MATHEMATICS 300 — FALL 2018
Introduction to Mathematical Reasoning
H. J. Sussmann

MIDTERM EXAM — *December 4, 2018*

SOLUTIONS

Problem 1.

Define "greatest common divisor".

ANSWER: If a, b are integers, a greatest common divisor of a and b is an integer g such that

1. g divides a and g divides b,
2. if c is an integer that divides a and b, then $c \leq g$.

ANOTHER CORRECT ANSWER: Let a, b, g be integers, We say that g is a greatest common divisor of a and b if

$$g|a \wedge g|b \wedge (\forall c \in \mathbb{Z})\Big((c|a \wedge c|b) \Longrightarrow c \leq g\Big).$$

Define "prime number".

ANSWER: A prime number is a natural number p such that $p > 1$ and the only natural numbers that divide p are 1 and p.

ANOTHER CORRECT ANSWER: Let p be an integer. We say that p is a prime number if $p>1$ and the only natural numbers that divide p are 1 and p.

A THIRD CORRECT ANSWER: Let p be an integer. We say that p is a prime nuumber if

$$p > 1 \wedge (\forall k \in \mathbb{N})\Big(k|p \Longrightarrow (k = 1 \vee k = p)\Big).$$

A FOURTH CORRECT ANSWER: A prime number is an integer p such that

$$p > 1 \wedge (\forall j \in \mathbb{N})(\forall k \in \mathbb{N})\Big(p = jk \Longrightarrow (j = 1 \vee j = p)\Big).$$

A FIFTH CORRECT ANSWER: A prime number is an integer p such that

$$p > 1 \wedge (\forall j \in \mathbb{N})(\forall k \in \mathbb{N})\Big(p = jk \Longrightarrow (j = 1 \vee k = 1)\Big).$$

Prove that if the greatest common divisor of two integers exists, then it is unique.

ANSWER: Let a, b be integers. Suppose that g_1 and g_2 are greatest common divisors of a and b. We want to prove that $g_1 = g_2$.

Since g_1 is a GCD of a and b, every integer c such that $c|a$ and $c|b$ satisfies $c \leq g_1$. In particular, since g_2 is a GCD of a and b, g_2 divides a and b, so $g_2 \leq g_1$.

A similar argument shows that $g_1 \leq g_2$. Hence $g_1 = g_2$. **Q.E.D.**

Prove that if a, b are integers that are not both zero, then the greatest common divisor g of of a and b exists, and is equal to the smallest positive integer linear combination of a and b. (This result is known as *Bézout's Lemma.*)

ANSWER: Let a, b be integers. Assume that a and b are not both zero, that is, that $a \neq 0 \vee b \neq 0$.

Let S be the set of all natural numbers that are integer linear combinations of a and b. That is,

$$S = \{c \in \mathbb{N} : (\exists u \in \mathbb{Z})(\exists v \in \mathbb{Z})c = ua + vb\}\,.$$

Then S is a subset of $\mathbb{N}$, and S is nonempty because, for example, the number $|a| + |b|$ (or the number $a^2 + b^2$) belongs to S.

Hence, by the well-ordering principle, S has a smallest member s.

We will prove that s is the greatest common divisor of a and b. For this purpose, we have to prove that

$$s|a \wedge s|b\,, \tag{1}$$

$$(\forall k \in \mathbb{Z})\Big((k|a \wedge k|b) \Longrightarrow k \leq s\Big)\,. \tag{2}$$

To prove (1), we assume that s does not divide a. Then we can use the division theorem, and write

$$a = sq + r\,, \qquad 0 \leq r < s\,. \tag{3}$$

It follows that $r > 0$, because $r \geq 0$ and r cannot be 0, since we are assuming that s does not divide a.

On the other hand, $r = a - sq$. Since $s \in S$, we may write

$$s = ua + vb\,,\;\; u \in \mathbb{Z}\,,\;\; v \in \mathbb{Z},.$$

Then $r = a - sq = a - (ua + vb)q = (1 - uq)a + (-vq)b$, so r is an integer linear combination of a and b. Since $r \in \mathbb{Z}$ and $r > 0$, r belongs to S. Since s is the smallest member of S, $\boxed{r \geq s}$.

But $\boxed{r < s}$. So we have reached a contradiction. Hence $\boxed{s \text{ divides } a}$.

