INTEGERS

PETER MAYR (MATH 2001, CU BOULDER)

In this section we aim to show the following:

Goal. Every natural number can be written uniquely as a product of primes.

1. Divisibility

Definition. Let $a, b \in \mathbb{Z}$. Then $a|b$ (a **divides** c) if there exists $q \in \mathbb{Z}$ such that $b = aq$ (Then we also call a a **divisor** of c and c a **multiple** of a).

Definition. $p \in \mathbb{N}$ is **prime** if $p > 1$, and 1 and p are the only divisors of p. Otherwise p is **composite**.

Lemma 1. *Let $a, b, c \in \mathbb{Z}$. If $a|b$ and $a|c$, then $a|b + c$.*

Proof. Assume $a|b$ and $a|c$. We want to show $a|b + c$.

By definition of divisibility, b, c are both multiples of a. That is, we have $m, n \in \mathbb{Z}$ such that $b = ma, c = na$. Consider

$$b + c = ma + na = (m + n)a.$$

Since $m + n \in \mathbb{Z}$, we see that $b + c$ is a multiple of a. Thus $a|b + c$. □

Definition. $a \in \mathbb{Z}$ is **even** if $2|a$, i.e., $a = 2n$ for some $n \in \mathbb{Z}$.

$a \in \mathbb{Z}$ is **odd** if $2 \nmid a$, i.e., $a = 2n + 1$ for some $n \in \mathbb{Z}$.

Lemma 2. *Let $a \in \mathbb{Z}$. If a is odd, then a^2 is odd.*

Proof. Assume a is odd. We want to show a^2 is odd.

By definition, we have $n \in \mathbb{Z}$ such that $a = 2n + 1$. Consider

$$a^2 = (2n + 1)^2 = 4n^2 + 4n + 1 = 2(2n^2 + 2n) + 1.$$

Thus a^2 is odd. □

The previous two Lemmas are conditional statements: "If P, then Q." We used what is called a **direct proof** to show them:

Assume P holds. Show that Q holds.

Date: October 26, 2020.

2. The greatest common divisor

Definition. The **greatest common divisor** $\gcd(a,b)$ of integers a,b is the largest integer d that divides both a and b.

The **least common multiple** $\operatorname{lcm}(a,b)$ of integers a,b is the smallest positive integer m such that $a|m$ and $b|m$.

Example.

$$\begin{array}{ll}
\gcd(18,24) = 6 & \operatorname{lcm}(18,24) = 72 \\
\gcd(10,-4) = 2 & \operatorname{lcm}(10,-4) = 20 \\
\gcd(5,0) = 5 & \operatorname{lcm}(5,0) \text{ not defined} \\
\gcd(0,0) \text{ not defined} &
\end{array}$$

Fact. For $a,b \in \mathbb{N}$,

$$\gcd(a,b) \cdot \operatorname{lcm}(a,b) = ab$$

(to be proved later).

How to compute the gcd? Instead of factoring the numbers, the following lemma allows us to reduce to smaller numbers.

Lemma 3. *Let $a,b,q \in \mathbb{Z}$. Then $\gcd(a,b) = \gcd(a-qb,b)$.*

Example. The **Euclidean algorithm** for computing the gcd is based on Lemma 3. We explain it by an example:

$\gcd(30,12) = \gcd(30-2\cdot 12,12) = \gcd(12,6) = \gcd(12-2\cdot 6,6) = \gcd(0,6) = 6$

In each step we subtract a multiple of the smaller number from the bigger until we get to 0. Then $\gcd(0,a) = a$ for $a \in \mathbb{N}$.

3. The division algorithm

In the Euclidean algorithm for $\gcd(a,b)$ we want to subtract an as large as possible multiple qb from a to get a number $a-qb$ that is strictly smaller than b. This is always possible because of the following:

Division Algorithm. For all $a,b \in \mathbb{Z}$ with $b > 0$, there exist uniquely determined integers q,r (quotient, remainder) with $0 \leq r < b$ such that

$$a = qb + r.$$

Example. For $b = 5$,

$$11 = 2 \cdot b + 1$$

$$-11 = (-3)b + 4$$

Note that the remainder r is always non-negative.

Proof of the Division Algorithm. We have to show

(1) q, r exist,
(2) q, r are unique.

Proof of (1).

Consider the set of all non-negative integers of the form a minus a multiple of b,

$$A := \{n \in \mathbb{N}_0 \ : \ n = a - qb \text{ for } q \in \mathbb{Z}\}$$

For r we want to pick the smallest element in A. This exists by the following property of the natural numbers that we take without proof.

