Math. 55 EXAM. Model Solutions

This 35 minute exam, to be administered in your discussion section, can be answered with the aid of any texts, notes and calculating instruments. Answers may be worked out on scratch paper but must be entered on this sheet in the spaces provided. Each correct answer earns one point; each incorrect answer loses one point; space left blank loses nothing, so **DON'T JUST GUESS.** And check your work. Finally hand this sheet and *all* your used scratch paper to the Teaching Assistant, who will return the scored sheet some time later. Your score *will* affect your final grade. You must not discuss this exam's questions with anyone else until tomorrow.

1. "John hunts no birds or snakes." _ $(\neg b) \vee s$, or $b \to s$ _.

"John hunts no birds nor snakes." _ $\neg(b \vee s)$, or $(\neg b) \wedge (\neg s)$ _.

Assuming that these sentences have different meanings, explain them by filling in the blanks that follow them with expressions using logical operators like $\neg, \wedge, \vee, \ldots$ and the two propositions

b := "John hunts birds." s := "John hunts snakes."

2. Wilson's Theorem says " If n is a prime then $(n-1)! \equiv -1$ **mod** n ." State this theorem's converse: _ If $(n-1)! \equiv -1$ **mod** n then n is a prime. _

Is the converse of Wilson's Theorem true? (YES or NO) _ YES _. (*Except* if $n \leq 1$.)
(If $n > 1$ is not prime, GCD(n, (n–1)**!**) is a product of prime factors of n , not 1 .)

3. Find the smallest (in magnitude) difference between different solutions x of all three congruences { $3x \equiv 2$ **mod** 5 , $x \equiv 2$ **mod** 6 , and $2x \equiv 3$ **mod** 7 } : _ 210 , $= 5 \cdot 6 \cdot 7$ _.

4. The following algorithm is proposed to find factors of any given huge odd integer n :
For $k = \lceil \sqrt{n} \rceil$, $\lceil \sqrt{n} \rceil + 1$, $\lceil \sqrt{n} \rceil + 2$, … in turn test whether $m := \sqrt{(k^2 - n)}$ is an integer, in which case stop and exhibit $n = (k-m) \cdot (k+m)$.
Must this algorithm stop? (YES or NO) _ YES _.
(This is Fermat's algorithm; it has to stop for $k \leq (n+1)/2$.)

5. If a finite string of bits is the one's complement representation of integer x and also the two's complement representation of integer $y \neq x$, what is $x - y$? _ +1 _.
(If x and y were positive they'd be equal; instead n-bit unsigned $2^n - 1 + x = 2^n + y$.)

6. Among all pairs (x, y) of integers that satisfy $93x + 20y = 1$
find the minimum of $|x - y|$: _ 17 _.
(x = -3 and y = 14 .)

7. Solve $\begin{bmatrix} 3 & 7 \\ 2 & 5 \end{bmatrix} \begin{bmatrix} x \\ y \end{bmatrix} \equiv \begin{bmatrix} 2 \\ 4 \end{bmatrix}$ **mod** 11 for x **mod** 11 = _ 4 _. (And y **mod** 11 = 8 .)

The maximum score on this test is 9 points.

Prof. W. Kahan Wed. 3 March. 1999

This document was created with FrameMaker 4.0.4

Math. 55 EXAM. Model Solutions

This 35 minute exam, to be administered in your discussion section, can be answered with the aid of any texts, notes and calculating instruments. Answers may be worked out on scratch paper but must be entered on this sheet in the spaces provided. Each correct answer earns one point; each incorrect answer loses one point; space left blank loses nothing, so **DON'T JUST GUESS.** And check your work. Finally hand this sheet and *all* your used scratch paper to the Teaching Assistant, who will give back the scored sheet some time later. Your score *will* affect your final grade. You must not discuss this exam's questions with anyone else until tomorrow.

1. Wilson's Theorem says " If n is a prime then $(n-1)! \equiv -1$ **mod** n ." State this theorem's converse: _ If $(n-1)! \equiv -1$ **mod** n then n is a prime. _

Is the converse of Wilson's Theorem true? (YES or NO) _ YES _. (*Except* if $n \le 1$.)
(If $n > 1$ is not prime, GCD(n, (n–1)!) is a product of prime factors of n , not 1 .)

2. "John hunts no birds nor snakes." _ $\neg(b \vee s)$, or $(\neg b) \wedge (\neg s)$ _.

"John hunts no birds or snakes." _ $(\neg b) \vee s$, or $b \to s$ _.
Assuming that these sentences have different meanings, explain them by filling in the blanks that follow them with expressions using logical operators like $\neg, \wedge, \vee, \ldots$ and the two propositions

b := "John hunts birds." s := "John hunts snakes."

