Midterm Exam

Math 258
(Fall 2005)

Solve the following problems. Show all your work in the space under each problem.

1. Construct a truth table for each of the compound propositions $\neg(p \oplus q)$ and $p \leftrightarrow q$ and determine whether they are equivalent. (2 pts)

P	q	P⊕q	-(P⊕q)	P↔q
T	T	F	T	T
T	F	T	F	F
F	T	T	F	F
F	F	F	T	T

Since the columns of the propositions -(P⊕q) and P↔q contain the same truth values, they are equivalent.

2. Determine the truth value of the following statements, if the universe of discourse consists of all real numbers. Explain. (2 pts)

(a) $\forall x \exists y(xy = 0)$

True, take $y = 0$

(b) $\exists x \forall y(y \neq 0 \rightarrow xy = 1)$

False, each y has its own inverse. It's not necessary that one x will work for every y.

(c) $\forall x \exists y(x + y = 1)$

True, take $y = 1 - x$

(d) $\exists x \exists y(x + y \neq y + x)$

False, commutativity is true $\forall x, y$ in the reals.

3. Prove or disprove that product of a non-zero rational number and an irrational number is irrational. (*Hint*: Use the fact that the product of two rational numbers is rational) (2 pts)

Let $r = \frac{a}{b}$, be a non-zero rational (ie $a \neq 0$)
Let i be an irrational.
Their product $ri = \frac{a}{b} i = \frac{ai}{b}$.
Assume that ri is rat., ie $ri = \frac{c}{d}$, $c, d \in \mathbb{Z}$, $d \neq 0$
Then, $ri = \frac{c}{d} \Rightarrow \frac{ai}{b} = \frac{c}{d} \Rightarrow i = \frac{cb}{da}$, which is a rat. as the product of c, d and d, a is a rat.
But this says that i is rat., which is a contradiction (as i is irrat.).

4. (a) Find two sets A and B such that $A \in B$ and $A \subset B$. (2 pts)

$A = \emptyset$, $B = \{\emptyset\}$

(b) Find the power set of the set $\{\emptyset, \{\emptyset, \{\emptyset\}\}\}$.

$P = \{\emptyset, \{\emptyset\}, \{\{\emptyset, \{\emptyset\}\}\}, \{\emptyset, \{\emptyset, \{\emptyset\}\}\}\}$

5. The **symmetric difference** of two sets A and B, denoted by $A \oplus B$, is the set containing those elements that belong to either A or B, but not in both. Prove or disprove: If $A \oplus C = B \oplus C$, then $A = B$. (2 pts)

Assume $A \neq B$, ie $\exists\, x \in A$ st $x \notin B$ or $\exists x \in B$ st $x \notin A$.

Supp: $x \in A$. Then, x is either in C or not.

Supp. $x \in A \wedge x \in C \Rightarrow x \notin A \oplus C \Rightarrow x \notin B \oplus C$ ↯ (bec. as $x \notin B \wedge x \in C \Rightarrow x \in B \oplus C$)

Supp. $x \in A \wedge x \notin C \Rightarrow x \in A \oplus C \Rightarrow x \in B \oplus C \Rightarrow x \in B$ (as $x \notin C$ and $x \in B \oplus C$) $\Rightarrow$ ↯

Similar arguments hold when we assume $x \in B$.

6. Show that if $2^n - 1$ is a prime, then n is a prime. (2 pts)
(*Hint*: Use the identity $2^{ab} - 1 = (2^a - 1)(2^{a(b-1)} + 2^{a(b-2)} + \cdots + 2^a + 1)$)

Assume n is not a prime, ie $n = ab$, $a, b > 1$

Then, $2^n - 1 = 2^{ab} - 1 = \underbrace{(2^a - 1)}_{c}\underbrace{(2^{a(b-1)} + 2^{a(b-2)} + \cdots + 2^a + 1)}_{d}$

ie, $2^n - 1 = cd$, $c, d > 1$ ↯ , bec. $2^n - 1$ is prime.

7. Find the gcd(224,106) using the Euclidean algorithm. (2 pts)

$224 = 2 \cdot 106 + 12$

$106 = 8 \cdot 12 + 10$

$12 = 2 \cdot 10 + \boxed{2}$

$10 = 2 \cdot 5 + 0$

ie, $\gcd(224, 106) = 2$.

8. Use the *extended Euclidean algorithm* to write the gcd(218,105) as a linear combination of 218 and 105. Use that relation to find the inverse of 105 in $\mathbb{Z}_{218}$. (2 pts)

The Eucl. alg. gives : $218 = 2 \cdot 105 + 8$
$105 = 13 \cdot 8 + 1$

ie, $\gcd(218,105) = 1$.

By the extended Eucl. alg. we have : $1 = 1 \cdot 105 - 13 \cdot 8$
$1 = 1 \cdot 105 - 13(218 - 2 \cdot 105)$
$1 = (-13)218 + (27)105$

In $\mathbb{Z}_{218}$, $1 = (-13)\cancel{218}^{0} + (27)105$. That is $1 = 27 \cdot 105$.

Hence, the inverse of 105 in $\mathbb{Z}_{218}$ is $\boxed{27}$.

9. Solve the congruence $3x \equiv 7 \bmod 17$. List at least three integers that are solutions of the congruence. (2 pts)

The inverse of 3 in $\mathbb{Z}_{17}$ is 6 (Indeed, $3 \cdot 6 = 18 = 1$ in $\mathbb{Z}_{17}$)

So, $3x \equiv 7 \bmod 17 \Rightarrow 6 \cdot 3x \equiv 6 \cdot 7 \bmod 17$
$\Rightarrow x \equiv 42 \bmod 17$
$\Rightarrow x \equiv 8 \bmod 17$ (bec. $42 = 2 \cdot 17 + 8$)

ie, $\boxed{x = 8}$.

Another two solutions are 25 and 42.

10. Solve the system of congruences: $x \equiv 1 \bmod 2$
$x \equiv 2 \bmod 3$
$x \equiv 3 \bmod 5$ (2 pts)

Since 2, 3, 5 are pairwise relatively prime, the system has a unique solution modulo $\underbrace{2 \cdot 3 \cdot 5}_{30}$.

Let $M_1 = 30/2 = 15$, $M_2 = 30/3 = 10$, $M_3 = 30/5 = 6$.

Then, 1 is the inverse of 15 modulo 2
1 " " 10 " 3
1 " " 6 " 5.

So, the solution to the system is :

$x \equiv (1 \cdot 15 \cdot 1 + 2 \cdot 10 \cdot 1 + 3 \cdot 6 \cdot 1) \bmod 30 \Rightarrow x \equiv 53 \bmod 30$
$\Rightarrow \boxed{x \equiv 23 \bmod 30}$