Homework on Number Theory

Benjamin Cosman, Patrick Lin and Mahesh Viswanathan

Fall 2020

Problem 1. Recall that the proof of the Fundamental Theorem of Arithmetic relied on Euclid's lemma, which required Bézout's lemma to prove. Prove the following converse of Euclid's lemma, which, as it turns out, does not rely on Bézout's lemma.

Suppose a, b_1, b_2 are integers. If $a \nmid b_1 b_2$, then $a \nmid b_1$ and $a \nmid b_2$.

Problem 2. Prove that for all integers a, b and m,
$\gcd(a, b) = \gcd(a + bm, b)$.

Problem 3. In this problem, we will actually prove Bézout's lemma:

Bézout's Lemma. *Let a, b be non-zero integers. Then there exist integers x, y such that $ax + by = \gcd(a, b)$.*

The proof will come from analyzing the following variant of the Euclidean algorithm seen on the Worksheet.

Euclidean algorithm

```
gcd(a,b): // a > b > 0
  x = a
  y = b
  while y > 0:
    r = rem(x,y)
    q = quot(x,y) // This line is new
    x = y
    y = r
  return x
```

Let q_n, x_n, y_n be the respective values of q, x, y after the n-th iteration of the while loop. By definition, we know that for $n > 1$, $y_n = \mathsf{rem}(x_{n-1}, y_{n-1})$, $q_n = \mathsf{quot}(x_{n-1}, y_{n-1})$, so $x_{n-1} = y_{n-1}q_n + y_n$.

a) Prove (by induction) that for all $n \geq 1$, after the n-th iteration of the while loop, there exist integers s_n, t_n so that $y_n = as_n + bt_n$.[1]

b) Explain how the previous part implies Bézout's lemma.

[1] Hint: Rewrite the equation $x_{n-1} = y_{n-1}q_k + y_n$ to be solely in terms of y's.

Problem 4. Prove that congruence modulo n is an equivalence relation over $\mathbb{Z}$.