MATHEMATICS 300 — SPRING 2006

Introduction to Mathematical Reasoning

H. J. Sussmann—April 17, 2006

REVIEW QUESTIONS

Remember that when you are asked to do something, the answer could be "It cannot be done", in which case you must prove that it cannot be done. For as example of how this works, look at Review Question No. 2.

Review Question 1. Prove that $(\exists m \in \mathbb{Z})(\exists n \in \mathbb{Z})m^2 - n^2 = 32$.

ANSWER: $6^2 - 2^2 = 36 - 4 = 32$, so $(\exists m \in \mathbb{Z})(\exists n \in \mathbb{Z})m^2 - n^2 = 32$ by the Witness Rule (Rule $\exists_{get}$).

Review Question 2. Prove that $(\exists m \in \mathbb{Z})(\exists n \in \mathbb{Z})m^2 - n^2 = 30$.

ANSWER: This statement cannot be proved because it is not true. *Proof that it is not true:* Suppose the statement was true. Then we may pick integers m, n such that $m^2 - n^2 = 30$. Then $(m - n)(m + n) = 30$. Let $a = m - n$, $b = m + n$. Then $ab = 30$, and $b = a + 2n$. Now, a is either even or odd. Suppose a is even. Then we may pick $k \in \mathbb{Z}$ such that $a = 2k$. Then $b = a + 2n = 2k + 2n = 2(k + n)$. So $30 = ab = 4k(k + n)$, so that 30 is divisible by 4. Now consider the case when a is odd. Then b is odd as well, since $b = a + 2n$. Therefore 30 is odd, since $30 = ab$. So we have shown that 30 is either divisible by 4 or odd, But 30 is neither divisible by 4 nor odd, Hence we have reached a contradiction.

Review Question 3. Define "equivalence" (of propositional forms). (This is done in the book, p. 5.)

Review Question 4. Define "tautology." (This is done in the book, p. 6.)

Review Question 5. Define "contradiction." (This is done in the book, p. 7.)

Review Question 6. Define "truth set" (of a one-variable predicate). (This is done in the book, p. 20.)

Review Question 7. Define "equivalence" (of one-variable predicates). (This is done in the book, p. 20.)

Review Question 8. Define the predicates "divides" and "is divisible by" in terms of a sentence that, in addition to the predicate being defined, uses only the basic vocabulary of arithmetic.

ANSWER: Let a, b be integers. We say that a **divides** b, or that b **is divisible by** a, if there exists an integer k such that $b = ak$.

IN SYMBOLIC NOTATION: we write "$a|b$" for "a divides b" , or "b is divisible by a", and then "$a|b$" is defined by: $(\forall a \in \mathbb{Z})(\forall b \in \mathbb{Z})(a|b \Leftrightarrow (\exists k \in \mathbb{Z})b = ak)$.

Review Question 9. Define the predicate "is prime" in terms of a sentence that, in addition to the predicate being defined, uses only the basic vocabulary of arithmetic.

ANSWER: Let a be an integer. We say that a **is prime** (or a **is a prime number**) if $a > 1$ and there do not exist integers k, ℓ such that $1 < k$, $k < a$, and $a = k\ell$.

IN SYMBOLIC NOTATION:
$(\forall a \in \mathbb{Z})(a$ **is prime** $\Leftrightarrow (a > 1 \wedge \sim (\exists k \in \mathbb{Z})(\exists \ell \in \mathbb{Z})((1 < k \wedge k < a) \wedge a = k\ell)))$.

Review Question 10. Define the predicate "is prime" in terms of a sentence that, in addition to the predicate being defined, uses only the basic vocabulary of arithmetic and the predicate "divides".

ANSWER: Let a be an integer. We say that a **is prime** (or a **is a prime number**) if $a > 1$ and there does not exist an integer k such that $1 < k$, $k < a$, and k divides a.

IN SYMBOLIC NOTATION:
$(\forall a \in \mathbb{Z})(a$ **is prime** $\Leftrightarrow (a > 1 \wedge \sim (\exists k \in \mathbb{Z})((1 < k \wedge k < a) \wedge k|a)))$.

Review Question 11. Define the predicate "is even" in terms of a sentence that, in addition to the predicate being defined, uses only the basic vocabulary of arithmetic.

ANSWER: Let a be an integer. We say that a **is even** (or a **is an even number**) if there exists an integer k such that $a = k + k$.

IN SYMBOLIC NOTATION: $(\forall a \in \mathbb{Z})(a$ **is even** $\Leftrightarrow (\exists k \in \mathbb{Z})a = k + k)$.

Review Question 12. Define the predicate "is odd" in terms of a sentence that, in addition to the predicate being defined, uses only the basic vocabulary of arithmetic.

ANSWER: Let a be an integer. We say that a **is odd** (or a **is an odd number**) if there exists an integer k such that $a = (k + k) + 1$.

IN SYMBOLIC NOTATION: $(\forall a \in \mathbb{Z})(a$ **is odd** $\Leftrightarrow (\exists k \in \mathbb{Z})a = (k + k) + 1)$.

Review Question 13. Define the predicate "is even" in terms of a sentence that, in addition to the predicate being defined, uses only the basic vocabulary of arithmetic and the number 2.

