Monday: Binary operations

Binary operations

Definition. *Let A be a set. A* binary operation *on A is a function from $A \times A$ to A. [We usually omit the word "binary".] A* unary *operation on A is a function from A to A.*

We often use infix notation for binary operations. For example, if the operation is $*$, we write $x * y$ instead of $*(x, y)$.

Example 1. *The most familiar operations are $+$, $\cdot$ on $\mathbb{R}$ (or $\mathbb{Z}$ or $\mathbb{N}$ or $\mathbb{Q}$).*

Example 2. *The average operation given by*

$$\text{ave}(x, y) = \frac{x + y}{2}$$

is an operation on $\mathbb{R}$.

Example 3. *The exponentiation operation $\hat{}$ given by $x\hat{}y = x^y$ is an operation on $\mathbb{N}$.*

Example 4. *Subtraction is* **not** *an operation on $\mathbb{N}$, but it is an operation on $\mathbb{Z}$. Division is* **not** *an operation on $\mathbb{R}$.*

Example 5. *Let A be a set. Then $\cap$, $\cup$ and $\setminus$ are binary operations on $\mathcal{P}(A)$, and $\overset{c}{A}$ is a unary operation on $\mathcal{P}(A)$.*

The symmetric difference $\triangle$ on $\mathcal{P}(A)$, defined by $X \triangle Y = (X \cup Y) \setminus (X \cap Y)$ is an operation.

Definition. *An operation $*$ on A is* commutative *if for all $x, y \in A$ we have $x * y = y * x$.*

Exercise 6. *Which of the above operations are commutative?*

Definition. *An operation $*$ on A is* associative *if for all $x, y, z \in A$ we have $x * (y * z) = (x * y) * z$.*

Exercise 7. *Which of the above operations are associative?*

Definition. *Let $*$ be an operation on A. An* identity *element is an $e \in A$ with the property that for all $x \in A$, $e * x = x * e = x$.*

Exercise 8. *Which of the above operations have an identity element?*

Tuesday: The Natural Numbers and the Integers

The Natural Numbers and the Integers [6.1]

Our next topic is *Number Theory*. This is the study of the arithmetic of the natural numbers $\mathbb{N}$ and the integers $\mathbb{Z}$. Although this might seem a very simple area, in fact there are some problems which have so far been impossible to solve, despite being very easy to state. The simplest is probably the "Twin Prime

Conjecture": the statement that there are infinitely many numbers n such that n and $n+2$ are both prime. Nobody knows whether this statement is true or false.

It is important to put the theory on a firm foundation: it would be a waste of time for me to convince myself that I have a proof of the twin prime conjecture, and for me to try to convince you, only for you to say that you disagree with my initial assumptions. So the first thing we do when we are studying number theory is to give our *axioms*. In principle, at least, everything we prove in number theory should come just from these axioms and not from our intuition of what the natural numbers look like (though, of course, we may use our intuition to find the proof in the first place: the point is that the proof must not **rely** on that intuition).

Our axioms for the natural numbers and integers are the following:

- $\mathbb{N}$ and $\mathbb{Z}$ are endowed with two commutative and associative operations, $+$ and $\cdot$. (As usual, we abbreviate $a \cdot b$ as ab). Multiplication distributes over addition, i.e. for all $x, y, z \in Z$ we have $x(y+z) = xy + xz$.
- We have two unique, distinct integers 0 and 1 with the properties that $x + 0 = x$ for all $x \in \mathbb{Z}$ and $1x = x$ for all $x \in \mathbb{Z}$ (in other words, 0 is an identity for $+$ and 1 is an identity for $\cdot$).
- Every $m \in \mathbb{Z}$ has an *additive inverse*, that is an integer $-m$ with the property that $m + (-m) = 0$. We abbreviate $m + (-n)$ by $m - n$.
- $\mathbb{N}$ and $\mathbb{Z}$ have a total order $\leq$ which meshes with $+$ in $\cdot$ in the following way: for any $x, y, z \in \mathbb{Z}$, $x \leq y \iff x + z \leq y + z$ and for any $x, y \in \mathbb{Z}$ and $z \in \mathbb{N}$, $x \leq y$ iff $xz \leq yz$. Further, $n+1$ is an immediate successor of n for each $n \in \mathbb{Z}$, i.e. $n < n+1$ and there is no z with $n < z < n+1$.
- $\mathbb{N}$ satisfies the induction axiom: if $S \subseteq \mathbb{N}$ with $1 \in S$ and, for each $s \in S$, $s+1 \in S$, then $S = \mathbb{N}$.
- $\mathbb{Z} = \mathbb{N} \cup \{0\} \cup \{ -n : n \in \mathbb{N} \}$.

