Lesson 7: Remainders, Primes and the Euclidean Algorithm

Konstantin Miagkov

May 5, 2019

Problem 1.
Compute: the remainder of -7 when divided by -2, the remainder of -153 when divided by 15, the remainder of 153 when divided by -15.
Answers: $-1, 12, 3$.

Problem 2.
Show that a prime number greater than 3 can be expressed as $6n+1$ or $6n+5$ for some nonnegative integer n.

Proof. Any positive number m can be represented uniquely as one of $6n$, $6n+1$, $6n+2$, $6n+3$, $6n+4$, $6n+5$ for some nonnegative integer n. If m is prime, it doesn't have any divisors other than 1 and itself. $6n$, $6n+2$ and $6n+4$ have divisor 2. $6n+3$ has divisor 3. So they can't be a prime greater than 3. Therefore a prime number greater than 3 must be able to be represented as either $6n+1$ or $6n+5$for some nonnegative integer n. □

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

b) Show how to construct infinitely many such examples.

Proof. We will do part b) directly: Let us take any three distinct positive integers x, y, z, and set our numbers to be xy, yz and xz. They are all distinct: indeed, if $xy = yz$, then $x = z$, and we took x, y, z to be distinct. Same goes for the other pairs. Once we know that xy, yz and xz are distinct, we jut need to check that the product of any two is divisible by the third. Indeed, $xz \cdot yz = xy \cdot z^2$ and so is divisible by xy, $xz \cdot xy = yz \cdot x^2$ and so is divisible by yz, $yz \cdot xy = xz \cdot y^2$ and so is divisible by xz. A numerical example representing this construction would be for $x = 1$, $y = 2$ and $z = 3$, yielding $2, 3, 6$. □

Problem 4.
a) Let a, b be positive integers such that $a \leq 100$ and $b \leq 100$. Show that computing $\gcd(a, b)$ with the Euclidean algorithm takes at most 20 steps.

b) Show that in fact it takes at most 11 steps.

Proof. Assume $a \geq b$. Let r be the remainder for the first iteration of Euclidean algorithm. If $b \leq a/2$, then we have $r \leq a/2$ because of the definition of division. Otherwise, $b > a/2$, then we will have $a = 1 \cdot b + r$ when dividing a by b since $2b > a$. So

$$r = a - b < a - a/2 = a/2$$

In either case, we have $r \leq a/2 \leq 50$. Let r' be the remainder for the second iteration of Euclidean algorithm, i.e. dividing b by r. By the definition of division, $r' < r \leq a/2 \leq 50$. We can see that every two iterations of Euclidean Algorithm will make the two numbers at least half. After four steps, the two numbers will be less or equal to 25 and so on. After eight steps, both positive numbers are at most 6. We can write out all the cases:
6 and 5:

$$6 = 5 \cdot 1 + 1$$

$$5 = 1 \cdot 5 + 0$$

6 and 4:

$$6 = 4 \cdot 1 + 2$$

$$4 = 2 \cdot 2 + 0$$

5 and 4:

$$5 = 4 \cdot 1 + 1$$

$$4 = 1 \cdot 4 + 0$$

5 and 3:

$$5 = 3 \cdot 1 + 2$$

$$3 = 1 \cdot 2 + 1$$

$$2 = 1 \cdot 2 + 0$$

5 and 2:

$$5 = 2 \cdot 2 + 1$$

$$2 = 1 \cdot 2 + 0$$

two steps 4 and 3:

$$4 = 3 \cdot 1 + 1$$

$$3 = 1 \cdot 3 + 0$$

two steps 3 and 2:

$$3 = 2 \cdot 1 + 1$$

$$2 = 1 \cdot 2 + 0$$

two steps All the other cases will finish in one step since one is a divisor of the other. We can conclude that it takes at most $8 + 3 = 11$ steps. □