

Four Basic Sets

\mathbb{Z} = the integers

\mathbb{Q} = the rationals

\mathbb{R} = the real numbers

\mathbb{C} = the complex numbers

Divisors

Definition 1. Suppose $a \neq 0$ and $b = ax$, where a , b , and x are integers. Then we say a **divides** b (or a is a **divisor** of b or b is a **multiple** of a).

Notation: Write $a|b$ for a divides b and $a \nmid b$ for a does not divide b .

Example: $2|12$, $3 \nmid 20$.

Divisor Facts

For each of the following divisibility statements, (1) give an example and (2) give an argument explaining why the statement is true. Here a , b , c , r , and s are integers.

(1) $a|b$ implies $a|rb$

(2) $a|b$ and $b|c$ implies $a|c$

(3) $a|b$ and $a|c$ implies $a|rb + sc$

(3') [Special case of (3)] $a|b$ and $a|c$ implies $a|b + c$ and $a|b - c$

(4) $a|b$ and $b|a$ implies $a = \pm b$

(5) $a|b$, $a > 0$, $b > 0$ implies $a \leq b$

(6) What can you say about $a|b$ (i) if $b = 0$; (ii) if $a = 1$?

The Division Algorithm

The Division Algorithm. Suppose a and b are integers and $a > 0$. Then there is a unique pair of integers q and r such that

$$b = aq + r \quad \text{where} \quad 0 \leq r < a.$$

Examples. (a) 23 and 5; (b) 17 and 3; (c) 666 and 21.

Well Ordering

Well Ordering Principle. A nonempty set S of nonnegative integers always contains a smallest element m , that is, m satisfies the following two conditions: (i) m is in S and (ii) $m \leq n$ for every number n in S .

Example. There is a smallest prime.

Example. All positive integers are interesting.

Proof 1 of the Division Algorithm. Use Well-Ordering Principle.

Use the set S consisting of all numbers of the form $b - n \cdot a$, where (i) n ranges over all integers in \mathbb{Z} and (ii) $b - n \cdot a \geq 0$.

INDUCTION

Principle of Induction $P(n)$ is a statement about the positive integer n . In order to show that $P(n)$ is true for all positive integers n , it suffices to show that

(i) *First Case:* $P(1)$ is true;

(ii) *Next Case:* If $P(n)$ is true for the integer n , then statement P is true for the next integer $n + 1$.

Example: Find the sum of consecutive odd numbers. Let's experiment:

$$1 = 1$$

$$1 + 3 = 4$$

$$1 + 3 + 5 = 9$$

$$1 + 3 + 5 + 7 = 16$$

Question: What is the pattern 1, 4, 9, 16?

Answer: They are all squares.

Question: Does this pattern continue for the next sum when $n = 5$?

Answer: Let's check:

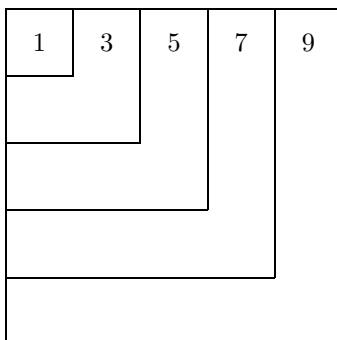
$$1 + 3 + 5 + 7 + 9 = 16 + 9 = 25,$$

another square.

Conjectured Formula:

$$1 + 3 + 5 + \cdots + (2n - 1) = n^2$$

Geometric Proof: For example, when $n = 5$, we can decompose a 5 square into five L-shaped pieces whose area are 1, 3, 5, 7, and 9.



Induction Proof:

$$P(n) : 1 + 3 + 5 + \cdots + (2n - 1) = n^2$$

First Step: $P(1)$ is true: $1 = 1$

Next Step: Assume $P(n)$ is true and show that $P(n + 1)$ is also true. The idea is to start with the formula $P(n)$. Add the next odd number $2(n + 1) - 1$ to both sides, and hopefully transform the equation into $P(n + 1)$, like this:

$$\begin{aligned} 1 + 3 + 5 + \cdots + (2n - 1) &= n^2 && [P(n)] \\ 1 + 3 + 5 + \cdots + (2n - 1) + (2(n + 1) - 1) &= n^2 + 2(n + 1) + 1 && [\text{add } 2(n + 1) + 1] \\ 1 + 3 + 5 + \cdots + (2n - 1) + (2(n + 1) - 1) &= n^2 + 2n + 1 && [\text{algebra}] \\ 1 + 3 + 5 + \cdots + (2n - 1) + (2(n + 1) - 1) &= (n + 1)^2 && [P(n + 1)] \end{aligned}$$

Proof 2 of the Division Algorithm. Induction.

