

## Introduction to Number Theory

Given integers  $a$  and  $b$ , we say that  $a$  divides  $b$  (denoted  $a|b$ ) iff  $b = ka$  for some integer  $k$ . Here are some facts that you will be able to easily verify:

- a. If  $a|b$ , then  $a|kb$ ,  $ka|kb$ .
- b. If  $ka|kb$  and  $k \neq 0$ , then  $a|b$ .
- c. If  $a|b$  and  $b|c$ , then  $a|c$ .
- d. If  $a|b$  and  $a|c$ , then  $a|(mb + nc)$ .
- e. If  $a|b$  and  $b|a$ , then  $a = \pm b$ .
- f. If  $a|b$ ,  $a, b > 0$ , then  $a \geq b$ .
- g. For any choice of  $a, b$ , there exists a unique  $q, r$ ,  $0 \leq r < a$  s.t.  $b = qa + r$ , and  $r = 0 \iff a|b$ .

Given a prime  $p$  and an integer  $b$ , we say that  $p^k$  **fully divides**  $b$  (denoted  $p^k || b$  iff  $p^k | b$  but  $p^{k+1} \nmid b$ , that is, if  $k$  is the largest exponent of  $p$  that makes  $p^k$  a divisor.

Given any two integers  $a$  and  $b$ , the **greatest common divisor** is the largest integer that divides both  $a$  and  $b$ . This is denoted  $\gcd(a, b)$  or, in some cases, simply  $(a, b)$ . Bezout's identity offers another way of thinking about the greatest common divisor:

**Theorem 1** (Bezout's Identity). Given integers  $a, b$ , then  $\gcd(a, b) = g$  iff there exist integers  $x$  and  $y$  such that  $ax + by = g$ . Stated more generally, given integers  $a_1, a_2, \dots, a_n$ , then  $\gcd(a_1, a_2, \dots, a_n) = g$  iff there exist integers  $x_1, x_2, \dots, x_n$  such that  $a_1x_1 + a_2x_2 + \dots + a_nx_n = g$ . (This can be proved from the  $n = 2$  case by using the fact that  $\gcd(a, b, c) = \gcd(\gcd(a, b), c)$ .)

This theorem can be used to prove a number of useful facts about the GCD that may seem intuitively obvious. (All variables are assumed to represent integers unless otherwise noted.)

- a.  $\gcd(ma, mb) = m \cdot \gcd(a, b)$
- b. If  $d|a$ ,  $d|b$ , and  $d > 0$ , then  $\gcd\left(\frac{a}{d}, \frac{b}{d}\right) = \frac{1}{d} \gcd(a, b)$ .
- c. If  $\gcd(a, m) = \gcd(b, m) = 1$ , then  $\gcd(ab, m) = 1$ .
- d. If  $\gcd(a, b) = 1$ , then  $a$  and  $b$  are said to be **relatively prime**; this is denoted as  $a \perp b$ .
- e. If  $c|ab$  and  $\gcd(b, c) = 1$ , then  $c|a$ .

**Problem 1.** Is it possible to measure out 1 pint of water using only a 9-pint and 16-pint container?

The canonical method for calculating the gcd of two numbers is to use the Euclidean algorithm, which is based on the fact that

$$\gcd(a, b) = \gcd(a, b - a) = \gcd(a - b, b).$$

(This can be proved by noting that  $a = bm + r$  implies that  $\gcd(r, b) = \gcd(a, b)$ .)

**Problem 2** (HMMT 2004). Compute  $\gcd(2002 + 2, 2002^2 + 2, 2002^3 + 2, \dots)$ .

The **least common multiple** of a pair of numbers  $a, b$  is the smallest integer that is divisible by both  $a$  and  $b$ . This is often denoted  $\text{lcm}(a, b)$  or simply  $[a, b]$ . It is a remarkable fact that

$$\gcd(a, b) \cdot \text{lcm}(a, b) = ab.$$

This can be proven by examining individual primes. But here we offer a nicer proof:

$b|m$  and  $a|m$ , so  $ab|ma$  and  $ab|mb$ . So  $\frac{ab}{m}|a$  and  $\frac{ab}{m}|b$ . But by the definition of  $d$ , if  $x|a$  and  $x|b$ , then  $x|d$ . In this case, we have  $x = \frac{ab}{m}$ , and so  $\frac{ab}{m}|d$ , or  $ab|md$ .

But  $d|a$  and  $d|b$ , so  $db|ab$  and  $da|ab$ . So  $b|\frac{ab}{d}$  and  $a|\frac{ab}{d}$ . But by the definition of  $m$ , if  $a|y$  and  $b|y$ , then  $m|y$ . In this case, we have  $y = \frac{ab}{d}$ , and so  $m|\frac{ab}{d}$ , or  $md|ab$ .

The only way that we can have  $ab|md$  and  $md|ab$  is if  $ab = md$ , as desired.

**Problem 3** (Russia 1995). Let  $a$  and  $b$  be positive integers such that  $\text{lcm}(a, b) + \text{gcd}(a, b) = a + b$ . Prove that one number is divisible by the other.

**Problem 4**. Prove that, if the terms of an infinite arithmetic progression of natural numbers are not all equal, they cannot all be primes.

**Problem 5**. The numbers 1059, 1417, and 2312, when all leave the same remainder  $r$  when divided by some integer  $d$ . Find  $d$  and  $r$ .

**Problem 6**. You are given any 51 integers taken from 1, 2, ..., 100. Prove that there are two that are relatively prime.

**Problem 7**. Compute

$$\frac{\text{lcm}(2, 4, 6, \dots, 100)}{\text{lcm}(1, 2, 3, \dots, 50)}.$$

**Problem 8**. Let  $(a, b) = 1$ . Prove that  $(a + b, a^2 - ab + b^2) = 1$  or 3.

**Problem 9**. The product of the greatest common factor and least common multiple of two numbers is 384. If one number is 8 more than the other number, compute the sum of two numbers.

**Problem 10** (AIME I 2007 #4). Three planets revolve about a star in coplanar circular orbits with the star at the center. All planets revolve in the same direction, each at a constant speed, and the periods of their orbits are 60, 84, 140 years each. The positions of the star and all three planets are currently collinear. They will next be collinear after  $n$  years. Find  $n$ .

**Problem 11**. Prove that  $\text{gcd}(a^m - 1, a^n - 1) = a^{\text{gcd}(m, n)} - 1$ .

**Problem 12**. Prove that any two consecutive terms of the Fibonacci sequence are relatively prime.

**Problem 13** (AIME 1987 #7). Let  $[r, s]$  denote the least common multiple of positive integers  $r$  and  $s$ . Find the number of ordered triples  $(a, b, c)$  of positive integers for which  $[a, b] = 1000$ ,  $[b, c] = 2000$ , and  $[c, a] = 2000$ .

**Problem 14** (UK 1998). Let  $x, y, z$  be positive integers such that  $\frac{1}{x} - \frac{1}{y} = \frac{1}{z}$ . Let  $h = \text{gcd}(x, y, z)$ . Prove that  $hxyz$  and  $h(y - x)$  are perfect squares.