3. If a finite string of bits is the one's complement representation of integer x and also the two's complement representation of integer $y \neq x$, what is $y - x$? _ –1 _.
(If x and y were positive they'd be equal; instead n-bit unsigned $2^n - 1 + x = 2^n + y$.)

4. Among all pairs (x, y) of integers that satisfy $93x + 20y = 1$
find the minimum of $|x + y|$: _ 11 _.
(x = -3 and y = 14 .)

5. Find the smallest (in magnitude) difference between different solutions x of all three congruences { $4x \equiv 3$ **mod** 5 , $x \equiv 1$ **mod** 6 , and $3x \equiv 5$ **mod** 7 } : _ 210 , $= 5 \cdot 6 \cdot 7$ _.

6. The following algorithm is proposed to find factors of any given huge odd integer n :
For $k = \lceil \sqrt{n} \rceil$, $\lceil \sqrt{n} \rceil + 1$, $\lceil \sqrt{n} \rceil + 2$, … in turn test whether $m := \sqrt{(k^2 - n)}$ is an integer, in which case stop and exhibit $n = (k-m) \cdot (k+m)$.
May this algorithm fail to stop? (YES or NO) _ NO _.
(This is Fermat's algorithm; it has to stop for $k \le (n+1)/2$.)

7. Solve $\begin{bmatrix} 3 & 7 \\ 2 & 5 \end{bmatrix} \begin{bmatrix} x \\ y \end{bmatrix} \equiv \begin{bmatrix} 2 \\ 4 \end{bmatrix}$ **mod** 11 for y **mod** 11 = _ 8 _. (And x **mod** 11 = 4 .)

The maximum score on this test is 9 points.

Math. 55 EXAM. Model Solutions

Oops! I blundered in the problem about Wilson's Theorem and its converse by taking for granted that the *Universe of Discourse* was obviously integers $n > 1$. This should have been stated explicitly; the problem should have been worded " For integers $n > 1$ Wilson's Theorem says … ." In that Universe of Discourse, the converse of Wilson's Theorem is true. In a larger Universe of Discourse the situation is different; $(1–1)! = 1 \equiv –1$ **mod** 1 but 1 is not a prime.

Worse, $(n – 1)!$ can be defined for non-integers; it is called the "Gamma" function $\Gamma(n)$ then. Also " $x \equiv y$ **mod** n " can be defined for non-integers n to mean that $(x–y)/n$ is an integer. Whether $\Gamma(n) \equiv –1$ **mod** n for some non-integer n is a question too interesting to be put on a mid-term test whose questions must be answered in a few minutes each on average. (In fact it happens for non-integers like $n = 4.154439…$ and $4.56215…$ and lots more.) This question must have handicapped students who had enough imagination to contemplate non-integers n . Therefore *all* students' answers to this question will be disregarded during grading.

In short, an integer $n > 1$ is a prime if and only if $(n–1)! \equiv –1$ **mod** n .

I apologize for the blunder.

W. Kahan

. . . . . .

Nobody doubts that "John hunts no birds *nor* snakes" means $\neg(b \vee s)$ and $(\neg b)\wedge(\neg s)$. Many students (and others) have disputed that, if "John hunts no birds *or* snakes" means something different, it must mean $(\neg b) \vee s$ or equivalently $b \rightarrow s$. These latter meanings look strange to most Americans, who usually mean the first quoted sentence when they utter the second. However, sentences like the second have been uttered with an intentional " or " in a place where " nor " would convey an unintended meaning. Here is an example drawn from the DURABLE POWER OF ATTORNEY FOR HEALTH CARE DECISIONS (*California Probate Code Sections 4600-4753*) © California Medical Association 1996 (revised):

> " …, this document gives your agent power to consent to your doctor
> not giving treatment or stopping treatment necessary to keep you alive."

Here replacing " or " by " nor " would be a mistake. The last line would be clearer were it restated

> " … refraining from or stopping treatment necessary to keep you alive."

In English generally the scopes of negating words " no " and " not " can be ambiguous when they precede " or " or " and ". The words " nor " and " but " can help to reduce ambiguity. Although $s \vee (\neg b)$ is logically equivalent to $(\neg b) \vee s$, still " S or not B " is linguistically different from " not B or S " in so far as the latter is ambiguous; it may (or may not) have been intended to mean the same as " not B nor S " which means $\neg(b \vee s)$. Similarly ambiguous is "John hunts no birds and snakes"; it could mean the same as "John hunts snakes but no birds" just as $(\neg b)\wedge s$ is logically equivalent to $s\wedge(\neg b)$, or it could mean the same as "John hunts no birds nor snakes" ($(\neg b)\wedge(\neg s)$) . (But "but not" is usually preferable to "and not".)

A writer sensitive to their potential ambiguities avoids unnecessary negations. So should you.

One measure of our own perfection is the extent to which we tolerate others' imperfections without imitating them.