

# MATH221-001 200630 Sample Final Exam Solutions DRAFT

Edward Doolittle

January 8, 2007

1. (a) We use the Euclidean Algorithm. Repeatedly dividing,

$$7205 = 1705 \times 4 + 385$$

$$1705 = 385 \times 4 + 165$$

$$385 = 165 \times 2 + 55$$

$$165 = 55 \times 3.$$

It follows that  $\text{GCD}(7205, 1705) = 55$ .

- (b) We rewrite three of the above division equations with the remainder on one side and everything else on the other:

$$385 = 7205 - 1705 \times 4$$

$$165 = 1705 - 385 \times 4$$

$$55 = 385 - 165 \times 2.$$

Now we substitute the second last equation into the last equation to obtain

$$385 = 7205 - 1705 \times 4$$

$$55 = 385 - (1705 - 385 \times 4) \times 2 = 385 \times 9 - 1705 \times 2.$$

Again, we substitute the second last equation into the last equation to obtain

$$55 = (7205 - 1705 \times 4) \times 9 - 1705 \times 2 = 7205 \times 9 - 1705 \times 38.$$

So we have  $d = 55 = 7205x + 1705y$  where  $x = 9$  and  $y = -38$ . You can easily check with arithmetic that the final result is correct.

2. Consider the Venn diagrams in Figure 1. Since not all the yellow parts of Figure 1(a) are not contained in the yellow parts of Figure 1(b), it is apparent that the set inclusion is false. But to prove that it is false, we need a specific counter-example. We try to find simple sets  $A$ ,  $B$ ,  $C$  for which there is an element in a yellow region in the left diagram that is not in a yellow region in the right diagram. The simplest example I can find is if there is an element in the region which is inside  $A$ , inside  $C$ , but outside  $B$ . So take, for example, the sets  $A = \{1\}$ ,  $B = \emptyset$ ,  $C = \{1\}$ ,  $U = \{1, 2\}$ . Then  $A \cap B = \emptyset$ ,  $(A \cap B)^c = U = \{1, 2\}$ ,  $A \cap C = \{1\}$ ,  $B \cap C = \emptyset$ ,  $(A \cap C) \cup (B \cap C) = \{1\} \cup \emptyset = \{1\}$ , and  $((A \cap C) \cup (B \cap C))^c = \{1\}^c = \{2\}$ . In this case  $(A \cap B)^c = \{1, 2\}$  is not a subset of  $((A \cap C) \cup (B \cap C))^c = \{2\}$ , which disproves the general statement.
3. It's easy to find a bijection  $k : \mathbb{N} \rightarrow S$ : let  $k(n) = n^3$ . We need to check that it is a bijection. It's obviously a surjection because  $T$  was defined as the image of  $k$ . It's an injection because  $k(n)$  is an increasing function of  $n$  (why?). So  $k$  is a bijection, so it has an inverse,  $h : S \rightarrow \mathbb{N}$ , which is also a bijection. (We could call  $h$  a cube root function, but it's only defined on numbers which are cubes.)

It's a little harder to find a bijection  $g : \mathbb{N} \rightarrow T$ . Draw a spiral starting at 0 and going to 2, -2, 4, -4, 6, -6, ... Then we start counting along the spiral: 0 is the first number, 2 is the second, -2 is

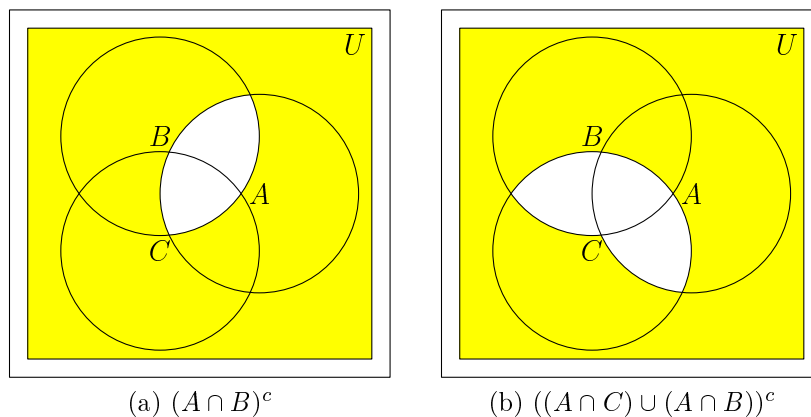


Figure 1: Venn diagrams for question 2

the third, 4 is the fourth, and so on. We should notice some patterns. After a little thought you could write

$$g(n) = \begin{cases} n, & n \text{ even} \\ -n + 1, & n \text{ odd} \end{cases}.$$

To prove that  $g$  is a surjection requires considering two cases. First, suppose  $m$  is even and positive. Then let  $n = m$ , so  $g(n) = m$ , so  $m$  is in the image of  $g$ . On the other hand, suppose  $m$  is even and non-positive, i.e., 0 or negative. Then let  $n = -m + 1$ . The number  $n$  is odd so  $g(n) = -n + 1 = -(-m + 1) + 1 = m - 1 + 1 = m$ , so again  $m$  is in the image of  $g$ . Therefore every even integer is in the range of  $g$ , and  $g$  is a surjection.

To show that  $g$  is an injection requires three cases. If  $n_1$  and  $n_2$  are both even, then  $g(n_1) = g(n_2)$  implies  $n_1 = n_2$ . If  $n_1$  and  $n_2$  are both odd, then  $g(n_1) = g(n_2)$  implies  $-n_1 + 1 = -n_2 + 1$  implies  $-n_1 = -n_2$  implies  $n_1 = n_2$ . And if  $n_1$  is odd and  $n_2$  is even (or vice versa) then  $g(n_1)$  is positive,  $g(n_2)$  is nonpositive, so  $g(n_1) = g(n_2)$  is impossible. In all possible cases we have  $g(n_1) = g(n_2)$  implies  $n_1 = n_2$ , so the function is an injection.

Altogether we have  $h : S \rightarrow \mathbb{N}$  a bijection,  $g : \mathbb{N} \rightarrow T$  a bijection, so the composition  $f = g \circ h : S \rightarrow T$  is a bijection and we are done.

That level of detail in the above solution is perhaps unnecessarily complete; but the problem is largely solved by noting that  $h$  is the cube root function and drawing a spiral diagram to describe  $g$ . Then a few points for recognizing each of the facts that has to be proven (facts about surjections, injections, inverses, and compositions), and a point for at least sketching out some of the proofs.

4. You might get started on this by “getting your hands dirty”, that is, looking at what happens for various values of  $n$ . For example, we have the values in Table 1. We notice a few interesting things. Clearly

$n$	$n^2 + 24n - 25$
-2	$-69 = -3 \times 23$
-1	$-50 = -2 \times 5 \times 5$
0	$-25 = -1 \times 5 \times 5$
1	$0 = 0 \times \text{something}$
2	$27 = 1 \times 3^3$
3	$56 = 2 \times 2^2 \times 7$

Table 1: Some values of  $n^2 + 24n - 25$

none of the numbers so far is prime. However, the most important is probably that  $n^2 + 24n - 25 = 0$

when  $n = 1$ , so  $n - 1$  is a factor, and we can factorize  $n^2 + 24n - 25 = (n - 1)(n + 25)$ . In general, that will be a composite number because it is the product of two integer factors!

However, there is one additional complication: in the cases  $n = 0$  and  $n = 2$ , the first factor of  $(n - 1)(n + 25)$  is a unit (either  $+1$  or  $-1$ ); however, note that the results are still not prime in those cases anyway, so we're safe. Or are we? There are two other cases where one of the factors is a unit: namely  $n = -24$  and  $n = -26$ . In the first case we have  $(-24 - 1)(-24 + 25) = -25$  is not a prime, and in the second we have  $(-26 - 1)(-26 + 25) = 27$  is not a prime. So in all cases but four we have  $n^2 + 24n - 25 = (n - 1)(n + 25)$  is not a prime because it is the product of two non-unit factors; we need to check the other four cases by hand, but the result is true in those cases too.

The bulk of the problem is noticing that  $n^2 + 24n - 25$  factors. The four special cases are the finishing touch for full marks.

5. This is an induction question; whenever you see the ellipsis  $\dots$  you should recognize the question as an induction question. First we check the base: when  $n = 1$  the left hand side is  $1/\sqrt{1} = 1$ , the right hand side is  $\sqrt{1} = 1$ , we have  $1/\sqrt{1} \geq \sqrt{1}$ , so the statement is true. At this point it might help to "get your hands dirty" and try a few more of the statements to get a feel for how they might be connected, e.g., try to prove the statement for  $n = 2$ ,  $n = 3$ ,  $n = 4$  without yet worrying about constructing a general induction proof.

Now assume the induction hypothesis that

$$\frac{1}{\sqrt{1}} + \frac{1}{\sqrt{2}} + \dots + \frac{1}{\sqrt{k}} \geq \sqrt{k}$$

for some natural number  $k$ . In the induction step we want to use the induction hypothesis to prove the next result, i.e.,

$$\frac{1}{\sqrt{1}} + \frac{1}{\sqrt{2}} + \dots + \frac{1}{\sqrt{k}} + \frac{1}{\sqrt{k+1}} \geq \sqrt{k+1}.$$

The two most recent displayed inequalities are different kinds of statements! The first is assumed to be true. The second is only a conjecture at this point. You might want to keep the difference straight by writing a question mark over the inequality sign in the second. Anyway, let us start with the induction hypothesis and modify it to look more like the conclusion we want:

$$\begin{aligned} \frac{1}{\sqrt{1}} + \frac{1}{\sqrt{2}} + \dots + \frac{1}{\sqrt{k}} &\geq \sqrt{k} \\ \frac{1}{\sqrt{1}} + \frac{1}{\sqrt{2}} + \dots + \frac{1}{\sqrt{k}} + \frac{1}{\sqrt{k+1}} &\geq \sqrt{k} + \frac{1}{\sqrt{k+1}}. \end{aligned}$$

That is something like the conclusion we want. Now for some wishful thinking: if we had the result

$$\sqrt{k} + \frac{1}{\sqrt{k+1}} \geq \sqrt{k+1} \tag{1}$$

then we could write

$$\frac{1}{\sqrt{1}} + \frac{1}{\sqrt{2}} + \dots + \frac{1}{\sqrt{k}} + \frac{1}{\sqrt{k+1}} \geq \sqrt{k} + \frac{1}{\sqrt{k+1}} \geq \sqrt{k+1}$$

and by the transitivity of  $\geq$  we'd be done. Let's see if we can prove (1). Multiplying both sides by  $\sqrt{k+1}$  (which is a positive number so doesn't change the direction of the inequality sign) we have that our goal is equivalent to

$$\sqrt{k}\sqrt{k+1} + 1 \geq (\sqrt{k+1})^2.$$

Simplifying we have that our goal is equivalent to

$$\sqrt{k}\sqrt{k+1} \geq k.$$

But that statement is true because

$$\begin{aligned}\sqrt{k} &\geq \sqrt{k} \\ \sqrt{k+1} &\geq \sqrt{k}\end{aligned}$$

and we can multiply those inequalities together to get the desired result. Reversing our steps, we have a chain of reasoning that establishes the induction step. The statement therefore holds for all natural numbers  $n$  by the Principle of Mathematical Induction.

The last step is rather tricky, but the rest of the problem is straightforward.

6. (a)  $(3, 2) \sim (1, 4)$  because  $3 + 2 = 5 = 1 + 4$ , but  $(8, -1) \not\sim (0, 9)$  because  $8 + -1 = 7 \neq 9 = 0 + 9$ .
  - (b) We need to prove RST: reflexive, symmetric, and transitive. Reflexive:  $(x, y) \sim (x, y)$  is always true because  $x + y = x + y$  is always true. Symmetric:  $(x, y) \sim (z, w)$  implies  $x + y = z + w$  implies  $z + w = x + y$  implies  $(z, w) \sim (x, y)$ . Transitive:  $(x, y) \sim (z, w)$  and  $(z, w) \sim (u, v)$  implies  $x + y = z + w$  and  $z + w = u + v$  implies  $x + y = u + v$  implies  $(x, y) \sim (u, v)$ . Since the relation  $\sim$  is reflexive, symmetric, and transitive, it is an equivalence relation.
  - (c) The equivalence class of  $(2, 3)$  is the set of all points  $(x, y)$  satisfying  $(x, y) \sim (2, 3)$ , i.e.,  $x + y = 2 + 3$ , i.e.,  $x + y = 5$ . That is a line in the plane, specifically the line passing through the points  $(0, 5)$  and  $(5, 0)$ . Graph that line on the plane.
  - (d) Existence:  $(x, y) \sim (a, 0)$  is equivalent to  $x + y = a$ ; setting  $a$  to that value gives us a point of the form  $(a, 0)$  which is equivalent to  $(x, y)$ . Uniqueness: if  $(x, y) \sim (a, 0)$  and  $(x, y) \sim (b, 0)$ , then by the properties of the equivalence relation we have  $(a, 0) \sim (b, 0)$ , i.e.,  $a + 0 = b + 0$ , i.e.,  $a = b$ , so the point  $(a, 0)$  was unique after all.
7. The key to solving this problem is finding an inverse for 63 modulo 128, which we can do by finding an expression of the form  $63x + 128y = 1$ . That kind of expression should look familiar, from question 1 for example. We apply the Euclidean Algorithm to 63 and 128:

$$\begin{aligned}128 &= 63 \times 2 + 2 \\ 63 &= 2 \times 31 + 1 \\ 2 &= 1 \times 2\end{aligned}$$

so  $\text{GCD}(63, 128) = 1$ . But more than that, we can find integers  $x$  and  $y$  such that  $63x + 128y = 1$  by rewriting the above division equations:

$$\begin{aligned}2 &= 128 - 63 \times 2 \\ 1 &= 63 - 2 \times 31 = 63 - (128 - 63 \times 2) \times 31 = 63 \times 63 - 128 \times 31\end{aligned}$$

which you should be able to check with easy arithmetic. It follows that  $1 \equiv 63 \times 63 \pmod{128}$ , so an inverse for 63 modulo 128 is (coincidentally) 63.

Now we take the equation with which we started and multiply both sides by 63 to obtain

$$\begin{aligned}63x &\equiv 119 \pmod{128} \\ 63 \times 63x &\equiv 63 \times 119 \pmod{128} \\ 1 \times x &\equiv 63 \times 119 \pmod{128} \\ x &\equiv 63 \times 119 \pmod{128}.\end{aligned}$$

We can now write the solution set  $S$  as the set of all numbers which are in the same residue class as  $63 \times 119$  modulo 128; namely, the solution set can be written  $S = \{63 \times 119 + 128n : n \in \mathbb{Z}\}$ . You can do the arithmetic to simplify the description of  $S$ , but I'm fine with it the way it stands.

8. The idea behind this question is if I'm trying to figure out what  $\text{GCD}(x, y)$  is, I can add or subtract any integer multiple of  $x$  to  $y$  or vice versa and leave the result unchanged. As a simple example, if  $a$  and  $b$  are relatively prime I can conclude that  $\text{GCD}(a, a + b) = 1$  because  $\text{GCD}(a, a + b) = \text{GCD}(a, (a + b) - a) = \text{GCD}(a, b) = 1$  because  $a$  and  $b$  are relatively prime.