A similar argument shows that s divides b, So (1) has been proved.

To prove (2), we let k be an arbitrary integer, and assume that $k|a \wedge k|b$. We want to prove that $k \leq s$. This is clearly true if $k \leq 0$, because $s > 0$. Now assume that $k > 0$. Then we may write

$$a = mk\,,\;\; b = nk\,,\;\; m \in \mathbb{Z}\,,\;\; n \in \mathbb{Z}\,.$$

Hence $s = ua + vb = umk + vnk = (um + vn)k$.

Let $p = um + vn$. Then $p \in \mathbb{Z}$ and p must be positive, because $s = pk$ and both s, k are positive. So $p \geq 1$. Then $pk \geq k$, so $s \geq k$. Hence we have proved that $k \leq s$, and this completes our proof that s is the greatest common divisor of a and b. **Q.E.D.**

Problem 2. ***Prove***, using Bézout's Lemma, and *without using the Fundamental Theorem of Arithmetic*, that if a, b, p are integers, p is prime, and p divides ab, then p divides a or p divides b. (This result is known as *Euclid's Lemma.*)

ANSWER: Let a, b, p be integers such that p is prime. Assume that $p|ab$. We want to prove that $p|a \vee p|b$.

We use the rule for proving a disjunction: to prove $A \vee B$, we assume $\sim A$ and prove B.

Assume that p does not divide a. Since p is prime, the only possible positive integer common factor of p and a is 1. Hence we can write

$$1 = ua + vp\,,\;\; u \in \mathbb{Z}\,,\;\; v \in \mathbb{Z}\,.$$

Since $p|ab$, we can write

$$ab = kp\,,\;\; k \in \mathbb{Z}\,.$$

Then

$$\begin{aligned} b &= b \times 1 \\ &= b \times (ua + vp) \\ &= uab + bvp \\ &= ukp + bvp \\ &= (uk + bv)p\,. \end{aligned}$$

Since $uk + bv \in \mathbb{Z}$, it follows that $p|b$.

Since we have proved that $p|b$ assuming that $\sim p|a$, it follows that $\boxed{p|a \vee p|b}$. **Q.E.D.**

ANOTHER CORRECT PROOF[1]***:*** Let a, b, p be integers such that p is prime. Assume that $p|ab$. We want to prove that $p|a \vee p|b$. We will do it by contradiction.

[1]This proof was unknown to me until Sunday December 9, when I found it in one of the papers I was grading. It's really a nice proof.

Assume that p does not divide a and does not divide b. (That is, assume the negation of "$p|a \vee p|b$".)

Then p and a are coprime and p and b are coprime. So we may write

$$1 = ma + np\,, \;\; 1 = ub + vp \quad m, n, u, v \in \mathbb{Z}\,.$$

Then, multiplying the above equations, we get

$$1 = (ma+np)(ub+vp) = mnab+npub+mavp+nvp^2 = mnab+(nub+mav+nvp)p\,.$$

So 1 is an integer linear combination of p and ab.

Therefore the greatest common divisor of p and b is 1. So $\boxed{p \text{ does not divide } ab}$.

But $\boxed{p \text{ divides } ab}$. So we got a contradiciton, proving that $p|a \vee p|b$. **Q.E.D.**

Problem 3. ***Prove*** that if a, b are integers and c, n are natural numbers then the number $(a + b\sqrt{c})^n + (a - b\sqrt{c})^n$ is an integer. (HINT: First prove by induction that there are integers u_n, v_n such that $(a+b\sqrt{c})^n = u_n + v_n\sqrt{c}$ and $(a-b\sqrt{c})^n = u_n - v_n\sqrt{c}$.)

ANSWER: We follow the hint.

Let $P(n)$ be the predicate

$$(\exists u_n \in \mathbb{Z})(\exists v_n \in \mathbb{Z})\Big((a + b\sqrt{c})^n = u_n + v_n\sqrt{c} \wedge (a - b\sqrt{c})^n = u_n - v_n\sqrt{c}\Big)\,.$$

We prove that $(\forall n \in \mathbb{N})P(n)$ by induction.

Basis step. We have to prove $P(1)$. But $P(1)$ says that there exist integers u_1, v_1 such that $a + b\sqrt{c} = u_1 + v_1\sqrt{c}$ and $a - b\sqrt{c} = u_1 - v_1\sqrt{c}$. And this existential statement follows by choosing as witnesses $u_1 = a$, $v_1 = b$. So $P(1)$ is true.

