March 29, 2026 Math 8

Handout 22. Number theory 1: Introduction to divisibility.

Numbers

The oldest kind of numbers are "counting" numbers: 1, 2, 3, ... They can be described (not very rigorously) as the numbers you get if keep adding 1 to number 1. Mathematicians call them *natural numbers* and use letter ℕ to denote the set of all natural numbers:

$$\mathbb{N} = \{1,2,3, \dots\}$$

One problem with natural numbers is that if you want to be able to subtract two numbers, you might not be able to do so within ℕ. To deal with this problem, people have invented zero and negative numbers. Adding them to the set of natural numbers, we get the set of all *integer* numbers:

$$\mathbb{Z} = \{\dots, -3, -2, -1, 0, 1, 2, 3, \dots\} = \mathbb{N} \cup \{0\} \cup \{-n | n \in \mathbb{N}\}$$

In this assignment, the word "number" will mean "integer number" (unless explicitly stated otherwise).

As with Euclidean geometry, it is possible to build a rigorous theory of numbers by starting with a few axioms and proving everything else from them. This would take significant time, though. So instead, we take it for granted that for integer numbers, one has:

- Comparison relations: equalities, $m = n$, and inequalities, $m < n$, again satisfying the familiar number comparison rules (reflexivity, symmetry, transitivity)
    - $=$ equal to $7 = 5 + 2$ but not $7 = 5$
        - Reflexivity: $a = a$
        - Symmetry: $a = b \Rightarrow b = a$
        - Transitivity: $a = b, b = c \Rightarrow a = c$
    - $\neq$ not equal to $7 \neq 5$ but not $7 \neq 7$
        - Antireflexivity: $not\ a \neq a$
        - Symmetry: $a \neq b \Rightarrow b \neq a$
    - $<$ less than $5 < 7$ but not $5 < 5$
    - $>$ greater than $5 > 4$ but not $5 > 5$
        - Antireflexivity: $not\ a > a, not\ a < a$
        - Asymmetry: $a > b \Rightarrow not\ b > a, a < b \Rightarrow not\ b < a$
        - Transitivity: $a > b, b > c \Rightarrow a > c, a < b, b < c \Rightarrow a < c$
    - $\leq$ less than or equal to $5 \leq 7$, $5 \leq 5$, but not $7 \leq 5$
    - $\geq$ greater than or equal to $7 \geq 5$, $7 \geq 7$, but not $5 \geq 7$
        - Reflexivity: $a \leq a, a \geq a$
        - Antisymmetry: $a \leq b, b \leq a \Rightarrow a = b, a \geq b, b \geq a \Rightarrow a = b$
        - Transitivity: $a \leq b, b \leq c \Rightarrow a \leq c, a \geq b, b \geq c \Rightarrow a \geq c$
- Arithmetic operations: addition, multiplication, satisfying all the usual algebraic laws (commutativity, associativity, distributivity, . . .)

In addition, there is one more property which is used commonly:

- In any non-empty set of natural numbers, there must be the smallest number.

This is known as the well-ordering principle, or the principle of least integer, and is the foundation of the induction principle, which will be discussed in detail in Math 9. We will derive all other familiar properties of integers (such as prime factorization) from the ones above.

Divisors

We begin with some definitions and notations. Given integer numbers m, n, we say

- Number d is a divisor of m, or $d|m$, if $m = dk$ for some integer number k. (Also called a factor, with exactly the same meaning). In this situation we also say that m is a multiple of d.
- d is a common divisor of m, n if $(d|m) \wedge (d|n)$. (Also called a common factor)
- $d > 0$ is the greatest common divisor of m, n, written $d = gcd(m, n)$ or simply $d = (m, n)$, if d is greater than or equal to every common divisor of m, n.
- m, n are relatively prime if $gcd(m, n) = 1$. (Also called mutually prime, or co-prime).
- l is a common multiple of m, n if $(m|l) \wedge (n|l)$.
- $l > 0$ is the least common multiple of m, n, written $l = lcm(m, n)$, if l is less than or equal to every common multiple of m, n.

We will continue our numbers journey with the following theorems, which have interesting ramifications:

Theorem 1. If $d|m$ and $d|n$, then $d|(m - n)$ and $d|(m + n)$.

