

MAS 117

Introduction to Algebra

In-term Test

Solutions and comments

Here are correct solutions with explanations and comments about where you went wrong.

1 (20 marks)

(a) Write down the *contrapositive* of the statement

“If n is an even integer greater than 2, then n is the sum of two prime numbers.”

Remark: The statement given happens to be a famous open problem known as Goldbach’s conjecture. A few years ago, a novel called *Uncle Petros and Goldbach’s Conjecture* was published. The publishers offered a £1,000,000 prize for a proof within a year of the novel’s publication. Nobody claimed the prize!

The *contrapositive* of the statement “if A , then B ” is the statement “if not- B , then not- A ”. This is logically equivalent to the original statement.

So the answer to the question is:

If n is not the sum of two prime numbers, then n is not an even integer greater than 2.

Warning: “not an even integer greater than 2” is not the same as “an odd integer greater than 2”. [WHY?] Also, quite a few people thought that “not the sum of two primes” is the same as “the sum of two non-primes”; well, it isn’t.

(b) Write down the *converse* of the above statement.

The *converse* of the statement “if A , then B ” is the statement “if B , then A ”. This is usually *not* logically equivalent to the original statement.

So the answer to the question is:

If n is the sum of two prime numbers, then n is an even integer greater than 2.

Some people wrote

If n is not an even integer greater than 2, then n is not the sum of two prime numbers.

This is the contrapositive of the converse, and so is logically equivalent to the converse; I allowed marks for this answer.

(c) Is the converse true? Why or why not?

At this point I need to remind some of you that “sum” means add; “product” means multiply!

The converse is false, so we give a counterexample. The number 5 is the sum of two prime numbers (it is $3 + 2$) but is not an even integer greater than 2.

I allowed half marks if you gave an incorrect converse, but a correct proof or counterexample to the statement you gave.

2 (20 marks) Prove by induction that

$$1^2 + 2^2 + \cdots + n^2 = \frac{n(n+1)(2n+1)}{6}$$

for any positive integer n .

Let $A(n)$ be the proposition

$$1^2 + 2^2 + \cdots + n^2 = \frac{n(n+1)(2n+1)}{6}.$$

Starting the induction: $A(1)$ is the statement

$$1^2 = \frac{1 \cdot 2 \cdot 3}{6},$$

which is true.

Inductive step: assume that $A(n)$ is true. Now the left-hand side of $A(n+1)$ is

$$\begin{aligned} 1^2 + 2^2 + \cdots + n^2 + (n+1)^2 &= \frac{n(n+1)(2n+1)}{6} + (n+1)^2 \\ &= \frac{(n+1)(n(2n+1) + 6(n+1))}{6} \\ &= \frac{(n+1)(2n^2 + 7n + 6)}{6} \\ &= \frac{(n+1)(n+2)(2n+3)}{6}, \end{aligned}$$

which is the right-hand side of $A(n+1)$ (obtained by replacing n by $n+1$ in the right-hand side of $A(n)$). So $A(n+1)$ holds.

By induction, $A(n)$ holds for all integers $n \geq 1$.

If you started the induction correctly, and did the inductive step correctly, but forgot to conclude that the statement was now proved for all n , you lost marks.

Warning: Please don't write $n = n + 1$. This makes no sense. If you want to assume that $A(k)$ is true and prove that $A(k+1)$ is true, that's OK; then you get $A(k+1)$ by putting $n = k+1$ in $A(n)$. This is a good, safe strategy.

3 (20 marks) True or false? Give reasons.

(a) The operation of matrix multiplication satisfies the commutative law.

False. For example

$$\begin{pmatrix} 0 & 1 \\ 2 & 3 \end{pmatrix} \begin{pmatrix} 1 & 1 \\ 1 & 1 \end{pmatrix} = \begin{pmatrix} 1 & 1 \\ 5 & 5 \end{pmatrix} \neq \begin{pmatrix} 2 & 4 \\ 2 & 4 \end{pmatrix} = \begin{pmatrix} 1 & 1 \\ 1 & 1 \end{pmatrix} \begin{pmatrix} 0 & 1 \\ 2 & 3 \end{pmatrix}.$$

Comment: If you think it is false, give a specific counterexample!

(b) The operation of multiplication on the integers satisfies the inverse law.

False. The integer 2 has no inverse; there is no integer x such that $2x = 1$.

Comment: As above!

A common mistake was to say that it is true because, if $a \neq 0$, then $a \cdot a^{-1} = 1$, and to forget that a^{-1} is usually not an integer.

(c) The operation of union on the subsets of a set $\mathcal{S}$ satisfies the associative law.

True. If A, B, C are subsets of $\mathcal{S}$, then $(A \cup B) \cup C$ consists of all elements which are in A , or in B , or in C ; and so does $A \cup (B \cup C)$.

Comment: This time of course we need a general proof. If you use Venn diagrams, make sure that your diagrams are both clearly drawn and clearly explained!

4 (20 marks)

(a) What does it mean to say that a function $F : A \rightarrow B$ is (i) *one-to-one*, (ii) *onto*?

- F is one-to-one if, for all $a_1, a_2 \in A$, if $a_1 \neq a_2$ then $F(a_1) \neq F(a_2)$. [Or you can use the contrapositive: ... if $F(a_1) = F(a_2)$ then $a_1 = a_2$.]

Don't say

F is one-to-one if, for every input, there is a unique output.

That is the definition of a function! Informally, F is one-to-one if different inputs give different outputs.

- F is onto if, for every $b \in B$, there exists $a \in A$ such that $F(a) = b$.

Informally, every element of B is the output for some input.

It is *not* correct to say that “onto” means that, for any output, there is more than one input. This is “not one-to-one”.

(b) Which of these properties does the function $F : \mathbb{Z} \rightarrow \mathbb{Z}$ given by $F(x) = x^3$ enjoy?

F is one-to-one: for, if $F(a_1) = F(a_2)$, then $a_1^3 = a_2^3$, so that $a_1 = a_2$ (taking the cube root).

A table of a few values of F will not do as an answer.

F is not onto, since there is no number $a \in \mathbb{Z}$ such that $a^3 = 2$. For $F(x) = x^3$ is an increasing function of x , and $1^3 = 1$, $2^3 = 8$; so a number a with $a^3 = 2$ would have to lie between 1 and 2, and there is no such integer.

5 (20 marks) Use Euclid's Algorithm to find the greatest common divisor d of 63 and 204, and to express d in the form $63x + 204y$, where x and y are integers.

$$204 = 63 \cdot 3 + 15$$

$$63 = 15 \cdot 4 + 3$$

$$15 = 3 \cdot 5$$

so $\gcd(204, 63) = \gcd(63, 15) = \gcd(15, 3) = \gcd(3, 0) = 3$.

From the above equations,

$$\begin{aligned} 3 &= 63 - 4 \cdot 15 \\ &= 63 - 4 \cdot (204 - 3 \cdot 63) \\ &= 13 \cdot 63 - 4 \cdot 204 \end{aligned}$$

so the equation holds with $x = 13$, $y = -4$.

Warning: If you said that $204 = 2^2 \cdot 3 \cdot 17$ and $63 = 3^2 \cdot 7$, so the greatest common divisor is 3, you didn't get marks, since the question specifically told you to use Euclid's algorithm.