- $\mathbb{N}=\{1,2,3,\ldots\}$ are the **natural numbers**.
- $\mathbb{Z}=\{0,\pm1,\pm2,\ldots\}$ are the **integers** ("Zahlen").
- $\mathbb{Q}=\left\{\frac{p}{q}:\ p\in\mathbb{Z},q\in\mathbb{N}\right\}$ are the **rationals**.
- $\mathbb{R}$ are the **reals** (limits of sequences of rationals).
- $\mathbb{C}$ are the **complex numbers**.

**Advanced comment.** Number theory is also very much concerned with the study of the **algebraic numbers** $\bar{\mathbb{Q}}$, which are those numbers that are the roots of polynomials with integer coefficients. For instance, $\sqrt{5}$ (a root of $x^2-5$) and $i$ (a root of $x^2+1$) are examples of simple algebraic numbers (neither of which is rational).

**Comment.** The numbers $\pi$ and $e$ are probably the most fundamental mathematical constants, which are not rational. However, we understand the nature of these numbers so little that we do not even know whether $e+\pi$ is rational or not. (Overwhelming evidence suggests that $e+\pi$ is irrational but we do not have a proof.) Isn't that shocking and shameful?!

**Example 5.** $\sqrt{5}$ is not rational.

**Proof.** Assume (for contradiction) that we can write $\sqrt{5}=\frac{n}{m}$ with $n,m\in\mathbb{N}$. By canceling common factors, we can ensure that this fraction is reduced.

Then $5m^2=n^2$, from which we conclude that $n$ is divisible by $5$. Write $n=5k$ for some $k\in\mathbb{N}$. Then $5m^2=(5k)^2$ implies that $m^2=5k^2$. Hence, $m$ is also divisible by $5$. This contradicts the fact that the fraction $n/m$ is reduced. Hence, our initial assumption must have been wrong. □

**Variations.** Does the same proof apply to, say, $\sqrt{7}$? Which step of the proof fails for $\sqrt{4}$?

# 1 Divisibility

## 1.1 Quotients and remainders

**Theorem 6.** Let $a,b\in\mathbb{Z}$, with $b\neq0$. Then there exist unique integers $q$ and $r$ such that

$$a=qb+r,\quad 0\leqslant r<|b| \qquad \text{(that is, } \frac{a}{b}=q+\frac{r}{b}\text{)}.$$

$q$ is the **quotient**, and $r$ the **remainder** in the division of $a$ by $b$.

**Example 7.** For $a=20$, $b=6$, we have $\frac{20}{6}=3+\frac{2}{6}$. That is, $q=3$ and $r=2$.
For $a=20$, $b=5$, we have $\frac{20}{5}=4+\frac{0}{5}$. That is, $q=4$ and $r=0$.

**Example 8.** When $b=2$, then $r\in\{0,1\}$, and every integer is either of the form $2q$ or of the form $2q+1$. We call numbers **even** or **odd** correspondingly.

**Example 9.** Show that the square of an integer leaves the remainder $0$ or $1$ upon division by $4$.

That is, none of the squares $1,4,9,16,25,36,\ldots$ leave remainder $2$ or $3$ when dividing by $4$!!

**Proof.** Every integer is of the form $2q$ or $2q+1$. Upon division by $4$, $(2q)^2=4q^2$ leaves remainder $0$, $(2q+1)^2=4q^2+4q+1$ leaves remainder $1$.

**Example 10.** Show that the square of an integer leaves the remainder $0$ or $1$ upon division by $3$.

**Proof.** Every integer is of the form $3q$, $3q+1$ or $3q+2$. Upon division by $3$, $(3q)^2=9q^2$ leaves remainder $0$, while both $(3q+1)^2=9q^2+6q+1$ and $(3q+2)^2=9q^2+12q+4$ leave remainder $1$.

## 1.2 Greatest common divisor

**Definition 11.** Let $a, b \in \mathbb{Z}$ and $a \neq 0$. We write $a|b$ (and say $b$ is **divisible** by $a$) if $\frac{b}{a} \in \mathbb{Z}$.

In other words, $a|b$ if and only if there exists an integer $c$ such that $ac = b$.

**Example 12.** $3|9$ but $3 \nmid 10$.

**Definition 13.** Let $a, b \in \mathbb{Z}$ (not both zero). The **greatest common divisor** $\gcd(a, b)$ of $a$ and $b$ is the largest positive integer $c$ such that $c|a$ and $c|b$.

**Example 14.**

(a) $\gcd(2, 4) = 2$

(b) $\gcd(15, 28) = 1$

(c) $\gcd(30, 108) = \gcd(2 \cdot 3 \cdot 5, 2^2 \cdot 3^3) = 6$

(d) $\gcd(60, 2019) = \gcd(2^2 \cdot 3 \cdot 5, 3 \cdot 673) = 3$

**BAD?!** Computing $\gcd(a, b)$ by factoring $a$ and $b$ is not a good approach. Though small numbers might be easy to factor, it is very hard to factor even moderately large numbers in general.

Next class, we will learn about a good way to compute the gcd, which works well even for enormous numbers (in particular, it avoids factorizing the involved numbers).

Indeed, in 1991, RSA Laboratories challenged everyone to factor several numbers including:

135066410865995223349603216278805969938881475605667027524485143851526510604859533833940287150571909441798207282164471551373680419703964191743046496589274256239341020864383202110372958725762358509643110564073501\
508187510676594629205563685529475213500852879416377328533906109750544334999811150056977236890927563

Since then, nobody has been able to factor this 1024 bit number (309 decimal digits). Until 2007, cash prizes were offered up to 200,000 USD, with 100,000 USD for the number above (20,000 USD collected in 2005 for factoring a number with 193 decimal digits; 232 decimal digits factored in 2009, larger ones remain unfactored; largest one has 617 decimal digits). The reason people are very interested in factoring is that the difficulty of factoring is actually crucially used in many cryptosystems, including RSA.

https://en.wikipedia.org/wiki/RSA_Factoring_Challenge

**Course comment:**

Homework is posted after every class to our course website.

Today's homework is due online before Thursday, 8/29.