Lesson 6: Greatest Common Divisor

Konstantin Miagkov

May 5, 2019

Definition 1.
The *greatest common divisor* (GCD) of two positive integers a, b is the biggest positive integer d such that $d \mid a$ and $d \mid b$. We denote the GCD of a and b by $\gcd(a, b)$.

Problem 1.
Compute the GCD of 47124 and 11050.
Hint: answer is 34*, which can be determined by going through the divisors.*

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.

Proof. Suppose d is an element of S, that is d is a common divisor of a and b. Since $r = a - bq$, we get that d is a divisor of r and thus d is in T. Similarly if d is in T and thus is a common divisor of r and b, we have $a = bq + r$ and thus d is also a divisor of r, which means d is in S. □

b) Prove that $\gcd(a, b) = \gcd(b, r)$.
Hint: if two sets are the same, so are there maximal elements.

Problem 3.
Show that the fraction

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

is irreducible for all positive integers n.

Proof. Suppose it was reducible. Then both the numerator and the denominator share come factor $d > 1$. Since $d \mid 12n + 1$ we also have $d \mid 60n + 5$. But d is also a divisor of $30n + 1$, which makes it a divisor of $60n + 2$. If d is a divisor of $60n + 2$ and $60n + 5$, it also must be a divisor of their difference, 3. But $d > 1$, so it must be 3. On the other hand, $30n + 1$ cannot be divisible by 3 as 30 is, and 1 is not. This is a contradiction, which means the fraction really must be irreducible. □

Problem 4.
Can the GCD of two distinct positive integers be bigger than their difference?

Proof. No. Let d be the GCD of a and b, and suppose $a > b$. Since d is a divisor of a and b, it is also a divisor of $a - b$. Then $a - b = kd$ for some nonzero integer k. it is nonzero since $a - b$ is not zero. But then $k \geq 1$, which means $a - b = kd \geq d$. $\square$