 1. Let X be the random variable of the angle of the vector PQ with the positive x-axis. This variable X has values in $[0, 2\pi)$. The outcome of the pair (X, Y) is uniformly distributed over $[0, 2\pi) \times [0, 1)$. If $U \subseteq [0, 2\pi) \times [0, 1)$ then the probability that $(X, Y) \in U$ is exactly the area of U divided by 2π. Let U be the set of all points $(x, y) \in [0, 2\pi) \times [0, 1)$ for which the line-segment between $(0, y)$ and $(\cos(x), y + \sin(x))$ does not touch the line $y = 0$ or $y = 1$. This means that $0 \leq y + \sin(x) \leq 1$. The area of the set

$$U = \{(x, y) \mid 0 \leq x < 2\pi, 0 \leq y \leq 1, 0 \leq y + \sin(x) \leq 1\}$$

If $(x, y) \in U$ then for a fixed angle x, y must lie in an interval of length $1 - |\sin(x)|$. This means that the area of U is

$$\int_{x=0}^{2\pi} 1 - |\sin(x)| dx = 2 \int_{x=0}^{\pi} 1 - \sin(x) dx = 2x + 2\cos(x)]_0^{\pi} = 2\pi - 4.$$

The probability that the needle does not touch one of the lines is

$$\frac{2\pi - 4}{2\pi} = 1 - \frac{2}{\pi}.$$

□

4. Exercises

EXERCISE 10.1. * Assume that every born baby has exactly 50% to be a boy and 50% change to be a girl. Also assume that the life expectancy for boys and girls is the same. In some country, a new law is introduced which says that every couple may have at most one boy. This means that every couple who gave birth to a boy is not allowed to have any more children. What will happen to the population? Will there be more girls eventually? Or will there be more boys eventually? Or will ratio of boys and girls be close to 1?

EXERCISE 10.2. * There are three pancakes in a hat. One pancake has two yellow sides. One pancake has two brown sides. The third pancake has a brown and a yellow side. A random pancake is pulled from the hat and it is put on a plate such that only one side is visible to you. The side that you can see is brown. What is the probability that the other side is brown?

EXERCISE 10.3 (UMUMC 1997). ** 2000 students participated in a math competition. They had been arbitrarily assigned code numbers from 1 to 2000. All 2000 scores were different. Given that student 1 scored higher than students 2 through 1997, what is the probability that student 1 had the highest score overall?

EXERCISE 10.4 (UMUMC 1997). ***

(a) A and B plan to play a game where they take turns tossing a coin until someone flips head and thereby wins. On the basis of alphabetical order, A claims the right to go first, but B objects that this gives A an unfair advantage. To compensate, A, offers to allow B to use a biased coin, whereas A will use a fair coin. Prove that the game is still biased in A's favor.

(b) In view of your proof of part (a), B demands further adjustments in the probabilities of the individual coin flips. Because it is difficult to adjust the bias of a coin, the players agree to play the following variant of the game. A large (but finite) number of ping-pong balls are placed in a bag; some ar labeled A and some B. The players alternately draw one ball out of the bag (each ball being equally likely and the draws being independent). The first player to draw a ball labeled by his own name is the winner. Any balls drawn that doesn't win this way is put back into the bag before the next draw. A will draw first, but to compensate for this advantage, more balls will be labeled B than A. Is it possible to choose the number of balls with each label in such a way that the game is fair. If so, what should the numbers of balls be?

EXERCISE 10.5 (UMUMC 2003). **** An unbalanced penny and an unbalanced quarter, with probabilities of head p for the penny and q for the quarter, are tossed together over and over. The probability that the penny shows heads (strictly) before the quarter is 3/5, and the number of tosses required for both coins to show heads simultaneously has expected value exactly 4. Find the values of p and q.

EXERCISE 10.6 (Putnam 1989). **** If α is an irrational number, $0 < \alpha < 1$, is there a finite game with an honest coin such that the probability of one player winning the game is α? (An honest coin is one for which te probability of heads and the probabily of tails are both $\frac{1}{2}$. A game is finite if with probability 1 it must end in a finite number of moves.)

EXERCISE 10.7 (Putnam 2002). *** Shanillo O' Keal shoots free throws on a basketball court. She hits the first and misses the second, and thereafter the probability that she hits the next shot is equal to the proportion of shots she has hit so far. What is the probability she hits exactly 50 of her first 100 shots?