Inductive step. We have to prove that

$$(\forall n \in \mathbb{N})\Big(P(n) \Longrightarrow P(n+1)\Big)\,. \tag{4}$$

Let $n \in \mathbb{N}$ be arbitrary. We want to prove that $P(n) \Longrightarrow P(n+1)$.

Assume $P(n)$. Then we may write

$$(a + b\sqrt{c})^n = u_n + v_n\sqrt{c} \wedge (a - b\sqrt{c})^n = u_n - v_n\sqrt{c}\,, \;\; u_n, v_n \in \mathbb{Z}\,. \tag{5}$$

Then

$$\begin{aligned}(a + b\sqrt{c})^{n+1} &= (a + b\sqrt{c})^n(a + b\sqrt{c}) \\ &= (u_n + v_n\sqrt{c})(a + b\sqrt{c}) \\ &= u_n a + v_n bc + (u_n b + v_n a)\sqrt{c}\,,\end{aligned}$$

and

$$\begin{aligned}(a-b\sqrt{c})^{n+1} &= (a-b\sqrt{c})^n(a-b\sqrt{c})\\ &= (u_n - v_n\sqrt{c})(a-b\sqrt{c})\\ &= u_n a + v_n bc - (u_n b + v_n a)\sqrt{c}\,.\end{aligned}$$

Therefore, if we pick

$$u_{n+1} = u_n a + v_n b\,,\ \ v_{n+1} = (u_n b + v_n a)\,,$$

we see that

$$(a+b\sqrt{c})^{n+1} = u_{n+1} + v_{n+1}\sqrt{c}$$

and

$$(a-b\sqrt{c})^{n+1} = u_{n+1} - v_{n+1}\sqrt{c}\,.$$

So the integers u_{n+1}, v_{n+1} are witnesses for the existential statement $P(n+1)$. Hence we have proved $P(n+1)$.

Since we have proved $P(n+1)$ assuming $P(n)$, and we have done so for arbitrary $n \in \mathbb{N}$, and in additon we have proved $P(1)$, it follows that $(\forall n \in \mathbb{N})P(n)$.

End of the proof of the result of Problem 3. We want to prove that

$$(\forall n \in \mathbb{N})\Big((a+b\sqrt{c})^n + (a-b\sqrt{c})^n \in \mathbb{Z}\Big)\,.$$

(We are ***not*** going to do this part by induction. Induction would not work.)

Let $n \in \mathbb{N}$ be arbitrary.

Using the result proved before, we may write

$$(a+b\sqrt{c})^n = u_n + v_n\sqrt{c}\ \text{ and }\ (a-b\sqrt{c})^n = u_n - v_n\sqrt{c}\,,\ \ u_n, v_n \in \mathbb{Z}\,.$$

Then

$$(a+b\sqrt{c})^n + (a-b\sqrt{c})^n = 2u_n\,,$$

so $(a+b\sqrt{c})^n + (a-b\sqrt{c})^n$ is an integer, and our proof is complete. **Q.E.D.**

Problem 4. ***Prove*** that if x is a positive real number and n is natural number then

$$(1+x)^n \ge 1 + nx + \frac{n(n-1)}{2}x^2\,.$$

ANSWER: We want to prove that

$$(\forall x \in \mathbb{R})\Big(x > 0 \Longrightarrow (\forall n \in \mathbb{N})(1+x)^n \ge 1 + nx + \frac{n(n-1)}{2}x^2\Big)\,. \qquad (6)$$

Let x be an arbitrary real number. We want to prove

$$x > 0 \Longrightarrow (\forall n \in \mathbb{N})(1+x)^n \geq 1 + nx + \frac{n(n-1)}{2}x^2 \,. \tag{7}$$

Assume $x > 0$. We want to prove

$$(\forall n \in \mathbb{N})(1+x)^n \geq 1 + nx + \frac{n(n-1)}{2}x^2 \,. \tag{8}$$

We prove (8) by induction.

Let $P(n)$ be the predicate

$$(1+x)^n \geq 1 + nx + \frac{n(n-1)}{2}x^2 \,. \tag{9}$$

We prove $(\forall n \in \mathbb{N})P(n)$ by induction.