Well-ordering of $\mathbb{N}_0$. *Every non-empty subset of $\mathbb{N}_0$ has a least element.*

Let $r \in \mathbb{N}_0$ be the least element in A, let $q \in \mathbb{Z}$ with $a - qb = r$.

Claim. $r < b$

Proof by contradiction. Assume $r \geq b$. Then $r - b = r - (q+1)b \in A$ and $r - b < r$. This contradicts the assumption that r is smallest in A. Hence our assumption that $r \geq b$ cannot be true. We have $r < b$. □

This completes the proof of (1). We omit the proof of (2). □

> Here we used a **proof by contradiction** to show a statement P:
> **Assume $\sim$ P. Show this implies FALSE (a contradiction).**
> Then the assumption $\sim P$ must have been FALSE. Hence P is TRUE.

4. Bezout's identity

The Euclidean algorithm also allows us to write $\gcd(a, b)$ as a sum of a multiple of a and a multiple of b. Again we explain how to do that by an example.

Example. We compute $\gcd(147, 33)$ by repeatedly subtracting multiples of the smaller number from the bigger. Additionally we record how to write each number as a sum of multiples of 147 and 33.

$$\begin{aligned}
147 &= 1 \cdot 147 + 0 \cdot 33 \\
33 &= 0 \cdot 147 + 1 \cdot 33 && \text{subtract 4 times from the previous equation} \\
15 &= 1 \cdot 147 - 4 \cdot 33 && \text{subtract 2 times from the previous} \\
3 &= -2 \cdot 147 + 9 \cdot 33 && \text{subtract 5 times from the previous} \\
0 &
\end{aligned}$$

In the penultimate line we find $\gcd(147, 33) = 3 = -2 \cdot 147 + 9 \cdot 33$.

Bezout's identity. *Let $a, b \in \mathbb{Z}$, not both 0. Then there exist $u, v \in \mathbb{Z}$ such that*

$$\gcd(a, b) = u \cdot a + v \cdot b$$

u, v are called **Bezout's cofactors** *and can be computed by the* **Euclidean algorithm**.

Proof. Follows from the Euclidean algorithm. □

Euclid's Lemma. Let p be prime, $a, b \in \mathbb{Z}$. If $p|ab$, then $p|a$ or $p|b$.

Proof. Exercise. □

5. Checking for primes

Lemma 4. *Let $a, b, c \in \mathbb{N}$. If $ab = c$, then $a \leq \sqrt{c}$ or $b \leq \sqrt{c}$.*

Contrapositive proof. Assume $a > \sqrt{c}$ and $b > \sqrt{c}$. Show $ab \neq c$.

By assumption $ab > \sqrt{c} \cdot \sqrt{c} = c$. Hence $ab \neq c$. □

Above we showed the statement "If P, then Q" by proving its contrapositive "If ∼ Q, then ∼ P" (which is logically equivalent). This is called a **contrapositive proof**:

Assume ∼ Q. Show ∼ P.

Corollary 5. *If $a \in \mathbb{Z}$ is not prime, then it has a divisor d with $1 < d \leq \sqrt{a}$.*

6. Irrationality of $\sqrt{2}$

Lemma 6. *Let $a \in \mathbb{Z}$. Then a is even iff a^2 is even.*

Definition. $x \in \mathbb{R}$ is **rational** if $x = \frac{a}{b}$ for some $a, b \in \mathbb{Z}$ with $b > 0$; otherwise x is **irrational**.

Theorem 7. *$\sqrt{2}$ is irrational.*

Proof by contradiction. Suppose $\sqrt{2}$ is rational.

Then we have $a, b \in \mathbb{Z}$ with $\gcd(a, b) = 1$ such that

$$\sqrt{2} = \frac{a}{b}$$

By squaring

$$2b^2 = a^2$$

Hence a^2 is even. By Lemma 6 also a is even. So $a = 2c$ for some $c \in \mathbb{Z}$. Then

$$2b^2 = (2c)^2 = 4c^2$$

yields $b^2 = 2c^2$. So b^2 and consequently b is even by Lemma 6. c Now $2|a$ and $2|b$ contradict our assumption that $\gcd(a, b) = 1$. Thus our assumption was wrong, no such a, b exist, and $\sqrt{2}$ is not rational. □

7. Modular arithmetic

Definition. Let $a, b \in \mathbb{Z}, n \in \mathbb{N}$.

(1) $a \bmod n$ is the remainder of a by division by n. So $a \bmod n \in \{0, \ldots, n-1\}$.
(2) a, b are **congruent modulo** n (written $a \equiv b \bmod n$ or $a \equiv_n b$) if $n|a - b$.

Note $a \equiv b \bmod n$ iff $a \bmod n = b \bmod n$.