Every other property we need about $\mathbb{N}$ and $\mathbb{Z}$ can be deduced from these assumptions. For example, we can **prove** that $\mathbb{N} = \{ n \in \mathbb{Z} : 0 < n \}$. Of course we already knew this, so what is the point? The point is that there is no **alternative** ordering, different from the standard one, which satisfies all the axioms but has $n < 0$ for some $n \in \mathbb{N}$.

Definition. *A poset $(A, \preceq)$ is* well-ordered *if every non-empty subset has a least element. [Notice that if $\{x, y\}$ has a least element, then the least element is either x or y: if x is a least element then $x \preceq y$ and if y is a least element then $y \preceq x$. Thus, for every $x, y \in A$ we have $x \preceq y$ or $y \preceq x$, so a well-ordered set is totally ordered.]*

Example 9. *$(\mathbb{Z}, \leq)$ is* **not** *well-ordered, and neither is $([0,1], \leq)$.*

Theorem 10 (Well ordering of $\mathbb{N}$). *$\mathbb{N}$ is well-ordered by the usual order $\leq$.*

Proof. Let $S \subseteq \mathbb{N}$. We must prove that if $S \neq \emptyset$ then S has a least element: by contraposition it is enough to prove that if S has no least element then $S = \emptyset$. So suppose S has no least element. We prove by complete induction that for all $n \in \mathbb{N}$, $n \notin S$, from which it follows that $S = \emptyset$. □

The following follows from the well ordering of $\mathbb{N}$:

Theorem 11. *If $S \subseteq \mathbb{Z}$ is non-empty and bounded below then it has a least element. If S is non-empty and bounded above then it has a greatest element.*

Thursday: Least common multiples and greatest common divisors

Divisibility in $\mathbb{Z}$ [6.2]

Theorem 12 (The Division Algorithm). *For any $m \in \mathbb{Z}$ and $n \in \mathbb{N}$, there exist unique integers q and r with $0 \leq r < n$ and $m = qn + r$. We call q the* quotient *and r the* remainder *when m is divided by n.*

Proof. If $m, n \in \mathbb{N}$ then there exist $q, r \in \mathbb{Z}$ with $0 \leq r < n$ and $m = qn + r$.

If $n = 1$ then $m = mn + 0$, so there is no work to be done. So we will assume that $n > 1$. Let P_m be the statement "There exist integers q and r such that $m = qn + r$ and $0 \leq r < n$".

Base case: $(m = 1)$. We have $1 = 0n + 1$, and $0 \leq 1 < n$, so P_1 is true.

Inductive step: Suppose $m \in \mathbb{N}$ and P_j is true for $1 \leq j \leq m$. We consider three cases: $m + 1 < n$, $m + 1 = n$ or $m + 1 > n$.

Case 1: if $m + 1 < n$ then we have $m + 1 = 0n + (m + 1)$ and $0 \leq m + 1 < n$.

Case 2: if $m + 1 = n$ then we have $m + 1 = 1n + 0$ and $0 \leq 0 < n$.

Case 3: if $m+1 > n$, put $j = (m+1)-n$. Then $1 \leq j \leq m$, so by the ind. hyp. there exist $q_j, r_j \in \mathbb{Z}$ with $0 \leq r_j < n$ and $j = q_j n + r_j$. But then $m + 1 = j + n = (q_j n + r_j) + n = (q_j + 1)n + r_j$.

