Math 55

PROFESSOR KENNETH A. RIBET

First Midterm Examination
February 19, 2015
2:10–3:30 PM, 100 Lewis Hall

All five questions were worth six points. The maximum possible score was 30 points.

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

Each page had this honor code at the bottom:

> *As a member of the UC Berkeley community, I act with honesty, integrity, and respect for others.*

I must say that this seems to be the easiest exam that I've given in a very long time. People walked out early! I'm known for giving insanely hard exams; I told one student at the exit that this exam was only "sanely hard." I really hope that you guys did OK!!

1. Use existential and universal quantifiers to express the statement "Everyone has exactly two biological parents" using the propositional function $P(x, y)$, which represents "x is the biological parent of y."

This is problem 25 on page 113 of the book. There is a one-line answer on page S-12 (in the back of the book):

$$\forall x \exists y \exists z (y \neq z \wedge \forall w (P(w, x) \leftrightarrow (w = y \vee w = z))).$$

(I hope that I didn't introduce any typos in copying what is in the book.)

2. Decide whether or not the compound proposition

$$(\neg q \vee (p \to q)) \to \neg p$$

is a tautology.

A tautology is a proposition that is true (T) for all possible truth values of the simple propositions that make it up. If p and q are both true, then $p \to q$ is true, so $(\neg q \vee (p \to q))$ is true. The implication is then false because the "hypothesis" $(\neg q \vee (p \to q))$ is true but the "conclusion" $\neg p$ is false. Hence the compound proposition is not a tautology.

3. Let $\{a_n\}$ be the sequence of positive odd numbers defined by: $a_0 = 3$ and $a_n = a_0 a_1 \cdots a_{n-1} + 2$ for $n \geq 1$. The sequence begins 3, 5, 17, 257, 65537,.... If n and m are natural numbers with $m < n$, show that 1 is the only positive integer that divides both a_m and a_n.

This problem was basically on my midterm two years ago. The equation $a_n = a_0 a_1 \cdots a_{n-1} + 2$ may be rewritten $2 = a_n - a_0 a_1 \cdots a_{n-1}$. If d divides a_m, it divides $a_0 a_1 \cdots a_{n-1}$. If it divides both a_n and a_m, it therefore divides $a_n - a_0 a_1 \cdots a_{n-1} = 2$. The only divisors of 2 are 1 and 2. The numbers involved are given to be odd, so 2 can be eliminated as a divisor. That leaves us with 1 as the only possible divisor.

4. Suppose that $f : A \to \mathcal{P}(A)$ is a function from a set to its power set. Let

$$B = \{\, b \in A \,|\, b \notin f(b) \,\},$$

and let c be an element of A. Show that $f(c) \neq B$ by deriving a contradiction from the assumption $f(c) = B$.

This was surely the hardest and most confusing question on the exam. It is based on one of the last lectures that I gave in 10 Evans. You all follow my lectures, right?

The first thing to understand is that f takes each element of A to an element of $\mathcal{P}(A)$, which is the set whose elements are the subsets of A. Thus $f(a)$ is a subset of A when a is an element of A. You can ask whether or not the element a of A happens to lie in the subset $f(A)$; maybe it does and maybe it doesn't. The set B consists of those a in A for which the question has a negative answer. In other words, if $a \in B$, then $a \notin f(a)$. If a is not an element of B, then $a \in f(a)$.

We are asked to show that if c is an element of A, then $f(c)$ is not B. A proof by contradiction is suggested. So suppose that $f(c) = B$; can we get a contradiction?

Since $f(c) = B$, $c \in f(c)$ if and only if $c \in B$.

But remember that, for all a in A, $a \in B \Leftrightarrow a \notin f(a)$. We can take $a = c$; then $c \in B \Leftrightarrow c \notin f(c)$. Since $B = f(c)$, we have the ridiculous equivalence

$$c \in B \Leftrightarrow c \notin B.$$

This is really a contradiction because c either is in B or isn't in B.

5. Using the identity $1 = 54 \cdot 129 - 35 \cdot 199$, write down an integer that is congruent to 35 (mod 129) and to 54 (mod 199). You can leave your answer as an arithmetic expression (i.e., one involving products, sums, differences) — don't worry about simplifying!

One way to do this problem is to write $x = 35 + 129t$ and try to find t. The first congruence is assured, and t needs to be determined so that $x \equiv 54 \bmod 199$. This means $35 + 129t \equiv 54 \bmod 199$, or $129t \equiv 19 \bmod 199$. Now the inverse of 129 mod 199 can be read off from the given identity: it's 54. Hence $t \equiv 19 \cdot 54 \bmod 199$, i.e., $t \equiv 31 \bmod 199$. Hence we might as well take $x = 35 + 129 \cdot 31$; x really is a number mod $129 \cdot 199 = 25671$. Our answer is $x \equiv 35 + 129 \cdot 31 = 4034 \bmod 25671$. This is actually correct according to `sage`.

The way that I was recommending in class was to take

$$x = (54 \cdot 129) \cdot 54 + (-35 \cdot 199)35 = 132389.$$

Note that $619939 \equiv 4034 \bmod 25671$. The answer is the same.

You get full credit if you write the answer as $x = (54 \cdot 129) \cdot 54 + (-35 \cdot 199)35 = 132389$, at least if you provide some explanation (as you were asked to do). It is not necessary to calculate the numerical answer.