Basis step. We prove $P(1)$. Statement $P(1)$ says "$1+x \geq 1+x$", which is obviously true. So we have proved $\boxed{P(1)}$.

Inductive step. We have to prove that

$$(\forall n \in \mathbb{N})\big(P(n) \Longrightarrow P(n+1)\big) \,. \tag{10}$$

Let $n \in \mathbb{N}$ be arbitrary. We want to prove that $P(n) \Longrightarrow P(n+1)$.

Assume $P(n)$. Then

$$(1+x)^n \geq 1 + nx + \frac{n(n-1)}{2}x^2 \,. \tag{11}$$

Since $1+x > 0$ (because $x > 0$), we may multiply both sides of (11) by $1+x$, and get

$$(1+x)^n(1+x) \geq \Big(1 + nx + \frac{n(n-1)}{2}x^2\Big)(1+x) \,. \tag{12}$$

But

$$\begin{aligned}
\Big(1 + nx + \frac{n(n-1)}{2}x^2\Big)(1+x) &= 1 + nx + \frac{n(n-1)}{2}x^2 + x + nx^2 + \frac{n(n-1)}{2}x^3 \\
&= 1 + (n+1)x + \Big(n + \frac{n(n-1)}{2}\Big)x^2 + \frac{n(n-1)}{2}x^3 \\
&= 1 + (n+1)x + \Big(\frac{2n}{2} + \frac{n(n-1)}{2}\Big)x^2 + \frac{n(n-1)}{2}x^3 \\
&= 1 + (n+1)x + \frac{2n + n(n-1)}{2}x^2 + \frac{n(n-1)}{2}x^3 \\
&= 1 + (n+1)x + \frac{n(n+1)}{2}x^2 + \frac{n(n-1)}{2}x^3 \\
&\geq 1 + (n+1)x + \frac{n(n+1)}{2}x^2 + nx^2 \,,
\end{aligned}$$

where we dropped the term $\frac{n(n-1)}{2}x^3$ because it is positive, since $x > 0$. So

$$\begin{aligned}(1+x)^{n+1} &= (1+x)^n(1+x)\\ &\geq 1+(n+1)x+\frac{n(n+1)}{2}x^2+nx^2\,.\end{aligned}$$

Hence $P(n+1)$ holds.

This completes the induction. **Q.E.D.**

Problem 5. ***Prove*** by induction that

$$n < 2^n \qquad \text{for every } n \in \mathbb{N}\,.$$

ANSWER: We want to prove that

$$(\forall n \in \mathbb{N})P(n)\,, \tag{13}$$

where $P(n)$ is the predicate "$n < 2^n$".

We will prove (13) by induction.

Basis step. We prove $P(1)$. Statement $P(1)$ says "$1 < 2$" which is obviously true. So we have proved $\boxed{P(1)}$.

Inductive step. We have to prove that

$$(\forall n \in \mathbb{N})\big(P(n) \Longrightarrow P(n+1)\big)\,. \tag{14}$$

Let $n \in \mathbb{N}$ be arbitrary. We want to prove that $P(n) \Longrightarrow P(n+1)$.

Assume $P(n)$. Then

$$n < 2^n\,. \tag{15}$$

And then

$$\begin{aligned}n+1 &< 2^n+1\\ &< 2^n+2^n\\ &= 2.2^n\\ &= 2^{n+1}\,.\end{aligned}$$

So

$$n+1 < 2^{n+1}\,. \tag{16}$$

This means that $P(n+1)$ holds, and our inductive proof is complete. **Q.E.D.**

Problem 6. ***Define*** each of the following concepts:

1. union,.
2. intersection,
3. subset,
4. power set,
5. Cartesian product of sets.

