MATH221-001 200530 Problem Set 3 Solutions

Edward Doolittle

October 24, 2005

1. (a) the set of even integers
   (b) the union of the set of composite integers (including 0) and $\{-1, 1\}$
   (c) the union of the set of prime numbers and $\{-1, 1\}$ (note that -2, etc., are prime)
   (d) the set of all integers the squares of which are less than or equal to 100, i.e., the set

$$\{-10, -9, -8, -7, -6, -5, -4, -3, -2, -1, 0, 1, 2, 3, 4, 5, 6, 7, 8, 9, 10\}.$$

2. The truth table for $(p \Rightarrow q) \wedge (q \Rightarrow p)$ can be constructed as in Table 1. (Note that I have added extra

p	q	$p \Rightarrow q$	q	p	$q \Rightarrow p$	$(p \Rightarrow q) \wedge (q \Rightarrow p)$
F	F	T	F	F	T	T
F	T	T	T	F	F	F
T	F	F	F	T	T	F
T	T	T	T	T	T	T

Table 1: Truth table for $(p \Rightarrow q) \wedge (q \Rightarrow p)$

columns for q and p which I find helpful when working with sub-expressions like $q \Rightarrow p$ which reverse the order of p and q.) Since the column for $(p \Rightarrow q) \wedge (q \Rightarrow p)$ matches the column for $p \Leftrightarrow q$ as given in the problem set, the two expressions are logically equivalent, and we can write $(p \Rightarrow q) \wedge (q \Rightarrow p) \equiv p \Leftrightarrow q$.

3. The statement "$6n - 1$ is a multiple of 5" is equivalent to the statement "$6n - 1 \equiv 0 \bmod 5$" which is equivalent to the statement "$n - 1 \equiv 0 \bmod 5$" which is equivalent to the statement "$n \equiv 1 \bmod 5$" which is true for infinitely many values of n, in particular $n = 5k + 1$, $k = 1, 2, \ldots$. For those values of n, $6n - 1 = 6(5k + 1) - 1 = 30k + 6 - 1 = 30k + 5 = 5(6k + 1)$ is a multiple of 5.

   We are not quite done, though. Some multiples of 5 are prime numbers, specifically -5 and 5. However, note that $6k + 1 > 1$ for $k \geq 1$, so for $n = 5k + 1$, $k \geq 1$ we have $6n - 1 = 5(6k + 1)$ is the product of two integers each greater than 1, so for that infinite set of values of n, $6n - 1$ is composite.

   (I chose the factor 5 because the argument is relatively simple for that factor; however we could have looked for factors different from 5, e.g., 7, 11, 25, etc. The argument becomes more complicated for those factors, though; try it! On the other hand, some factors won't work. Can you find a criterion that separates the factors that work from those that don't? Hint: for what numbers p is there a k such that $6n + pk = 1$?)

4. Note that $s = (p \Rightarrow q)$ where p is the statement "n is greater than 3 and n is prime" and q is the statement "$n + 1$ is not prime". The contrapositive of s is $\neg q \Rightarrow \neg p$. In words, $\neg q$ is "it is not the case that $n + 1$ is not prime", or more simply, "$n + 1$ is prime". In words, $\neg p$ is "it is not the case that: n is greater than 3 and n is prime", or simply "n is less than or equal to 3 or n is not prime". So in words, the contrapositive of s is "if $n + 1$ is prime then n is less than or equal to 3 or n is not prime".

   The statement s is true. Proof: if n is greater than 3 and n is prime, then n is odd and greater than 3, then $n + 1$ is even and greater than 4, then n is the product of 2 and some other number greater than 1, so $n + 1$ is composite, so $n + 1$ is not prime.

The truth value of the contrapositve of a statement is the same as the truth value of the original statement, so the contrapositive of s is also true.

5. (a) Let $g = \gcd(m, n)$. Since g is a common divisor of m and n we can write $m = rg$ and $n = sg$ for some integers r and s. Since d is a divisor of g we can write $g = td$ for some integer t. Then $m = rg = r(td) = (rt)d$ and $n = sg = s(td) = (st)d$, so d divides both m and n.

   (b) Again let $g = \gcd(m, n)$. By the Euclidean algorithm, there are integers x and y such that $g = xm + yn$. Since d divides both m and n we can write $m = rd$ and $n = sd$ for some integers r and s. Then $g = xm + yn = x(rd) + y(sd) = (xr)d + (ys)d = (xr + ys)d$ and it follows that d divides g.

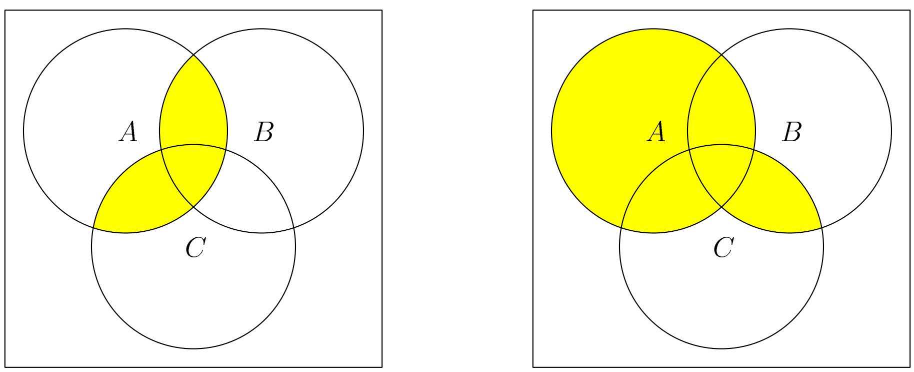
6. We need to prove two things, $D_{\gcd(m,n)} \subset D_m \cap D_n$ and $D_m \cap D_n \subset D_{\gcd(m,n)}$. As above, let $g = \gcd(m, n)$.