EXERCISE 10.8. **** Prove the inclusion-exclusion principle.

EXERCISE 10.9. ** In a classroom there are 22 students. Show that the probability that two of the students have the same birthday is more than 50% (for simplicity you may assume that no students were born on February 29, you may need a computer or a calculator).

EXERCISE 10.10. ***** [Putnam 1992] Four points are chosen at random on the surface of a sphere. What is the probability that the center of the spere lies inside the tetrahedron whose vertices are at the four points? (It is understood that each point is independently chosen relative to a uniform distribution on the sphere.)

EXERCISE 10.11. *** On a piece of paper we draw a grid. We have horizontal lines, and vertical lines. The horizontal lines are 1 inch apart and so are the vertical lines. A needle of one inch long is thrown at random on the piece of paper. What is the probability that the needle does not tuch any of the lines.

EXERCISE 10.12. **** [Putnam 1993] Two real numbers x and y are chosen at random in the interval $(0, 1)$ with respect to the uniform distribution. What is the probability that the closest integer to x/y is even? Express the answer in the form $r + s\pi$, where r and s are rational numbers.

EXERCISE 10.13 (UMUMC 1996). ***** One person in a ring of n people has a keg of beer. He takes a sip and passes the keg to the left or to the right with 50% probability. The

recipient of the keg takes a sip and also passes the keg to the left or to the right with 50% probability. The process is repeated until everyone has had at least one sip. What is the probability distribution of the final position of the keg?

EXERCISE 10.14 (UMUMC 2002). ***** Consider the sequence of first digits in the successive powers of 2:

$$2, 4, 8, 1, 3, 6, 1, \ldots$$

Does one fo the digits 7 and 8 appear more often in the sequence than the other one? (We say for example that 5 appears more often than 6 in the sequence if there exists a positive integer N such that for all $n \geq N$, 5 appears more often than 6 among the first n terms of the sequence.)

EXERCISE 10.15. **** Let C be the unit circle $x^2+y^2 = 1$. A point p is chosen randomly on the circumference C and another point q is chosen randomly from the interior of C (these points are chosen independently and uniformly over their domains). Let R be the rectangle with sides parallel to the x and y-axes with diagonal pq. What is the probability that no point of R lies outside of C?

CHAPTER 11

Games

1. Weighing Problems

There are many popular problems involving weighing with either a *balance scale* or a *numerical scale*. A balance scale has two sides. With one weighing there are three possible outcomes, the left side is heavier than the right side, the left side is lighter than the right side or the left and the right side have the same weight. A weighing scale which gives you the weight of an object in pounds (or another unit) we will call a numerical scale (to make a clear distinction).

EXAMPLE 11.1. Suppose that we have 25 coins that look identical. The coins are all the same except that one coin is counterfeit and heavier than the others. How can one determine, in three weighings on a balance scale, which coin is counterfeit.

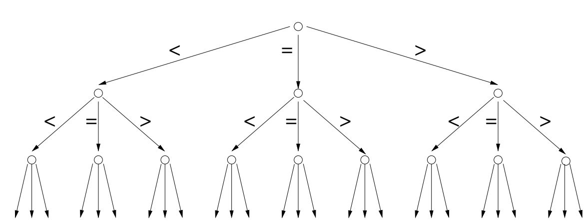
Divide the 25 coins up in three groups, say A, B and C such that A and B have 8 coins each and C has 7 coins. Put the A coins on the left side of the scale and the B coins on the right side of the scale. If A is heavier then A contains the counterfeit coin. If B is heavier then B contains the counterfeit coin. If both sides balance, then C has the counterfeit coin.

So we found a set of 7 or 8 coins of which we know that one is counterfeit. We may take (for convenience) 1 or 2 coins from the remaining genuine coins so that we have 9 coins. We have to find out, with two remaining weighings which is the counterfeit coin among these 9 coins. Split the 9 coins up in three groups, D,E and F, such that each group has exactly 3 coins. Put the D coins on the left and E coins on the right of the scale. Again we find out which of the groups D,E,F cointains the counterfeit coin.