Proof. Since $d|m$, we have $m = ad$ for some a; similarly, $n = bd$ for some b (note: we can not use letter a – it has already been used!). Then $m - n = ad - bd = d(a - b)$ and similarly $m + n = d(a + b)$. Thus, $m - n$ and $m + n$ both have d as a divisor. □

Theorem 2. If d is a common divisor of m, n, then for any integers x, y, we have $d|(xm + yn)$.

Proof. Let $m = ad$ and $n = bd$. Then $xm + yn = xad + byd = d(xa + by)$. □

The following concept is known as division with remainder.

Theorem 3. Let d, n be natural numbers. Then there exists unique pair of numbers q, r, such that $0 \leq r < d$ and $n = qd + r$. The number r is called remainder upon division of n by d.

Proof. Here is the sketch of the proof. Consider the set of non-negative numbers $\{n, n - d, n - 2d, \dots\}$ (note: we only include numbers which are ≥ 0). Take the smallest number in this set; let it be $r = n - qd$. Then we must have $r < d$ (why?), so we get $n = qd + r$, and $0 \leq r < d$ as required. □

The same statement also works if we allow n be an arbitrary integer, not necessarily positive. However, d must be positive, otherwise inequality $0 \leq r < d$ makes no sense. For example, if $n = -13$, $d = 10$, then $-13 = -20 + 7 = (-2) \times 10 + 7$, so in this case the remainder is 7.

In particular, if we take d =2, then we see that possible remainders upon division by 2 are 0 and 1. Numbers which give remainder 0 upon division by 2 (i.e. are divisible by 2) are called even, those that give remainder 1 are called odd.

Prime numbers

Definition. A natural number m is prime if it has no positive divisors other than 1 and m itself.

- $m > 1$ is composite if it is not prime.
- $p > 0$ is a prime factor of m if $p|m$ and p is prime.

Note: number 1 is usually not considered composite; thus, it is the only natural number which is neither composite nor prime.

Theorem 4. Any number greater than 1 can be written as a product of one or more primes. This is called prime factorization of a number.

Proof. Proof by contradiction. Assume it is not so, i.e. there are numbers > 1 that cannot be written as products of primes. Take the smallest such number n. It can not be prime, so it is composite; thus $n = ab$, $1 < a < n$, $1 < b < n$. Since a, b are less than n, each of them is a product of primes. Multiplying these two products together, we get a formula for n as a product of primes. □

It is also true that prime factorization is unique (up to changing the order of factors), but it is a much more difficult result. We will discuss it later.

Theorem 5 (Euclid). There are infinitely many prime numbers.

Proof. Proof of this theorem is given to you as an exercise (see Problem 6). □

Homework problems

1. Is 0 divisible by 5? Is 5 divisible by 0?
2.
    a. Prove that if a is even, then ab is even for any b.
    b. Prove that if a, b are odd, then ab is also odd. [Hint: if a is odd then by definition, $a = 2k + 1$ for some k.]
3. If $a|b$ and $b|c$, show that $a|c$.
4. Show that the set of common divisors of m, n is the same as the set of common divisors of $m, m - n$: if d is a common divisor of m, n, then d is also a divisor of $m - n$, and conversely if d is a common divisor of $m, m - n$, then d is also a divisor of n. Deduce from this that $gcd(m, n) = gcd(m, m - n)$.
5. Use the previous problem to compute $gcd(1007,501)$ without factoring each of them.
6. Show that if $p_1, \dots, p_k$ are prime, then the number $p_1 p_2 \dots p_k + 1$ is not divisible by any of p_i. Deduce from this that there are infinitely many primes (hint: use proof by contradiction, starting with "Assume there are only finitely many prime numbers...")
7.
    a. Show that for any integer n, $n^{2020} - 1$ is divisible by $n - 1$. [Hint: geometric progression]
    b. Show that for any integer n, $n^{2020} + 1$ is divisible by $n + 1$. [Hint: write $n = -m$].

8. Prove that equation $p^2 = 2q^2$ has no integer solutions. (This means that $\sqrt{2}$ is not a rational number.) Hint: if p, q have common factors, divide both p and q by them until we get a pair with no common factors. Now use problem 2 to show that p must be even and then argue why q must also be even.