MAT 311 Introduction to Number Theory

Problem Set 5

due Wednesday, March 4

Please prove all your answers.

Problem 1. Prove that for each natural n there are n consequtive integers each divisible by a square greater than 1. **Hint:** use the Chinese Remainder Theorem.

Problem 2. We used group theory to give another proof of Fermat's Little Theorem ($a^{p-1} \equiv 1 \mod p$ if p does not divide a) in class on Wednesday. Mimic this proof to get Euler's theorem: $a^{\phi(m)} \equiv \mod m$ if $(a, m) = 1$. Follow these steps:

(a) Consider all classes $\mod m$ that are relatively prime to m (in other words, classes corresponding to a reduced residue system). Define multiplication of two classes of a resp. b as the class of ab:

$$[a] \cdot [b] = [ab].$$

Check that this multiplication operation is well-defined, i.e. that $[ab]$ is independent of the choice of the two elements in classes $[a]$ and $[b]$, and that $[ab]$ is relatively prime to m if both $[a]$ and $[b]$ are.

(b) Show that the set of classes from (a) forms a group under multiplication. What is the order of this group?

(c) As we proved in class, the order of an arbitrary element in a finite group divides the order of the group (the Lagrange theorem). Use this to prove Euler's theorem.

If all else fails, you can find this proof in the book – but if you have to do so, please write the solution in your own words.

Problem 3. (a) Show that the set of all classes $\mod p$ (including $[0]$) does **not** form a group under multiplication.

(b) Show that if the set of all non-zero classes $\mod p$ forms a group under multiplication, then p must be prime. (That is, $(\mathbb{Z}/m\mathbb{Z})^*$ won't be a group for m composite.)

Problem 4. (a) Prove that $n^4 - n^2 + 1$ is composite for natural $n > 1$. **Hint:** $a^2 - a + 1 = (a-1)^2 - a$.

(b) Find prime decomposition of $2^{36} - 1$. Don't use a calculator and don't compute the decimal representation of $2^{36} - 1$; use algebra instead – part (a) should be useful, among other things.

Problem 5. This question exploits Pigeonhole principle: if there are k boxes and $k + 1$ objects, then there should be at least two objects in one of the boxes. (Proof: suppose not, then each box contains no more than one object, so the total number of objects is no more than k, a contradiction.)

(a) Show that there exist two distinct natural numbers m, n such that $2009|(2^m - 2^n)$. Can you give an easy proof with Pigeonhole Principle? Can you use one of the theorems that we learned?

(b) Show that there are two distinct natural numbers whose decimal notation contains only 1's and whose difference is divisible by 2009:

$$2009|(\underbrace{1111...111}_{n} - \underbrace{11...111}_{m})$$

(c) Show that there is a number 111...11 divisible by 2009. **Hint:** this follows from (b) and some number theory.