We now have three coins left. Put one coin on the left and one coin on the right of the scale. The coin that is the heaviest is the counterfeit. If both coins weigh the same, then the third coin is the counterfeit one.

EXAMPLE 11.2. Suppose that we have 30 coins that look identical. The coins are all the same except that one coin is counterfeit and heavier than the others. Is it always possible to determine, in three weighings on a balance scale, which coin is counterfeit.

The answer is no. Each weighing has three possible outcomes. One could graph the possible events as a tree:



From the 3 weighing events there can only be at most $3 \times 3 \times 3 = 27$ possible outcomes. By the pigeonhole principle there are two numbers i and j with $1 \leq i < j \leq 30$ such that the results of the weighings will be exactly the same if either the i-th coin or j-th coin is the cointerfeit coin. □

EXAMPLE 11.3. Suppose you have 10 barrel of coins. Each barrel contains all real coins or it contains all fake coins. The real coins weigh 10 grams, and the counterfeit coins weigh 11 grams. There is exactly one barrel with counterfeit coins. Determine, with only one weighing on a numerical scale, which barrel cointains the cointerfeit coins. (One may assume that the barrels cointain "enough" coins.)

PROOF. Take one coin from the first barrel, two coins from the second barrel, three coins from the third barrel, etc. Put these $1 + 2 + \cdots + 10 = 55$ coins on the scale. If barrel k contains the counterfeit coins, then the weight will be

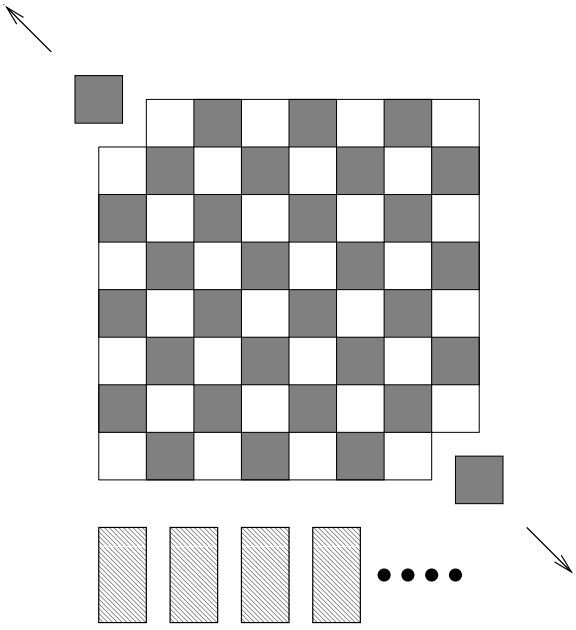
$$1 \cdot 10 + 2 \cdot 10 + \cdots + 10 \cdot 10 + (11 - 10) \cdot k = 550 + k.$$

grams. This means that we can tell immediately from the weight which barrel contains the counterfeit coins. If the weight is for example 557, then this means that barrel 7 cointains the counterfeit coins. □

2. Tilings

Vaguely speaking, an *invariant* is a quantity that remains the same after certain operations. For many problems it is useful to identify such *invariants*.

EXAMPLE 11.4. ** We cut out two opposite corner fields of a chessboard. Is it possible to put 31 domino tiles (of size 2×1) on the remaining 62 fields of the chessboard?



PROOF. The answer is no. The two corner which were cut out have the same color. Without loss of generality we may assume that they both were black. Let I be the number white fields that have been covered by domino tiles minus the number of black fields that

have been covered by domino tiles. If there are no domino tiles on the chessboard, then $I = 32-30 = 2$. Every time we put another domino tile on the chessboard, then this domino tile will cover exactly one black field and one white field. This means that the quantity I doesn't change. If the whole chessboard without the two corners would be covered with domino tiles, then $I = 0$ which is impossible because I is constant and equal to 2. □

EXAMPLE 11.5. Suppose that p, q and n are positive integers such that n is not divisible by p or by q. Prove that an $n \times n$ floor cannot be tiled by $p \times p$ or by $q \times q$ tiles.

PROOF. The idea of the proof is the following: Number the rows and columns with $0, 1, 2, \ldots, n-1$. Let us write numbers $a_{i,j}$ on square i, j such that: (1) The sum of all the numbers on a $p \times p$ or $q \times q$ square is always 0 and (2) the sum of all the numbers $a_{i,j}$, $1 \leq i, j \leq n$ is nonzero. This then would clearly prove that the $n \times n$ floor cannot be tiled with $p \times p$ and $q \times q$ tiles.