ANSWER:

Definition of "union": Let A, B be sets. Then the union of A and B is the set $A \cup B$ given by

$$A \cup B = \{x : x \in A \vee x \in B\}\,.$$

Definition of "intersection": Let A, B be sets. Then the intersection of A and B is the set $A \cap B$ given by

$$A \cap B = \{x : x \in A \wedge x \in B\}\,.$$

Definition of "subset": Let A, B be sets. We say that A is a subset of B, and write "$A \subseteq B$", if every member of A is a member of B. That is,

$$A \subseteq B \Longleftrightarrow (\forall x)(x \in A \Longrightarrow x \in B)\,.$$

Definition of "power set": Let A be a set. The power set of A is the set $\mathcal{P}(A)$ of all the subsets of A. That is,

$$\mathcal{P}(A) = \{X : X \subseteq A\}\,.$$

Definition of "Cartesian product": Let A, B be sets. The Cartesian product of A and B is the set $A \times B$ of all the ordered pairs (a, b) such that $a \in A$ and $b \in B$. That is,

$$A \times B = \{x : (\exists a \in A)(\exists b \in B)x = (a, b)\}\,.$$

Equivalently,

$$A \times B = \{(a, b) : a \in A \wedge b \in B\}\,.$$

Problem 7. For each of the following sentences:

i. ***Translate*** the sentence into English. Please write normal-sounding sentences. Do not write horrible things like "for every member of the set of integers" when you can say instead "for every integer".

ii. ***Indicate*** if the sentence is true or false.

iii. ***Give a reason*** (i.e., a brief proof) for your true-false answer to part ii.

1. $(\forall X)\emptyset \in X$.

   ANSWER: For every set X, the empty set belongs to X. This is ***false.*** ***Proof:*** To disprove the universal sentence "$(\forall X)\ldots$", we give a counterexample. Let $X = \emptyset$. Then $\emptyset$ is not a member of X, because X has no members.

2. $(\forall X)\emptyset \subseteq X$.

   ANSWER: For every set X, the empty set is a subset of X. This is ***true.*** ***Proof:*** To prove the universal sentence "$(\forall X)\ldots$", we use Rule $\forall_{prove}$, and start with "Let X be arbitrary". Let X be an arbitrary set. We want to prove "$\emptyset \subseteq X$", i.e., $(\forall x)(x \in \emptyset \Longrightarrow x \in X)$. Let x be arbitrary. Then the implication "$x \in \emptyset \Longrightarrow x \in X$" is true, because it's an implication whose premise is false, since $\emptyset$ has no members. So $(\forall x)\Big(x \in \emptyset \Longrightarrow x \in X\Big)$. So $\emptyset \subseteq X$.

3. $(\forall X)\emptyset \in \mathcal{P}(X)$.

   ANSWER: For every set X, the empty set belongs to the power set $\mathcal{P}(X)$. This is ***true.*** ***Proof:*** To prove the universal sentence "$(\forall X)\ldots$", we use Rule $\forall_{prove}$, and start with "Let X be arbitrary". Let X be an arbitrary set. We know that $\emptyset$ is a subset of X. And the power set of X is emptysetthe set of all subets of X. Hence $\emptyset \in \mathcal{P}(X)$.

4. $(\forall X)\emptyset \subseteq \mathcal{P}(X)$.

   ANSWER: For every set X, the empty set is a subset of the power set $\mathcal{P}(X)$. This is ***true.*** ***Proof:*** The empty set is a subset of every set, so in particular it is a subset of the set $\mathcal{P}(X)$.

5. $(\forall X)\{\emptyset\} \subseteq X$

   ANSWER: For every set X, the singleton of the empty set is a subset of X. This is ***false.*** ***Proof:*** To disprove the universal sentence "$(\forall X)\ldots$", we give a counterexample. Let X be the empty set. Then X has no members, so $\emptyset \notin X$. Now the set $\{\emptyset\}$ is a subset of X if and only if every member of $\{\emptyset\}$ belongs to X, that is, if and only if $\emptyset \in X$. But $\emptyset \notin X$, so $\{\emptyset\}$ is not a subset of X.

6. $(\forall X)\{\emptyset\} \in \mathcal{P}(X)$.

ANSWER: For every set X, the singleton of the empty set belongs to the power set $\mathcal{P}(X)$. This is ***false.*** ***Proof:*** To disprove the universal sentence "$(\forall X)\ldots$", we give a counterexample. Let X be the empty set. Then X has no members, so $\emptyset \notin X$. Now the set $\{\emptyset\}$ is a subset of X if and only if every member of $\{\emptyset\}$ belongs to X, that is, if and only if $\emptyset \in X$. But $\emptyset \notin X$, so $\{\emptyset\}$ is not a subset of X. Therefore $\{\emptyset\}$ is not a member of $\mathcal{P}(X)$.

7. $(\forall X)\{\emptyset\} \subseteq \mathcal{P}(X)$.

