MA4220: Number Theory (Spring 2011)
Exam 2

NAME:

Instructions

This exam is worth 15% of your overall grade and all of the problems have equal weight. 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 exam is due at the beginning of class on **Tuesday, April 26**. 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!

Part 1

Answer each of the following questions. You need to justify your answers with sufficient work and should not rely on technology such as a graphing calculator or `WolframAlpha`.

1. Find all integers x such that $1 \leq x \leq 65$ and $4x + 1 \equiv 1 \pmod{65}$.
2. Find all integers x such that $1 \leq x \leq 98$ and $8x + 5 \equiv 7 \pmod{98}$.
3. Find all integers x such that $1 \leq x \leq 65 \cdot 98$ and simultaneously satisfies $4x + 1 \equiv 1 \pmod{65}$ and $8x + 5 \equiv 7 \pmod{98}$.

Part 2

Complete any 2 of the following problems.

4. Prove that there is only one integer x such that $1 \leq x \leq 2011$ and satisfies $x^{13} \equiv 1 \pmod{2011}$.*
5. Let p and q be distinct primes such that $p - 1 | q - 1$. Prove that if $(a, pq) = 1$, then $a^{q-1} \equiv 1 \pmod{pq}$
6. Prove that there are infinitely many primes that are congruent to 5 modulo 6. You may not use Dirichlet's Theorem (i.e., the theorem following 2.39 in our textbook). You may freely use each of the following facts:
   (a) There are no primes congruent to 4 modulo 6 or 0 modulo 6.
   (b) If $r_1, \ldots, r_m$ are congruent to 1 modulo 6, then the product $r_1 \cdots r_m$ is congruent to 1 modulo 6.
7. A *Carmichael number* is defined to be a composite number n such that $a^{n-1} \equiv 1 \pmod{n}$ for every integer a with $(a, n) = 1$. Prove that 561 is Carmichael number.†

Part 3

Here are the instructions for this portion of the exam.

- Prove both of the following theorems.
- You are required to type your proofs and submit them to me via email at `dcernst@plymouth.edu`.
- Please put each proof on its own page. If you choose to type your entire exam, I would like these problems to be in a separate file.
- Send me a PDF file and name your file according to: `Exam2Part3Last-Name.pdf`.
- Do *not* include your name anywhere on the typeset document.

Like the first exam, these proofs will be sent to students at Wellesley College to be peer reviewed. You will receive a critical review of each proof from a student at Wellesley, but their critique will *not* impact your grade. Similarly, we will be reviewing proofs submitted by students from Wellesley in the near future.

Theorem 1. Let p be prime and let a be an integer such that $1 \leq a < p$. Then there exists a unique natural number b less than p such that $ab \equiv 1 \pmod{p}$.‡

Theorem 2. If p and q are distinct primes and a is a natural number such that $(a, pq) = 1$, then $a^{(p-1)(q-1)} \equiv 1 \pmod{pq}$.§

*You may use the fact that 2011 is prime.
†561 is the smallest Carmichael number. It is not known whether there are infinitely many Carmichael numbers.
‡This is Theorem 4.36 in our textbook. This theorem is making claims about multiplicative inverses.
§Make sure you only use results that we've actually proved. If there is a result that you want to use, then prove it.