So, whichever case holds, P_{m+1} is true.

Hence, by complete induction, P_m is true for all $m \in \mathbb{N}$.

We only dealt with the case when $m > 0$: we leave the cases $m = 0$ and $m < 0$ as an exercise.

For uniqueness, suppose $q_1, q_2, r_1, r_2 \in \mathbb{Z}$ with $0 \leq r_1, r_2 < n$ and $m = q_1 n + r_1 = q_2 n + r_2$. We must show that $q_1 = q_2$ and $r_1 = r_2$.

Rearranging the above, we know that $(q_1 - q_2)n = r_2 - r_1$.

Suppose for a contradiction that $r_1 \neq r_2$. WLOG $r_1 < r_2$. So $r_2 - r_1 > 0$, so $(q_1 - q_2)n > 0$, so $(q_1 - q_2) > 0$, so $(q_1 - q_2) \geq 1$, so $(q_1 - q_2)n \geq n$. But then $r_2 - r_1 \geq n$, and yet $r_2 - r_1 \leq r_2 - 0 = r_2 < n$, a contradiction. So we must have $r_1 = r_2$. But then we have $(q_1 - q_2)n = 0$, and $n \neq 0$, so $q_1 - q_2 = 0$, so $q_1 = q_2$ also. □

Recall that the relation $\mid$ is defined on $\mathbb{Z}$ by $m \mid n$ iff there is some $a \in \mathbb{Z}$ with $ma = n$. This gives us a partial order on $\mathbb{N}$: more generally we have the following, for any $a, b \in \mathbb{Z}$:

- $a \mid a$;
- $1 \mid a$ and $-1 \mid a$;
- $a \mid 0$;
- if $b \mid a$ then $b \mid (-a)$;
- if $a \mid b$ and $b \neq 0$ then $|a| \leq |b|$;
- if $a \mid b$ and $b \mid a$ then $a = \pm b$;

- if $a \mid b$ and $b \mid c$ then $a \mid c$.

Thus $\mid$ is a partial order on $\mathbb{N}$. We have a special name for greatest lower bounds and least upper bounds in this partial order.

Definition. *Let $a, b \in \mathbb{Z}$. We say that d is a* common divisor *of a and b if $d \mid a$ and $d \mid b$. We say that m is a* common multiple *of a and b if $a \mid m$ and $b \mid m$. We say that a and b are* relatively prime *if a and b have no positive common divisors other than 1.*

Definition. *Let $a, b \in \mathbb{N}$. The set of common divisors of a and b is bounded above by a and is nonempty (since it contains 1, so it has a greatest element. The set of positive common multiples of a and b is bounded below by a and is nonempty (since it contains ab), so it has a least element. We call these, respectively, the* greatest common divisor *of a and b,* $\gcd(a, b)$*, and the* least common multiple *of a and b,* $\operatorname{lcm}(a, b)$.

Theorem 13. *Let $a, b \in \mathbb{N}$. If c is a common divisor of a and b then $c \mid \gcd(a, b)$. If m is a common multiple of a and b then $\operatorname{lcm}(a, b) \mid m$.*

The Euclidean Algorithm [6.3]

Theorem 14. *Let $a, b, r \in \mathbb{N}$ with $a = qb + r$. Then $\gcd(a, b) = \gcd(b, r)$.*

Proof. Exercise. □

So, to find $\gcd(a, b)$, we can divide b into a, and reduce the problem to the simpler one of finding $\gcd(b, r)$. To do this we divide r into b and get a simpler problem still.... This carries on until one of the remainders is zero: of course if $b = qa + 0$, then $\gcd(a, b) = b$.

Example 15. *Find* $\gcd(36, 15)$.