   ANSWER: For every set X, the singleton of the empty set is a subset of the power set $\mathcal{P}(X)$. This is ***true.*** ***Proof:*** To prove the universal sentence "$(\forall X)\ldots$", we use Rule $\forall_{prove}$, and start with "Let X be arbitrary". Let X be an arbitrary set. We want to prove $\{\emptyset\} \subseteq \mathcal{P}(X)$. To prove this, we have to prove that every member of $\{\emptyset\}$ is in $\mathcal{P}(X)$. And this is true because the only member of $\{\emptyset\}$ is $\emptyset$, and we know that $\emptyset \in \mathcal{P}(X)$.

8. $(\forall m \in \mathbb{N})(\forall k \in \mathbb{N})\{n \in \mathbb{N} : m|n\} \subseteq \{n \in \mathbb{N} : km|n\}$.

   ANSWER: For all natural numbers m, k, the set of all natural numbers that are divisible by m is a subset of the set of all natural numbers that are divisible by km. This is ***false.*** ***Proof:*** To disprove the universal sentence "$(\forall m \in \mathbb{N})(\forall k \in \mathbb{N})\ldots$", we give a counterexample. Take $m = 2$, $k = 2$. Then $\{n \in \mathbb{N} : m|n\}$ is the set of all even natural numbers, and the set $\{n \in \mathbb{N} : km|n\}$ is the set of all natural numbers that are divisible by 4. Clearly, the first set is ot subset of the second set.

9. $(\forall m \in \mathbb{N})(\forall k \in \mathbb{N})\{n \in \mathbb{N} : km|n\} \subseteq \{n \in \mathbb{N} : m|n\}$.

   ANSWER: For all natural numbers m, k, the set of all natural numbers that are divisible by km is a subset of the set of all natural numbers that are divisible by m. This is ***true.*** ***Proof:*** To prove the universal sentence "$(\forall m \in \mathbb{N})(\forall k \in \mathbb{N})\ldots$", we use Rule $\forall_{prove}$, and start with "Let m, k be arbitrary". Let m, k be arbitrary natural numbers. Define sets A, B by letting $A = \{n \in \mathbb{N} : km|n\}$, $B = \{n \in \mathbb{N} : m|n\}$. If $n \in A$, then we can write $n = mkj$, $j \in \mathbb{Z}$. Then $m|n$, so $n \in B$. Hence $A \subseteq B$.

10. $(\forall x \in \mathbb{R})\Big(x > 0 \Longrightarrow (\exists u \in \mathbb{R})(\forall v \in \mathbb{R})(v > u \Longrightarrow v^2 < x)\Big)$

    ANSWER: For every positive real number x there exists a real number u such that every real number v for which $v > u$ satisfies $v^2 < x$. This is ***false.*** ***Proof:*** Suppose the statement was true. Then the statement "$(\exists u \in \mathbb{R})(\forall v \in \mathbb{R})(v > u \Longrightarrow v^2 < x)$", obtained by specializing to $x = 1$, would be true[2]. Then we can pick a witness u_*, so u_* is a real number such that $(\forall v \in \mathbb{R})(v > u_* \Longrightarrow v^2 < 1)$. Let $v_* = 1 + \max(u_*, 1)$. Then $v_* > u_*$, so $v_*^2 < 1$. But $v_* > 1$, so $v_*^2 > 1$. So we have arrived at a contradiction.

11. $(\forall x \in \mathbb{R})\Big(x > 0 \Longrightarrow (\exists u \in \mathbb{R})(\forall v \in \mathbb{R})(v > u \Longrightarrow \frac{1}{v^2} < x)\Big)$

ANSWER: For every positive real number x there exists a real number u such that every real number v for which $v > u$ satisfies $v^2 < x$. This is ***true.*** ***Proof:*** Let $x \in \mathbb{R}$ be arbitrary. Suppose $x > 0$. Pick $u_* = \frac{1}{\sqrt{x}}$. We show that u_* is a witness for the statement "$(\exists u \in \mathbb{R})(\forall v \in \mathbb{R})(v > u \Longrightarrow \frac{1}{v^2} < x)$". To show this, we have to prove that $(\forall v \in \mathbb{R})(v > u_* \Longrightarrow \frac{1}{v^2} < x)$. Let v be an arbitrary real number. Assume $v > u_*$. Then $v^2 > u_*^2$, so $\frac{1}{v_*^2} < \frac{1}{u_*^2}$. But $\frac{1}{u_*^2} = x$, so $\frac{1}{v_*^2} < x$, as desired.