We can verify the division algorithm by induction on the variable b . It simplifies the discussion to assume that the divisor a is greater than 1.

First Step: $b = 1$. Here

$$1 = 0 \times a + 1$$

When $b = 1$, the quotient is $q = 0$ and the remainder is $r = 1$.

Next step: Assume the division algorithm holds for the positive integer b , that is, assume

$$b = q \times a + r$$

Can we figure out the values of q and r for $b + 1$? That's easy.

$$b + 1 = q \times a + (r + 1)$$

Use the old value of q and just increase r by 1.

Wait a minute. What if $r = a - 1$? When we add 1 to r , the new value will not lie between 0 and $a - 1$.

For example, if $a = 5$ and $b = 22$, then from $22 = 4 \times 5 + 2$ we get the next statement $23 = 4 \times 5 + 3$. But if we start with $24 = 4 \times 5 + 4$, the next statement becomes $25 = 4 \times 5 + 5$, which is true, but the remainder 5 does not lie in the required range.

How can we handle this case?

What about the case where b is negative?

What about the case where $a = 1$?

The Floor Function

For any real number x , the **floor** of x , written $\lfloor x \rfloor$ is defined to be the largest integer n such that $n \leq x$. $\lfloor x \rfloor$ is also called the **greatest integer** function.

For example, $\lfloor \pi \rfloor = 3$, $\lfloor \sqrt{2} \rfloor = 1$, $\lfloor -6.57 \rfloor = -7$.

Note that if $n = \lfloor x \rfloor$, then $n \leq x < n + 1$.

Proof 3 of the Division Algorithm. Use the floor function.

Given integers $a > 0$ and b , let $q = \lfloor \frac{b}{a} \rfloor$. Then

$$\begin{aligned} q &\leq \frac{b}{a} < q + 1 \\ \implies qa &\leq b < (q + 1)a \\ \implies 0 &\leq b - qa < a \end{aligned}$$

Let $r = b - qa$. It follows that the only choices for the integer r are $0, 1, 2, \dots, a - 1$.

What about uniqueness?

Suppose Tom divides b by a and gets

$$b = q_1a + r_1$$

and Becky divides b by a and gets

$$b = q_2a + r_2.$$

Is it possible that both Tom and Becky could have correct, but different, answers?

Calculus Example: Find an antiderivative of $(x + 1)^2$

Tom: $\frac{1}{3}(x + 1)^3$

Becky: $\frac{1}{3}x^3 + x^2 + x$

Proof of uniqueness of q and r : We have

$$\begin{aligned} q_1a + r_1 &= q_2a + r_2 \\ \implies (q_1 - q_2)a &= r_2 - r_1 \\ \implies a &| r_2 - r_1 \end{aligned}$$

We know

$$\begin{aligned} 0 &\leq r_1 \leq a - 1 \text{ and } 0 \leq r_2 \leq a - 1 \\ \implies 0 &\leq r_1 \leq a - 1 \text{ and } -(a - 1) \leq -r_2 \leq 0 \\ \implies -(a - 1) &\leq r_1 - r_2 \leq a - 1 \\ \implies |r_1 - r_2| &\leq a - 1. \end{aligned}$$

Fact (5) about division says that if $a|r_1 - r_2$, $a > 0$, and $r_1 - r_2 \neq 0$, then $a \leq |r_1 - r_2|$. Assuming $r_1 - r_2 \neq 0$ puts us in a bind: $a \leq |r_1 - r_2|$ and $|r_1 - r_2| < a$. The only way out of this bind is to have $r_1 - r_2 = 0$, or $r_1 = r_2$.

Why does this imply $q_1 = q_2$?