Solution. We have

$$\begin{aligned} 36 &= 2 \cdot 15 + 6 \\ 15 &= 2 \cdot 6 + 3 \\ 6 &= 2 \cdot 3 + 0 \end{aligned}$$

The last non-zero remainder is 3, so $\gcd(36, 15) = 3$. □

Theorem 16. *Let $a, b \in \mathbb{N}$. Let $d = \gcd(a, b)$. Then there exist integers x and y such that $d = ax + by$.*

Proof. Put

$$S = \{\, n \in \mathbb{N} : (\exists x, y \in \mathbb{Z})(n = ax + by) \,\}.$$

Then S is a non-empty subset of $\mathbb{N}$, so it has a least element, k say. Since $k \in S$, we have $k = ax + by$ for some x, y.

Suppose, for a contradiction that $k \nmid a$. So we can write $a = qk + r$ with $k, r \in \mathbb{Z}$ and $0 < r < k$. Then $r = a - qk = a - q(ax + by) = a(1 - qx) + b(-qy)$, so $r \in S$, contradicting the assumption that k was the least element of S. Wo we cannot have $k \nmid a$, so $k \mid a$. Similarly, $k \mid b$.

If c is a common divisor of a and b, $a = cm$ and $b = cn$. So $k = ax + by = cmx + cny = c(mx + ny)$ so $c \mid k$ and hence k is greatest common divisor, as required, so $k = d$. □

We can find x and y using an modified version of the Euclidean algorithm, where we write three columns, n, x and y: each row represents an equation $n = ax + by$. Again, with the $\gcd(36, 15)$ example we get

n	x	y	
36	1	0	r_1
15	0	1	r_2
6	1	-2	$r_3 = r_1 - 2r_2$
3	-2	5	$r_4 = r_2 - 2r_3$
0	5	-12	$r_5 = r_3 - 2r_4$

From the second last row we see that $\gcd(36, 15) = 3$ and that $3 = (-2) \cdot 36 + 5 \cdot 15$. Incidentally the last row shows us that $\text{lcm}(36, 15) = 5 \cdot 36 = 12 \cdot 15$.

Friday: Prime numbers, relatively prime numbers and prime factorization

Definition. *A number $p \in \mathbb{N}$ is* prime *if $p > 1$ and p has no positive divisors other than 1 and p. A number n is* composite *if $n = ab$ for some $a, b \in \mathbb{N}$ with $1 < a, b < n$. So every natural number greater than 1 is either prime or composite but not both. [NB the definition in the textbook includes 1 as a composite number, but this is not standard.]*

Theorem 17. *Let $r, s \in \mathbb{Z}$. Suppose r and s are relatively prime. Then r and $r + s$ are relatively prime.*

Theorem 18. *Let $a, b \in \mathbb{Z}$. Then a and b are relatively prime iff there exist $x, y \in Z$ with $ax + by = 1$.*

Theorem 19. *Let $a, b, c \in Z$ with a and b relatively prime. If $a \mid bc$ then $a \mid c$.*

Proof. Suppose $a \mid bc$. Then there is some $z \in \mathbb{Z}$ with $bc = az$. Also, we know that there exist $x, y \in \mathbb{Z}$ with $ax + by = 1$. We have

$$c = c \cdot 1 = c(ax + by) = a(cx) + (bc)y = a(cx) + (az)y = a(cx + zy).$$

Since $cx + zy \in \mathbb{Z}$, $a \mid c$ as required. □

Theorem 20. *Let p be a prime number, $a, b \in \mathbb{Z}$. If $p \mid ab$ then $p \mid a$ or $p \mid b$.*

Proof. Suppose p is prime and $p \not| a$. We must show that in that case, $p \mid b$. Now, $\gcd(a, p) | p$, and the only positive divisors of p are 1 and p. Since $p \not| a$, we cannot have $\gcd(a, p) = p$, so $\gcd(a, p) = 1$, in other words a and p are relatively prime. So, by the previous result, since $p \mid ab$ we have $p \mid b$, as required. □

Theorem 21. *If $m_1, m_2, \ldots, m_k$ are integers, p is a prime number and $p \mid m_1 m_2 \cdots m_k$ then $p \mid m_i$ for some i.*

Proof. Use induction on k. □

Theorem 22 (The fundamental theorem of arithmetic). *Every natural number greater than 1 can be written as a product of prime numbers, and that factorization is unique up to the order of the factors.*