As a slightly more complicated example, if  $a$  and  $b$  are relatively prime, then  $\text{GCD}(a, a + 2b) = 1$  or  $2$  because  $\text{GCD}(a, a + 2b) = \text{GCD}(a, a + 2b - a) = \text{GCD}(a, 2b)$ . At this point, we can proceed in a number of ways. For example, we can split into cases  $a$  even or  $a$  odd and use unique factorization. Or we can write  $\text{GCD}(a, 2b) | \text{GCD}(2a, 2b)$  because multiplying an argument of the GCD function cannot remove factors from the result but can add factors to the result (again by unique factorization, fill in the details). However, the cleanest way to get the answer is probably by this kind of argument:  $a, b$  relatively prime implies  $ax + by = 1$  for some integers  $x, y$ . But then  $a(2x) + (2b)y = 2$ , and it follows that any common divisor of  $a$  and  $2b$  must divide  $2$ , so the greatest common divisor of  $a$  and  $2b$  must divide  $2$ , i.e., must be either  $1$  or  $2$ .

Now, turning to our problem, the most elegant way to proceed is to note that

$$\text{GCD}(a + b, a^2 + b^2) = \text{GCD}(a + b, a^2 + b^2 + k(a + b))$$

for any  $k$ . In particular, setting  $k = -(a - b)$  we have

$$\text{GCD}(a + b, a^2 + b^2) = \text{GCD}(a + b, a^2 + b^2 - (a - b)(a + b)) = \text{GCD}(a + b, 2b^2).$$

Since we are given that  $\text{GCD}(a, b) = 1$  we have  $ax + by = 1$  for some integers  $x, y$ , we have

$$(a + b)x_1 + by_1 = 1$$

where  $x_1 = x$  and  $y_1 = y - x$ . Rearranging and squaring,

$$by_1 = 1 - (a + b)x_1 \implies 2(by_1)^2 = 2(1 - (a + b)x_1)^2 = 2 - 4(a + b)x_1 + 2(a + b)^2x_1^2$$

Rearranging to be a linear relationship between  $a + b$  and  $2b^2$ ,

$$(a + b)[4x_1 - 2(a + b)x_1^2] + 2b^2[y_1^2] = 2.$$

We can conclude that any common divisor of  $a + b$  and  $2b^2$  divides  $2$ , so the greatest common divisor of those numbers divides  $2$ , so the greatest common divisor of those numbers is either  $1$  or  $2$ .

There are a number of other ways to proceed, using unique factorization for example, but they are messy in comparison with the above reasoning.

Admittedly, the problem is rather tricky, but the ideas are important.

9. The three given conditions can be translated to the statements  $p \vee q \implies \neg r$ ,  $p \vee s$ ,  $\neg s$ , and the question  $(C \cup D)^c = U$  translates to  $\neg(r \vee s)$ . We create a truth table like Table 2 and fill in the truth values of  $\neg s$ . Since we are given that  $\neg s$  is true, we can eliminate all the rows where  $\neg s$  is false, obtaining Table 3. Filling in the truth values of  $p \vee s$  in Table 3 and eliminating rows where that condition is false we obtain Table 4. Finally, eliminating rows where the condition  $p \vee q \implies \neg r$  is false and filling in the truth values of the question  $\neg(r \vee s)$  we obtain Table 5. We see that whenever all the given conditions are true, the conclusion is necessarily true. Translating back into set theory language, we have that if the three given conditions are true, the conclusion  $(C \cup D)^c = U$  must be true.
10. (a) Consider Table 6 of residues modulo 8 and their squares. Every odd number is congruent to 1, 3, 5, or 7 modulo 8 (why?) so the square of any odd number is congruent to 1 mod 8. Similarly, it follows from the table that the square of any even number is congruent to 0 or 4 mod 8.
- (b) By the above, the sum of two squares can only have the residues  $0 + 0 \equiv 0$ ,  $0 + 1 \equiv 1$ ,  $0 + 4 \equiv 4$ ,  $1 + 0 \equiv 1$ ,  $1 + 1 \equiv 2$ ,  $1 + 4 \equiv 5$ ,  $4 + 0 \equiv 4$ ,  $4 + 1 \equiv 5$ , or  $4 + 4 \equiv 0$  modulo 8. However,  $2006 \equiv 6 \pmod{8}$  which isn't in the list. It follows that the equivalence  $x^2 + y^2 \equiv 2006 \pmod{8}$  has no solution, so the equation  $x^2 + y^2 = 2006$  can have no solution either.

