

# Proof a Day — 2026

Alexander Crabtree

## Contents

<b>1</b>	<b>Weeks 1–13</b>	<b>2</b>
1.1	Week 1 (Jan 1–Jan 7) . . . . .	2
	2026-01-01 — Divisibility . . . . .	2
	2026-01-02 — Divisibility . . . . .	2
	2026-01-03 — Divisibility . . . . .	2
	2026-01-04 — Rings . . . . .	2
	2026-01-05 — Rings . . . . .	3

# 1 Weeks 1–13

## 1.1 Week 1 (Jan 1–Jan 7)

2026-01-01

Divisibility

**Theorem 1.1.** *If  $a|c$  and  $b|c$  and  $\gcd(a, b) = d$ , then  $ab|cd$ .  $a, b, c \in \mathbb{Z}$*

*Proof.* As  $d = \gcd(a, b)$ , we have that  $d = au + bv$  for some  $u, v \in \mathbb{Z}$ . We now have that  $cd = c(au + bv) = cau + cbv$ . Since  $a|c$  and  $b|c$ ,  $c = ax = by$  for some  $x, y \in \mathbb{Z}$ . Substituting  $c$  results in  $cd = cau + cbv = (by)au + (ax)bv = (ab)(yu + xv)$ . As  $u, v, x, y \in \mathbb{Z}$ ,  $yu + xv \in \mathbb{Z}$ . By definition of divisibility,  $ab|cd$ .  $\square$

2026-01-02

Divisibility

**Theorem 1.2.** *If  $a|bc$  and  $\gcd(a, b) = 1$ , then  $a|c$ .*

*Proof.* Assume that  $a|bc$  and  $\gcd(a, b) = 1$ . As  $a$  and  $b$  are relatively prime,  $au + bv = 1$  for some  $u, v \in \mathbb{Z}$ . If we multiply  $au + bv = 1$  by  $c$ , then we have  $cau + cbv = c$ . As  $a|bc$ ,  $bc = ax$  for some  $x \in \mathbb{Z}$ . Now, we have that

$$c = cau + cbv = cau + bcv = cau + (ax)v = a(cu + xv)$$

Since  $c, u, x, v \in \mathbb{Z}$  and by the definition of divisibility,  $a|c$ .  $\square$

2026-01-03

Divisibility

**Theorem 1.3.** *If  $\gcd(a, c) = 1$  and  $\gcd(b, c) = 1$ , then  $\gcd(ab, c) = 1$ .*

*Proof.* By way of contradiction, assume that  $\gcd(ab, c) \neq 1$ . Thus, there exists a prime  $p$  such that

$$p|ab \text{ and } p|c.$$

Since  $p$  is prime,  $p|a$  or  $p|b$ . If  $p|a$ , then  $\gcd(a, c) \geq p > 1$ , which contradicts the assumption that  $\gcd(a, c) = 1$ . If  $p|b$ , then  $\gcd(b, c) \geq p > 1$ , which contradicts the assumption that  $\gcd(b, c) = 1$ . Therefore  $ab$  and  $c$  share no such prime factors  $p$ , so  $\gcd(ab, c) = 1$ .  $\square$

2026-01-04

Rings

**Theorem 1.4.** *If  $a + b = a + c$  in a ring  $R$ , then  $b = c$ .*

*Proof.* Assume that for  $a, b, c \in R$ ,  $a + b = a + c$ . If we add  $-a$  and by using the associativity property of rings and negatives, we can show that

$$\begin{aligned} -a + (a + b) &= -a + (a + c) \\ (-a + a) + b &= (-a + a) + c \\ 0_R + b &= 0_R + c \\ b &= c \end{aligned}$$

□

**2026-01-05**

Rings

**Theorem 1.5.** *If  $a \neq 0_R$  and  $ab = ac$  in an integral domain  $R$ , then  $b = c$ .*

*Proof.* If  $ab = ac$ , then  $ab - ac = 0_R$ . Thus,  $a(b - c) = 0_R$ . As  $R$  is an integral domain and  $a \neq 0_R$ , it must be that  $b - c = 0_R$ . If  $b - c \neq 0_R$ , then  $a$  would be a zero divisor contradicting the zero-product property of integral domains. Thus  $b = c$ .

□