February 22th, 2016

Math 351

Luís Finotti
Spring 2016

Name: ....

Student ID (last 6 digits): XXX-................

Midterm 1

You have 50 minutes to complete the exam. Do all work on this exam, i.e., on the page of the respective assignment. Indicate clearly, when you continue your solution on the back of the page or another part of the exam.

Write your name and the last six digits of your student ID number on the top of this page. Check that no pages of your exam are missing. This exam has 6 questions and 8 printed pages (including this one and a page for scratch work in the end).

No books or notes are allowed on this exam!

Show all work! (Unless I say otherwise.) Correct answers without work will receive **zero**. Also, **points will be taken from messy solutions**.

Good luck!

Question	Max. Points	Score
1	20	
2	10	
3	10	
4	20	
5	20	
6	20	
Total	100	

1) [20 points] Use the *Extended Euclidean Algorithm* to write the GCD of 210 and 77 as a linear combination of themselves. *Show the computations explicitly!* [**Hint:** You should get 7 for the GCD!]

2) [10 points] Let

$$m = 2^a \cdot 3^5 \cdot 5^b \cdot 7,$$
$$n = 3^c \cdot 5 \cdot 7^d,$$

where $a, b, c, d \in \mathbb{Z}_{\geq 0}$. If $(m, n) = 3^2 \cdot 7$ and $[m, n] = 2 \cdot 3^5 \cdot 5 \cdot 7^3$, then find a, b, c and d. [Justify!]

3) [10 points] Express 327 in base 5. *Show the computations explicitly!*

4) [20 points] If

$$n \overset{\text{def}}{=} 3601292 \cdot (126517)^{5784683745} - 72342003,$$

then what is its remainder when divided by 3? [Justify! Correct answer with no explanation is worth 0.]

5) [20 points] Let

$$n \overset{\text{def}}{=} 13004385024102127.$$

Find the remainders of n when divided by 2, 4, 5, 9 and 10,000. [Justify! Correct answer with no explanation is worth 0.]

6) [20 points] For both parts below, let $a \in \mathbb{Z}$ and $m \in \mathbb{Z}_{\geq 2}$ with $(a, m) = 1$.

(a) Prove that there is $r \in \mathbb{Z}$ such that $a \cdot r \equiv 1 \pmod{m}$. [**Hint:** You *have* to use the fact that $(a, m) = 1$, but probably not the definition of GCD itself.]

(b) Given $b \in \mathbb{Z}$, prove that there is $x \in \mathbb{Z}$ such that $a \cdot x \equiv b \pmod{m}$. [You can use the previous part here, even if you could not do it!]

Scratch: