MA4220: Number Theory (Spring 2011)
Final Exam

NAME:

Instructions

The Final Exam is worth 15% of your overall grade. For each part of the exam, read the instructions carefully.

I expect your proofs to be *well-written, neat, and organized.* You should write in *complete sentences.* Do not turn in rough drafts. What you turn in should be the "polished" version of potentially several drafts. Feel free to type up your final version.

The LaTeX source file of this exam is also available if you are interested in typing up your solutions using LaTeX. I'll help you do this if you'd like.

The simple rules for the exam are:

1. You may freely use any theorems that we have discussed in class, but you should make it clear where you are using a previous result and which result you are using. For example, if a sentence in your proof follows from Theorem 1.41, then you should say so.
2. Unless you prove them, you cannot use any results from the textbook that we have not covered.
3. You are NOT allowed to consult external sources when working on the exam. This includes people outside of the class, other textbooks, and online resources.
4. You are NOT allowed to copy someone else's work.
5. You are NOT allowed to let someone else copy your work.
6. You are allowed to discuss the problems with each other and critique each other's work.

The Final Exam is due to my office by 5PM on **Friday, May 20**. You should turn in this cover page and all of the work that you have decided to submit.

To convince me that you have read and understand the instructions, sign in the box below.

Signature:

Good luck and have fun!

Written by D.C. Ernst

Part 1

Suppose that $pq = 11537$ and $E = 85$ and consider the following message that has been encrypted using pq and E:

8664, 1840,2615, 178, 1, 5483, 10096, 2373, 2615, 11393, 178, 8199, 10096, 178, 1793, 10098, 11393, 8664, 8321, 8664, 2373, 10098

Assume that the block length is 2 and that the dictionary from the RSA handout was used to encrypt. Use whatever means necessary to decipher the message. You may rely on technology such as `Sage` or `WolframAlpha`. However, you should explain what steps you took to solve the problem and how you utilized the technology.

Part 2

Complete any **four** of the following theorems.

Theorem 1 (Chinese Remainder Theorem)**.** Suppose $n_1, n_2, \ldots, n_L$ are positive integers that are pairwise relatively prime, that is, $(n_i, n_j) = 1$ for $i \neq j$, $1 \leq i, j, \leq L$. Then the system of L congruences

$$\begin{aligned} x &\equiv a_1 \pmod{n_1} \\ x &\equiv a_2 \pmod{n_2} \\ &\vdots \\ x &\equiv a_L \pmod{n_L} \end{aligned}$$

has a unique solution modulo the product $n_1 n_2 \cdots n_L$.[*]

Theorem 2 (Euler's Theorem)**.** If a and n are integers with $n > 0$ and $(a, n) = 1$, then

$$a^{\phi(n)} \equiv 1 \pmod{n}.$$[†]

Theorem 3. Let n and m be natural numbers that are relatively prime, and let a be an integer. If $x \equiv a \pmod{n}$ and $x \equiv a \pmod{m}$, then $x \equiv a \pmod{nm}$.[‡]

Theorem 4. Suppose that p is a prime number and a is an integer such that $(a, p) = 1$. Then for all $k \in \mathbb{N}$, we have

$$\operatorname{ord}_p(a^k) = \frac{\operatorname{ord}_p(a)}{(k, \operatorname{ord}_p(a))}.$$

Theorem 5. Suppose that n is a natural number and a is an integer such that $(a, n) = 1$ and $a^{n-1} \equiv 1 \pmod{n}$. Then $\operatorname{ord}_n(a) < n - 1$ iff there exists a prime p such that $p \mid n - 1$ and

$$a^{\frac{n-1}{p}} \equiv 1 \pmod{n}.$$

Theorem 6. Suppose that n is a natural number and a is an integer such that $(a, n) = 1$ and $a^{n-1} \equiv 1 \pmod{n}$. If $\operatorname{ord}_n(a) = n - 1$, then n is prime.

[*] This is Theorem 3.29 in our textbook. We discussed a potential proof for this one day in class, but no one presented a satisfactory proof. So, now is your chance. You can only use theorems that come before this theorem in the book to prove it.

[†] This is Theorem 4.32 in our textbook. As with the Chinese Remainder Theorem, no one presented a satisfactory proof. You can only use theorems that come before this theorem in the book to prove it.

[‡] This is Theorem 4.21 in the textbook. We've used this theorem a few times, but I'm pretty sure that we never proved it.