Lemma 8. *Let $a, b, c, d \in \mathbb{Z}$, $n \in \mathbb{N}$ with $a \equiv b \bmod n$ and $c \equiv d \bmod n$. Then*

(1) $a + c \equiv b + d \mod n$,
(2) $a \cdot c \equiv b \cdot d \mod n$.

Proof. Exercise. □

7.1. An application in cryptography.

When you login to your online bank account from home, messages between you and your bank are transmitted over the internet. To keep them safe (from your internet provider or anyone else), these messages are encrypted using a personal key between you and your bank. But how can you and your bank agree on such a secret key in the first place without sending it over the internet where it may be stolen?

Problem. Alice and Bob want to agree on a secret number (a **key**) over the internet where others might listen in on their conversation (an **unsecure channel**). Afterwards this secret key can be used to encode messages between Alice and Bob.

There are several ways to do this. The following is used in internet traffic for example.

Algorithm (Diffie-Hellman key exchange).

(1) Alice and Bob agree on a prime p and a base g (public).
E.g. $p = 31, g = 3$
(2) Alice chooses a secret integer $a > 0$, sends $x = g^a \mod p$ to Bob.
E.g., $a = 4$,

$$x = 3^4 \mod 31 = 9^2 \mod 31 = 19$$

Bob chooses a secret integer $b > 0$, sends $y = g^b \mod p$ to Alice.

E.g., $b = 6$,

$$y = 3^6 \mod 31 = 3^4 \cdot 3^2 \mod 31 = 19 \cdot 9 \mod 31 = 16$$

(3) Having received y, Alice computes $s = y^a \mod p$.

$$s = 16^4 \mod 31 = 2$$

Having received x, Bob computes $s = x^b \mod p$.

$$s = 19^6 \mod 31 = 2$$

Remark.

(1) Note that Alice and Bob both compute the same number s above since by Lemma 8

$$x^b \equiv (g^a)^b \equiv g^{ab} \equiv g^{ba} \equiv (g^b)^a \equiv y^a \mod p.$$

(2) Only a, b, s are kept secret (never transmitted) whereas p, g, x, y can be sent publicly.

(3) To compute s from p, g, x, y it seems that you need to know a or b. Note that $g^a = x$ could easily be solved for a by taking the logarithm of x with base g. However here we need to solve $g^a \equiv x \mod p$ for a. This is called the **discrete logarithm problem** and for p large enough (in practice, $p \sim 2^{1024}$) there is no efficient way known to do this.

Hence the safety of the Diffie-Hellman key exchange (and of most other modern cryptographic systems) depends on a Math problem that cannot be solved efficiently.

8. Prime factorizations

First we generalize Euclid's Lemma from 2 to an arbitrary number of factors.

Lemma 9. *Let $n \in \mathbb{N}, a_1, \dots, a_n \in \mathbb{Z}$, p prime. If $p | a_1 \cdots a_n$, then $p | a_i$ for at least one $i \in \{1, \dots, n\}$.*

Proof by induction on n.

Basis step: For $n = 1$, $p | a_1$ and the statement is true.

Induction hypothesis: For a fixed $k \in \mathbb{N}$, if $p | a_1 \cdots a_k$, then $p | a_i$ for at least one $i \in \{1, \dots, k\}$.

Inductive step: Show that the statement is true for $n = k + 1$. So assume $p | a_1 \cdots a_{k+1}$. Writing $a_1 \cdots a_{k+1} = (a_1 \cdots a_k) a_{k+1}$ as the product of 2 factors, Euclid's Lemma yields that $p | a_1 \cdots a_k$ or $p | a_{k+1}$. In the first case the induction hypothesis yields $p | a_i$ for at least one

$i \in \{1, \ldots, k\}$. Thus $p|a_1$ or $p|a_2$ or $\ldots p|a_k$ or $p|a_{k+1}$. The induction step is proved and so is the Lemma. □

Induction. To show that a statement S_n is true for every $n \in \mathbb{N}$:

(1) **basis step:** Show S_1.
(2) **inductive step:** Show $S_k \Rightarrow S_{k+1}$ for any $k \in \mathbb{N}$.

Fundamental Theorem of Arithmetic.

(1) Every integer $n > 1$ has a factorization into primes

$$n = p_1 p_2 \cdots p_k.$$

(2) This prime factorization of n is unique up to ordering. That is, if

$$n = p_1 p_2 \cdots p_k = q_1 q_2 \cdots q_\ell$$

for primes $p_1, \ldots, p_k, q_1, \ldots, q_\ell$, then $k = \ell$ and $(p_1, \ldots, p_k)$ is a permutation of $(q_1, \ldots, q_k)$.

Proof of (1) by strong induction on n.

Basis step: $n = 2$ is a prime.

Induction assumption: Assume for a fixed $n \in \mathbb{N}$ that all numbers $\leq n$ can be written as a product of primes.

Inductive step: Show $n + 1$ can be written as a product of primes. We distinguish two cases:

Case, $n + 1$ is prime: Then $n + 1$ has a prime factorization (just itself).

Case, $n+1$ is not prime: Then $n+1 = ab$ for some $1 < a, b < n+1$. Since $a, b \leq n$, the induction assumption applies to them. Then we have primes $p_1, \ldots, p_k, q_1, \ldots, q_\ell$ such that $a = p_1 \cdots p_k$, $b = q_1 \cdots q_\ell$. Now $n+1 = p_1 \cdots p_k q_1 \cdots q_\ell$ is also a product of primes. The induction step is proved and so is item (1) of the theorem.

Proof of (2) by minimal counterexample. Seeking a contradiction suppose that the statement is wrong. Then there is some counter-example, moreover since $\mathbb{N}$ is well-ordered, there must be a minimal counter-example n (Note that $n > 2$ because 2 has exactly one prime factorization). So let

$$n = p_1 p_2 \cdots p_k = q_1 q_2 \cdots q_\ell$$

for primes $p_1, \ldots, p_k$ and $q_1, \ldots, q_\ell$ that are not a permutation of each other. Since $p_1 | q_1 q_2 \cdots q_\ell$, we obtain that p_1 divides some q_i by the previous lemma. But since q_i is prime, this means $p_1 = q_i$. So dividing by p_1 yields

$$\frac{n}{p_1} = p_2 \cdots p_k = q_1 q_2 \cdots q_{i-1} q_{i+1} \cdots q_\ell.$$

Now $p_2, \ldots, p_k$ and $q_1, \ldots, q_{i-1}, q_{i+1}, \ldots, q_\ell$ are not permutations of each other because otherwise $p_1, \ldots, p_k$ and $q_1, \ldots, q_\ell$ would have been permutations of each other. That means $\frac{n}{p_1}$ has two different prime factorizations and is a counter-example to statement (2) contradicting our assumption that n was the smallest counter-example.

But if there cannot be a smallest counter-example, there cannot be any counter-example at all, which means that (2) is true for all $n \in \mathbb{N}$. □

Item (1) of the Fundamental Theorem was proved by

> **Strong Induction.** To show that a statement S_n is true for every $n \in \mathbb{N}$:
>
> (1) **basis step:** Show S_1.
> (2) **inductive step:** Show $S_1 \wedge S_2 \wedge \cdots \wedge S_k \Rightarrow S_{k+1}$ for any $k \in \mathbb{N}$.

Induction is called strong if you use the induction assumption that all statements $S_1, \ldots, S_k$ hold, not just S_k, in order to prove S_{k+1}.

Item (2) of the Fundamental Theorem was proved by a special version of a proof by contradiction:

> **Proof by minimal counter-example.** To show that a statement S_n is true for every $n \in \mathbb{N}$:
> Suppose that $k > 1$ is smallest such that S_k is false. Show that there exists some smaller $\ell < k$ still such that S_ℓ is false.

Lemma 10. *Let $p_1 = 2, p_2 = 3, p_3, \ldots$ be the list of all primes. Let $a = \prod_{i \in \mathbb{N}} p_i^{e_i}, b = \prod_{i \in \mathbb{N}} p_i^{f_i}$ with $e_i, f_i \in \mathbb{N}_0$ for all $i \in \mathbb{N}$. Then*

(1) $\gcd(a, b) = \prod_{i \in \mathbb{N}} p_i^{\min(e_i, f_i)}$,
(2) $\operatorname{lcm}(a, b) = \prod_{i \in \mathbb{N}} p_i^{\max(e_i, f_i)}$,
(3) $\gcd(a, b) \cdot \operatorname{lcm}(a, b) = ab$.

Proof of (1). Let $d = \prod_{i \in \mathbb{N}} p_i^{g_i}$ be a divisor of a and of b. Let $i \in \mathbb{N}$ and $g_i \geq 1$. Then p^{g_i} cannot divide $\frac{a}{p^{e_i}}$ by the Fundamental Theorem of Arithmetic. So $p^{g_i} | p^{e_i}$ and $g_i \leq e_i$. Similarly $g_i \leq d_i$. In any case

$g_i \leq \min(e_i, f_i)$ (Note that this is also trivially true for $g_i = 0$). Hence for any common divisor d of a and b we have

$$d \leq \prod_{i \in \mathbb{N}} p_i^{\min(e_i, f_i)}.$$

But clearly $\prod_{i \in \mathbb{N}} p_i^{\min(e_i, f_i)}$ divides both a and b. Hence it is the gcd of a and b.

Proof of (2),(3). Exercise □