$p$	$q$	$r$	$s$	$p \vee q \Rightarrow \neg r$	$p \vee s$	$\neg s$	$\neg(r \vee s)$
F	F	F	F			T	
F	F	F	T			F	
F	F	T	F			T	
F	F	T	T			F	
F	T	F	F			T	
F	T	F	T			F	
F	T	T	F			T	
F	T	T	T			F	
T	F	F	F			T	
T	F	F	T			F	
T	F	T	F			T	
T	F	T	T			F	
T	T	F	F			T	
T	T	F	T			F	
T	T	T	F			T	
T	T	T	T			F	

Table 2: Full truth table for all statements

$p$	$q$	$r$	$s$	$p \vee q \Rightarrow \neg r$	$p \vee s$	$\neg s$	$\neg(r \vee s)$
F	F	F	F		F	T	
F	F	T	F		F	T	
F	T	F	F		F	T	
F	T	T	F		F	T	
T	F	F	F		T	T	
T	F	T	F		T	T	
T	T	F	F		T	T	
T	T	T	F		T	T	

Table 3: Partial truth table, only rows where  $\neg s$

$p$	$q$	$r$	$s$	$p \vee q \Rightarrow \neg r$	$p \vee s$	$\neg s$	$\neg(r \vee s)$
T	F	F	F	T	T	T	
T	F	T	F	F	T	T	
T	T	F	F	T	T	T	
T	T	T	F	F	T	T	

Table 4: Only rows where  $\neg s$  and  $p \vee s$

$p$	$q$	$r$	$s$	$p \vee q \Rightarrow \neg r$	$p \vee s$	$\neg s$	$\neg(r \vee s)$
T	F	F	F	T	T	T	T
T	T	F	F	T	T	T	T

Table 5: Only rows where  $\neg s$  and  $p \vee s$  and  $p \vee q \Rightarrow \neg r$

$x$	$x^2 \pmod{8}$
0	0
1	1
2	4
3	1
4	0
5	1
6	4
7	1

Table 6: Squares modulo 8

- (c) We have  $1000 \equiv 0 \pmod{8}$  so by the above we must have  $x^2, y^2 \equiv 0 \pmod{8}$  or  $x^2, y^2 \equiv 4 \pmod{8}$ . In the former case, going back to Table 6 we have either  $x, y \equiv 4 \pmod{8}$  or  $x, y \equiv 0 \pmod{8}$ ; in both those cases we have  $4|x, y$  so  $16|(x^2 + y^2)$  so  $16|1000$ , impossible. It follows that we must have  $x^2, y^2 \equiv 4 \pmod{8}$  which, going back to Table 6, implies  $x, y \equiv 2 \pmod{4}$  (why?). So we can write  $x = 4m + 2 = 2(2m + 1)$ ,  $y = 4n + 2 = 2(2n + 1)$ . Squaring those we get

$$x^2 + y^2 = 4(2m + 1)^2 + 4(2n + 1)^2 = 1000$$

which means that we must express 250 as the sum of two odd squares. Checking all the possibilities, we see that  $15^2 + 5^2 = 250$  and  $9^2 + 13^2 = 250$ , giving us the four solutions  $(x, y) = (10, 30), (30, 10), (18, 26), (26, 18)$ .

Modular arithmetic didn't solve this equation for us, but helped us cut down on the number of solutions for us to try.

The last part of this problem is quite hard, but the first two parts should be accessible.