The Greatest Common Divisor and Euclidean Algorithm

Konstantin Miagkov, Los Angeles Math Circle

7 March 2021

Greatest Common Divisor

For the first half of this handout, we take a look at the greatest common divisor.

Definition 1.

The *greatest common divisor* (GCD) of two positive integers a, b is the biggest integer d such that $d|a$ and $d|b$. We denote the GCD of a and b by $\gcd(a, b)$.

Problem 1.

Compute the GCD of 47124 and 11050.

Problem 2.

a) Let a, b be positive integers, and $r > 0$ be the remainder of a when divided by b. Then $a = bq + r$ where q is an integer. Let S be the set of all common divisors of a and b, and let T be the set of common divisors of b and r. Prove that $S = T$.

   Hint: if you want to show that two sets are equal, you need to show that every element of S is also an element of T and vice-versa.

b) Prove that gcd(a, b)=gcd(b, r).

Problem 3.

Show that the fraction

$$\frac{12n+1}{30n+1}$$

is irreducible for all positive integers n (i.e., if you plug in a positive integer for n the resulting fraction cannot be further factored).

Problem 4.

Can the GCD of two distinct positive integers be bigger than their differences?

Euclid's Division Algorithm

We now take a look at the Euclidean algorithm (division algorithm).

Problem 1.

Compute:

1. The remainder of -7 when divided by -2.

2. The remainder of -153 when divided by 15.

3. The remainder of 153 when divided by -15.

Problem 2.

Show that a prime number greater than 3 can be expressed as $6n + 1$ or $6n + 5$ for some nonnegative integer n.

Problem 3.

a) Find 3 distinct positive integers greater than 1 such that the product of any two is divisible by the third.

b) Show how to construct infinitely many such examples.