Math 55 First Midterm
February 21, 2013
Sketchy solutions provided by Ken Ribet

Please put away all books, calculators, cell phones and other devices. You may consult a single two-sided sheet of notes. Please write clearly and carefully in *complete sentences.* Explain what you are doing since the paper you hand in will be your only representative when your work is graded.

Problem	1	2	3	4	5	6	*Total*
Max. points	6	3	7	3	4	7	30

1. *For each of these sets of premises, what relevant conclusions (if any) can be drawn:*

a. *"All insects have six legs." "Dragonflies are insects." "Spiders eat dragonflies."*

This problem was taken from the textbook. The obvious conclusion is that spiders eat some creatures with six legs.

b. *"I am either dreaming or hallucinating." "I am not dreaming." "If I am hallucinating, I see elephants running down the road."*

Since I am not dreaming, I am hallucinating. Therefore, I see elephants running down the road.

2. *If r, s and t are real numbers, prove that the products rs, rt and st are not all negative.*

Assume that rs and rt are both negative; we will prove that st is positive and therefore is not negative. The assumption implies that r, s and t are all non-zero. If r is positive, then s and t are both negative, so that st is positive. If r is negative, then s and t are both positive, so that rs is positive. In both situations, rs is positive; that's what we set out to prove.

3. *Consider the set of all sequences $\{a_n\}$ whose terms a_n are binary digits. (In other words, each a_n is 0 or 1.) Show that this set is uncountable.*

The set in question is clearly infinite. Call it S. We claim that it is not countably infinite and therefore that it is uncountable. To see this, we argue by contradiction, supposing that S is countably infinite. Then there is a first sequence $\{a_n^1\}$, a second sequence $\{a_n^2\}$, a third sequence $\{a_n^3\}$, and so on, in such a way that each element of S is one of the numbered sequences. Consider the sequence $\{b_n\}$, where b_n is defined to be $1 - a_n^n$ for $n \geq 1$. In other words, b_n is 0 if a_n^n is 1, and b_n is 1 if a_n^n is 0. It is clear that $\{b_n\}$ cannot be any of the numbered sequences $\{a_n^i\}$. Indeed, if $\{b_n\}$ were $\{a_n^i\}$, we'd have $b_i = a_i^i$ in particular. However, we have defined the bs so that $b_i \neq a_i^i$. The fact that $\{b_n\}$ is not an $\{a_n^i\}$ shows that there are elements of S that have not been numbered. This statement is in contradiction with our previous statement that every element of S is one of the numbered sequences. Since we have reached a contradiction, we must discard our initial assumption that the set is countably infinite.

4. *Suppose that p is a prime number and that x and y are integers. Show that if xy and $x+y$ are both divisible by p, then each of x and y is divisible by p.*

This problem was discussed in the book when $p = 2$; a number is divisible by 2 if and only if it is even. The proof given in the book works in our case as well. Namely, assume that xy and $x + y$ are divisible by p. Because p divides xy, p divides either x or y; this is a key property of prime numbers. If p divides x, then it divides y as well because it divides $x + y$. Similarly, p divides x if it divides y.

5. *Find the smallest positive multiple of 100 that leaves remainder 9 when divided by 19.*

We want the smallest positive x so that $100x \equiv 9 \pmod{19}$. Modulo 19, 100 is the same thing as 5 (because $100 - 5 = 19 \cdot 5$). The inverse of 5 mod 19 is 4 (since $4 \times 5 = 20$), so $x \equiv 4 \cdot 9 \equiv 17 \pmod{19}$. Hence the answer appears to be 1700. Sage agrees that $1700 \equiv 9 \pmod{19}$.

6. *Let $\{a_n\}$ be the sequence defined by the initial condition $a_0 = 3$ and the recurrence relation $a_n = a_0 a_1 \cdots a_{n-1} + 2$. The sequence begins 3, 5, 17,* *257, 65537, and we'll stipulate that all of the subsequent numbers are odd. (We can establish this parity statement by mathematical induction, but not until next week.)*

a. *For $n \geq 1$, show that the two numbers a_n and $a_0 a_1 \cdots a_{n-1}$ are relatively prime.*

Every divisor of these two numbers divides their difference, which is 2. Hence the only possible positive divisors of the two numbers are 1 and 2. But the numbers are odd, so 2 divides neither of them. Hence 1 is the only common divisor of the two and is therefore their gcd.

b. *For each i, let p_i be a prime number dividing a_i. Explain why the primes $p_1, p_2, p_3, \ldots$ are all different from each other.*

Suppose that $p_i = p_n$ with $i \neq n$. Without loss of generality, we can suppose that n is larger than i. The prime number p_i divides $a_0 \cdots a_{n-1}$ because a_i is one of the factors in this product. It divides a_n as well because $p_i = p_n$ divides a_n. Therefore, $a_0 \cdots a_{n-1}$ and a_n have a non-trivial common divisor, which is contrary to the conclusion of part (a).

Note: because the primes p_i are all different from each other, we see that there are infinitely many primes. In other words, we have proved Euclid's result about the infinitude of primes without using Euclid's argument.

The numbers a_n are called the *Fermat numbers*. You can stalk them easily on wikipedia or elsewhere. The first few are prime, and the next bunch (a large bunch) are known to be composite. No one knows if infinitely many of them are prime or if infinitely many of them are composite.