Elementary Number Theory: Practice Final Exam

Summer 2016

July 31, 2016

Name: ____ Student ID: _______________

Instructions

- This exam consists of 6 problems on 9 pages. The final two pages are for scratch work. If you need extra paper, it will be provided.
- Show all necessary steps. A solution without sufficient justification will not receive full credit.
- You may use Theorems from the lecture, unless stated otherwise. Please state clearly and explicitly any such results.
- Please write the solution in the space provided going to the back side if necessary.
- Write **clearly and legibly**. Points will be deducted if the solution or the logical sequence is not understood.
- A scientific calculator is allow as long as it can not be programmed.

Problem:	1	2	3	4	5	6	Total
Score:							

1. Show that 1105 is a Carmichael number.

2. Find all solutions $(x, y) \in \mathbb{Q}^2$ to each of the following or prove that none exist.
   (a) $x^2 + y^2 = 2$
   (b) $x^2 + y^2 = 3$

3. Let p be prime. In this problem do not use that $\mathbb{F}_p = \mathbb{Z}/p\mathbb{Z}$ is a field. (You will essentially prove this result here.)

   (a) For each $a \in \mathbb{Z}$ let $\overline{a}$ denote the equivalence class of a in $\mathbb{Z}/p\mathbb{Z}$. What exactly is $\overline{a}$? (You may find it helpful to recall the definition of $\mathbb{Z}/p\mathbb{Z}$.)

   (b) Let $a, b \in \mathbb{Z}$. We define $\overline{a} \cdot \overline{b} = \overline{ab}$. Prove that this notion is well-defined.

   (c) Let $a \in \mathbb{Z}$ such that $p \nmid a$. Prove that there exists $b \in \mathbb{Z}$ such that $ab \equiv 1 \pmod{p}$.

4. In this problem you may use the fact that $p = 53 = 2^2 \cdot 13 + 1$ is prime.
   (a) Show that $(\frac{7}{p}) = 1$.
   (b) Show that 3 is not a square modulo p.
   (c) Describe Tonelli's algorithm and use it to find all solutions to $x^2 \equiv 7 \pmod{p}$.

5. Suppose that $x \in \mathbb{R} \setminus \mathbb{Q}$. Let α_n be as in the continued fraction expansion algorithm, meaning that if $a_n = \lfloor \alpha_n \rfloor$ then $[a_0, a_1, a_2, \ldots]$ is the continued fraction expansion of x.

   (a) Suppose that $\alpha_j = \alpha_\ell$ for some $j > \ell$. Prove that this implies that the continued fraction expansion of x is periodic.

   (b) Find the continued fraction expansion of $\sqrt{7}$.

6. Show that $y^2 = x^3 + 1$ defines an elliptic curve E over the field $\mathbb{Q}$ of rational numbers. Recall that if E is given by $y^2 = x^3 + ax^2 + bx + c$ then $\Delta(E) = -4a^3c + a^2b^2 + 18abc - 4b^3 - 27c^2$ is the discriminant of E.

   (a) Does the given equation define an elliptic curve over the finite field $\mathbb{F}_p$ of p elements, for each $p \in \{2, 3, 5\}$? If so, determine the set $E(\mathbb{F}_p)$.

   (b) Find $E(\mathbb{Q})_{\text{tor}}$.