To ensure that the sum of all the numbers under a $p \times p$ square is 0, we could force that

$$a_{i,j} + a_{i+1,j} + \cdots + a_{i+p-1,j} = 0$$

for all i, j. To ensure that the sum of all the numbers under a $q \times q$ square is 0, we could force that

$$a_{i,j} + a_{i,j+1} + \cdots + a_{i,j+q-1} = 0$$

for all i, j. The easiest way to choose the $a_{i,j}$ in this fashion is to use complex numbers (but one could avoid this).

For any integer k, let $\zeta_k = e^{2\pi i/k}$ be the k-th primitive root of unity. Observe that

$$1 + \zeta + \zeta^2 + \cdots + \zeta^{l-1} = (1 - \zeta^l)/(1 - \zeta)$$

is equal to 0 if and only if l is divisible by k. Fill the $n \times n = n^2$ fields with complex numbers as follows. Number the rows and columns by $0, 1, 2, \ldots, n-1$. Put the complex number $\zeta_p^i \zeta_q^j$ on the field in row i and column j. The sum of all numbers over all fields is

$$\sum_{0 \leq i,j < n} \zeta_p^i \zeta_q^j = (1 + \zeta_p + \cdots + \zeta_p^{n-1})(1 + \zeta_q + \cdots + \zeta_q^{n-1})$$

is **nonzero** since p and q do not divide n. On the other hand, if we place a $p \times p$ tile (with one corner at (k, l)), then the sum of all complex numbers under the tile is

$$\sum_{i=k}^{k+p-1} \sum_{j=l}^{l+p-1} \zeta_p^i \zeta_q^j = \zeta^{2k} (\sum_{i=0}^{p-1} \zeta_p^i)(\sum_{i=0}^{p-1} \zeta_q^i) = 0$$

since

$$\sum_{i=0}^{p-1} \zeta_p^i = 0.$$

Similarly all the numbers under a $q \times q$ tile sum up to 0. This shows that it is not possible to tile the $n \times n$ floor with $p \times p$ and $q \times q$ tiles. □

3. Exercises

EXERCISE 11.1. * Suppose that we have 3^n coins that look identical. The coins are all the same except that one coin is counterfeit and heavier than the others. How can one determine, in n weighings on a balance scale, which of the coins is counterfeit?

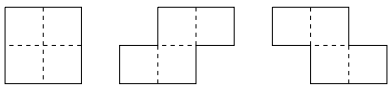
EXERCISE 11.2. **** Suppose that we have 12 coins that look identical. The coins are all the same except that one coin is counterfeit and does not have the same weight as the real coins. We do not now if the counterfeit coin is heavier or lighter than the real coins. How can one determine, in 3 weighings on a balance scale, which of the coins is counterfeit and whether the counterfeit coin is heavier or lighter?

EXERCISE 11.3. * Suppose that we have 14 coins that look identical. The coins are all the same except that one coin is counterfeit and does not have the same weight as the real coins. We do not know if the counterfeit coin is heavier or lighter than the real coins. Show that it is not always possible to determine, in 3 weighings on a balance scale, which coins is counterfeit and whether it is heavier or lighter at the same time.

EXERCISE 11.4. **** Suppose that we have a balance scale and exactly 5 weights, weighing exactly x_1, x_2, x_3, x_4 and x_5 grams. For any positive integer $n \leq 100$ one would like to be able to determine using the scale whether a given object weighs less than, more than or exactly n grams. How should one choose the weights x_1, x_2, x_3, x_4, x_5 such that this is always possible?

EXERCISE 11.5. *** Suppose you have 10 barrel of coins. Each barrel contains all real coins or it contains all fake coins. The real coins weigh 10 grams, and the counterfeit coins weigh 11 grams. This time, there may be several barrels with cointerfeit coins (or even all or none of them). Determine, with only one weighing on a numerical scale, exactly which of barrels cointain the cointerfeit coins. (One may assume that the barrels cointain "enough" coins.)

EXERCISE 11.6. *** Show that 12×11 rectangular floor cannot be covered using only tiles of the following shapes:



EXERCISE 11.7. ***** Suppose that p, q and r are distinct prime numbers and $N > 2pqr$. Show that an $N \times N$ floor can be tiled with $p \times p$, $q \times q$ and $r \times r$ tiles. (*Hint: Write $N = apq + bpr + cqr$ for certain nonnegative integers a, b, c. Use this to divide the $N \times N$ floor in regions which are easy to tile.*)

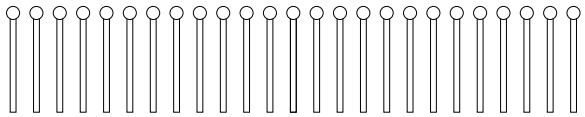
EXERCISE 11.8. ***** A rectangle R is divided into smaller rectangles. Each of the smaller rectangles has at least one side, whose length is an integer. Show that R itself has at least one side which is an integer.

EXERCISE 11.9. ** You are at the coordinates $(1, 0, 0)$ in $\mathbb{R}^3$ where we use the usual xyz coordinate axis. A three dimensional knight jump is if you move ± 1 along one coordinate axis, ± 2 along a second coordinate axis and ± 3 along the third coordinate axis. For example one could jump from $(1, 0, 0)$ to $(1, 0, 0) + (2, -1, 3) = (3, -1, 3)$. Then one could jump to

$(3,-1,3)+(-3,2,-1)=(0,1,2)$ and from there to $(0,1,2)+(1,2,-3)=(1,3,-1)$. Show that it is impossible to land at $(0,0,0)$ after finitely many three dimensional knight jumps.

4. Games

EXERCISE 11.10. ** There are 25 matches on the table. Two players take turns. Each turn they have to take away 1,2 or 3 matches. The person taking the last match loses. Show that the second player always can win this game. (Try it first with 5,9 and 13 matches instead.)



EXERCISE 11.11 (IMO). ***** To each vertex of a regular pentagon an integer is assigned in such a way that the sum of all five numbers is positive. If three consecutive vertices are assigned the numbers x, y, z respectively and $y < 0$ then the following operation is allowed: the numbers x, y, z are replaced by $x + y, -y, z + y$ respectively. Such an operation is performed repeatedly as long as at least one of the five numbers is negative. Determine whether this procedure necessarily comes to an end after a finite number of steps.

EXERCISE 11.12 (after a well-known puzzle). **** In a 4×4 square, we put the numbers $2, 1, 3, 4, 5, 6, \ldots, 15$ (see below). The last square is black. In each move, we may exchange the black square with one of its neighbors (neighbor means sharing an edge). Is it possible to get $1, 2, 3, \ldots, 15$ after finitely many moves (see second picture).

2	1	3	4
5	6	7	8
9	10	11	12
13	14	15	

1	2	3	4
5	6	7	8
9	10	11	12
13	14	15	

EXERCISE 11.13. Suppose that we have an $m \times n$ chocolate bar. We break the chocolate bar into two pieces. Then we take one piece and break it into two. We keep repeating this until we are only left with mn pieces of size 1×1. How many times do we have to break the chocolate bar? Prove your formula. (In particular, show that the number of breaks needed does not depend on how you proceed.)

EXERCISE 11.14. **** Define a sequence $x_1, x_2, x_3, \ldots$ by $x_1 = 1$, $x_2 = 5$ and

$$x_{n+1} = \frac{x_n}{2} + x_{n-1} - \frac{x_{n-1}^2}{2x_n}$$

for $n \geq 2$. What is $\lim_{n\to\infty} x_n$?

EXERCISE 11.15. *** We start with the numbers

$$1, 2, 3, 4, 5, 6, 7, 8, 9, 10$$

Then we replace two numbers, say x and y, by $xy/(x+y)$. We repeat this until there is only one number left. Show that, regardless how you do it, this number is always equal to 2520/7381. (For example, we could replace 3 and 6 by $3 \cdot 6/(3+6) = 2$ to get the sequence

$$1, 2, 4, 5, 7, 8, 9, 10, 2.$$

Then we can replace 9 and 10 by $9 \cdot 10/(9+10) = 90/19$ to get the sequence

$$1, 2, 4, 5, 7, 8, 2, 90/19.$$

etc.)