Lesson 8: Euclid's lemma

Konstantin Miagkov

December 3, 2017

Problem 1.
Suppose a has quotient q and remainder r when divided by b. What is the quotient and remainder of $3a$ when divided by $3b$?

Problem 2.
a) Use the Euclidean algorithm to find the gcd of the following pairs of numbers: $(52, 47)$, $(124, 1024)$, $(201, 315)$

b) Find at least one pair of integer solutions for each of the following equations

$$52x + 47y = 1$$

$$124x + 1024y = 4$$

$$201x + 315y = 3$$

c) Given two positive integers a, b, describe how to find at least one solution to the equation $ax + by = \gcd(a, b)$.

Problem 3.
In this problem, you can assume the conclusion of problem 2c): For any two positive integers a, b there exists an integer solution x, y to the equation $ax + by = \gcd(a, b)$.
a) Let a be an integer and p be a prime number that does not divide a. What is $\gcd(a, p)$?

b) (*Euclid's lemma*) Suppose a, b are positive integers and p is prime such that $p \mid ab$. Prove that $p \mid a$ or $p \mid b$. (Hint: assume that p does not divide a. Then by part a) you know $\gcd(a, p)$. Use that and 2c)

Problem 4.
Using problem 3b), it is possible to show that any positive integer has a

unique prime factorization: it can be written as a product of primes in a unique way. You can use this fact in this problem.
a) Find the smallest integer greater than 1 that has remainder 1 when divided by $2, 3, 5, 7$.

b) Find all such positive integers.