Problem 8. ***Prove*** the existence part of the Fundamental Theorem of Arithmetic (FTA): if $n \in \mathbb{N}$ and $n \geq 2$ then n is a product of primes, that is, there exist $k \in \mathbb{N}$ and a list $(p_1, p_2, \ldots, p_k)$ of prime numbers such that

$$n = \prod_{j=1}^{k} p_j\,.$$

ANSWER:

Let B be the set of all natural numbers n such that $n \geq 2$ and n is not a product of primes.

We want to prove that the set B is empty. For this purpose, we assume that B is not empty and try to get a contradiction.

So assume that $B \neq \emptyset$. By the well-ordering principle, B has a smallest member b. Then $b \in B$, so

a. b is a natural number,

b. $b \geq 2$,

c. $\boxed{b \text{ is not a product of primes}}$.

[2]Notice that what we are doing here is exactly "disproving the universal statement $(\forall x \in \mathbb{R})P(x)\ldots$ by giving a counterexample". We are taking x to be 1, and showing that for that x the sentence $P(x)$ is not true. and we are proving that by contradiction: if $P(x)$—that is, "$x > 0 \Longrightarrow (\exists u \in \mathbb{R})(\forall v \in \mathbb{R})(v > u \Longrightarrow v^2 < x)$"— was true, then $(\exists u \in \mathbb{R})(\forall v \in \mathbb{R})(v > u \Longrightarrow v^2 < x)$ would be true—because x is positive—so we could pick a witness u_*, etc.

And, in addition,

d. b is the smallest member of B, that is,

$$(\forall m)(m \in B \Longrightarrow m \geq b)\,.$$

Since b is not a product of primes, it follows in particular that b is not prime. (Reason: if b was prime, then b would be a product of primes according to our definition.)

Since b is not prime, there are two possibilities: either $b = 1$ or b has a factor k which is a natural number such that $k \neq 1$ and $k \neq b$.

But the fist possibility ($b = 1$) cannot arise, because $b \geq 2$.

Hence the second possibility occurs. That is, we can pick a natural number k such that k divides b, $k \neq 1$, and $k \neq b$.

Since $k|b$, we can write

$$b = jk\,, \quad j \in \mathbb{Z}\,.$$

And then j has to be a natural number. (Reason: we know that $k \in \mathbb{N}$, so $k > 0$. If j was ≤ 0, it would follow that $kj \leq 0$. But $kj = b$ and $b > 0$.)

Then $j \neq 1$ and $j \neq b$. (Reason: j cannot be 1 because if $j = 1$ then it would follow from $b = jk$ that $k = b$, and we know that $k \neq b$. And j cannot be b because if $j = b$ then it would folows from $b = jk$ that $k = 1$, and we know that $k \neq 1$.)

Then $j < b$ and $k < b$. (Reason: $k \geq 1$, because $k \in \mathbb{N}$; so $k > 1$, because $k \neq 1$; so $k \geq 2$; and then if j was $\geq b$ it would follow that $jk \geq 2j > j > b$, but $jk = b$. The proof that $k < b$ is exactly the same.)

Hence $j \notin B$ (because b is the smallest member of B, and $j < b$). And $j \geq 2$ (because $j > 1$). This means that j is a product of primes (because if j wasn't a product of primes it would be in B).

Similarly, k is a product of primes. So we can write $j = \prod_{i=1}^{m} p_i$ and $k = \prod_{\ell=1}^{\mu} q_\ell$, where $m \in \mathbb{N}$, $\mu \in \mathbb{N}$, and the p_i and the q_ℓ are primes. But then

$$b = \Big(\prod_{i=1}^{m} p_i\Big) \times \Big(\prod_{\ell=1}^{\mu} q_\ell\Big)\,,$$

so $\boxed{b \text{ is a product of primes}}$.

But we know that $\boxed{b \text{ is not a product of primes}}$. So we got two contradictory statements.

This contradiction was derived by assuming that $B \neq \emptyset$. So $B = \emptyset$, and this proves that every natural number n such that $n \geq 2$ is a product of primes, which is our desired conclusion. **Q.E.D.**