   (a) If $d \in D_{\gcd(m,n)}$ then d divides g. By 5a, d then divides m so $d \in D_m$, and d divides n so $d \in D_n$. Since d is in both D_m and D_n, it follows that $d \in D_m \cap D_n$. We have shown that every element of $D_{\gcd(m,n)}$ is also an element of $D_m \cap D_n$; therefore $D_{\gcd(m,n)} \subset D_m \cap D_n$.

   (b) If $d \in D_m \cap D_n$ then d divides both m and n. By 5b, it follows that d divides $\gcd(m, n)$ so $d \in D_{\gcd(m,n)}$. We have shown that every element of $D_m \cap D_n$ is also an element of $D_{\gcd(m,n)}$; therefore $D_m \cap D_n \subset D_{\gcd(m,n)}$.

   Since both $D_{\gcd(m,n)} \subset D_m \cap D_n$ and $D_{\gcd(m,n)} \supset D_m \cap D_n$, it follows that $D_{\gcd(m,n)} = D_m \cap D_n$.

7. Although it is not necessary for solving the problem, it is helpful to draw Venn diagrams for the sets in question; see Figure 1. If we can find sets A, B, and C for which there is an element in the shaded



(a) $A \cap (B \cup C)$ (b) $A \cup (B \cap C)$

Figure 1: Venn diagrams for $A \cap (B \cup C)$ and $A \cup (B \cap C)$

   region in Figure 1b which is not in the shaded region of 1a. One way to do that would be to let A be a set with an element that's not in B nor in C. The simplest example I can think of is to let $A = \{1\}$, $B = \{\}$, and $C = \{\}$. Then $A \cap (B \cup C) = \{1\} \cap (\{\} \cup \{\}) = \{1\} \cap \{\} = \{\}$ is not equal to $A \cup (B \cap C) = \{1\} \cup (\{\} \cap \{\}) = \{1\} \cup \{\} = \{1\}$.

   Of course, there are many other similar examples. Another class of examples can be found by constructing sets A, B, and C with an element in both B and C that is not in A.

8. Rearranging the examples from the textbook we have

$$\begin{aligned} 3^2 &= 5^2 - 4^2 = (5-4)(5+4) = 1 \times 9 \\ 5^2 &= 13^2 - 12^2 = (13-12)(13+12) = 1 \times 25 \\ 7^2 &= 25^2 - 24^2 = (25-24)(25+24) = 1 \times 49 \end{aligned}$$

and so on. We need to find two integers which differ by 1 and which sum to the square of an odd number. From the above pattern, if a^2 is an odd number, it seems we can use $c = (a^2+1)/2$ and $b = (a^2-1)/2$. Since a is odd, a^2 is odd, and $a^2 \pm 1$ is even and therefore divisible by 2, so b and c are integers. Furthermore,

$$a^2 + b^2 = a^2 + \left(\frac{a^2-1}{2}\right)^2 = a^2 + \frac{a^4}{4} - \frac{a^2}{2} + \frac{1}{4} = \frac{a^4}{4} + \frac{a^2}{2} + \frac{1}{4}$$

is in agreement with

$$c^2 = \left(\frac{a^2+1}{2}\right)^2 = \frac{a^4}{4} + \frac{a^2}{2} + \frac{1}{4}.$$

So for odd a, $(a, (a^2-1)/2, (a^2+1)/2)$ is a Pythagorean triple.

(Harder problem: find Pythagorean triples for even a which are "primitive", i.e., have no common factor.)

9. Let B be the statement "Bill is a Knight" and J the statement "John is a Knight". John's statement may then be written $\neg B \Rightarrow J$, and Bill's statement may be written $\neg(B \Leftrightarrow J)$. Then we have the truth table Table 2. The fourth line of the table can't represent the situation, because in it Bill is a

B	J	$\neg B$	J	$\neg B \Rightarrow J$	$B \Leftrightarrow J$	$\neg(B \Leftrightarrow J)$
F	F	T	F	F	T	F
F	T	T	T	T	F	T
T	F	F	F	T	F	T
T	T	F	T	T	T	F

Table 2: Truth table for $\neg B \Rightarrow J$ and $\neg(B \Leftrightarrow J)$

Knight (B is True) but he says something that is false ($\neg(B \Leftrightarrow J)$ is False). The third line of the truth table can't represent the situation either because in it John is a Knave (J is False) but he says something that is true ($\neg B \Rightarrow J$ is True). Nor can the second line of the truth table represent the situation because in it Bill is a Knave (B is False) but he says something that is true ($\neg(B \Leftrightarrow J)$ is True). However, the first line of the table can represent the situation because in it both Bill and John are Knaves and they both say something that is false. Therefore Bill must be a Knave and John must be a Knave.

There are other ways to solve the problem such as Boolean algebra which work just as well.

10. Yes.

One bonus mark for anyone who argued as follows: since the resident of the island was born, he/she cannot be infinitely old, and therefore made the statement "This is not the first time I have said what I am now saying" a first time. At that time, the statement must have been False, therefore the resident in question must have been a Knave when he/she said it. Since residents don't change from Knaves to Knights, he/she must still be a Knave now. (The reasoning breaks down if the individual made the statement an infinite number of times in the past; highly unlikely, if you ask me, but I had to rule out that possibility when I set up the question.)