ANSWER: Let a be an integer. We say that a **is even** (or a **is an even number**) if there exists an integer k such that $a = 2k$.

IN SYMBOLIC NOTATION: $(\forall a \in \mathbb{Z})(a \textbf{ is even} \Leftrightarrow (\exists k \in \mathbb{Z})a = 2k)$.

Review Question 14. Define the predicate "is odd" in terms of a sentence that, in addition to the predicate being defined, uses only the basic vocabulary of arithmetic and the number 2.

ANSWER: Let a be an integer. We say that a **is odd** (or a **is an odd number**) if there exists an integer k such that $a = 2k + 1$.

IN SYMBOLIC NOTATION: $(\forall a \in \mathbb{Z})(a \textbf{ is odd} \Leftrightarrow (\exists k \in \mathbb{Z})a = 2k + 1)$.

Review Question 15. Define the predicate "is even" in terms of a sentence that, in addition to the predicate being defined, uses only the basic vocabulary of arithmetic, the number 2, and the predicate "divides", or "is divisible by".

ANSWER: Let a be an integer. We say that a **is even** (or a **is an even number**) if a is divisible by 2.

IN SYMBOLIC NOTATION: $(\forall a \in \mathbb{Z})(a \textbf{ is even} \Leftrightarrow 2|a)$.

Review Question 16. Define the predicate "is rational" in terms of a sentence that, in addition to the predicate being defined, uses only the basic vocabulary of arithmetic.

ANSWER: Let a be a real number. We say that a **is rational** (or a **is a rational number**) if there exist integers m, n such that n is not equal to zero and $a = \frac{m}{n}$.

IN SYMBOLIC NOTATION:
$(\forall a \in \mathbb{Z})(a \textbf{ is rational} \Leftrightarrow (\exists m \in \mathbb{Z})(\exists n \in \mathbb{Z})((\sim n = 0) \wedge a = \frac{m}{n}))$.

Review Question 17. Define the predicate "is irrational" in terms of a sentence that, in addition to the predicate being defined, uses only the basic vocabulary of arithmetic.

ANSWER: Let a be a real number. We say that a **is irrational** (or a **is an irrational number**) if there do not exist integers m, n such that n is different from zero and $a = \frac{m}{n}$.

IN SYMBOLIC NOTATION:
$(\forall a \in \mathbb{Z})(a \textbf{ is irrational} \Leftrightarrow (\sim (\exists m \in \mathbb{Z})(\exists n \in \mathbb{Z})((\sim n = 0) \wedge a = \frac{m}{n})))$.

Review Question 18. Define the predicate "is irrational" in terms of a sentence that, in addition to the predicate being defined, uses only the basic vocabulary of arithmetic and the predicate "is rational".

ANSWER: Let a be a real number. We say that a **is irrational** (or a **is an irrational number**) if a is not rational.

IN SYMBOLIC NOTATION: $(\forall a \in \mathbb{Z})(a$ **is irrational** $\Leftrightarrow (\sim a$ is rational$))$.

Review Question 19. Define the predicate"is the greatest common divisor of" in terms of a sentence that, in addition to the predicate being defined, uses only the basic vocabulary of arithmetic and the predicate "divides", or "is divisible by".

ANSWER: Let a, b, c be integers. We say that c **is the greatest common divisor of** a **and** b if (i) c divides a, (ii) c divides b, and (iii) if h is any integer such that h divides a and h divides b, it follows that $h \leq c$.

IN SYMBOLIC NOTATION: if we write "GCD" for "greatest common divisor", then

$(\forall a \in \mathbb{Z})(\forall b \in \mathbb{Z})(\forall c \in \mathbb{Z})(c$ **is the GCD of** a **and** $b \Leftrightarrow$
$((c|a \wedge c|b) \wedge (\forall h \in \mathbb{Z})((h|a \wedge h|b) \Rightarrow h \leq c)))$.

Review Question 20. Define the predicate"is the greatest common divisor of" in terms of a sentence that, in addition to the predicate being defined, uses only the basic vocabulary of arithmetic.

ANSWER: Let a, b, c be integers. We say that c **is the greatest common divisor of** a **and** b if (i) there exist integers k, ℓ such that $a = kc$ and $b = \ell c$, (ii) if h is any integer such that there exist integers κ, λ for which $a = \kappa h$ and $b = \lambda h$, it follows that $h \leq c$.

IN SYMBOLIC NOTATION: if we write "GCD" for "greatest common divisor", then

$(\forall a \in \mathbb{Z})(\forall b \in \mathbb{Z})(\forall c \in \mathbb{Z})(c$ **is the GCD of** a **and** $b \Leftrightarrow$
$((\exists k \in \mathbb{Z})(\exists \ell \in \mathbb{Z})(a = kc \wedge b = \ell c) \wedge$
$(\forall h \in \mathbb{Z})((\exists \kappa \in \mathbb{Z})(\exists \lambda \in \mathbb{Z})(a = \kappa h \wedge b = \lambda h) \Rightarrow h \leq c)))$.

Review Question 21. Define the predicate"is the least common multiple of" in terms of a sentence that, in addition to the predicate being defined, uses only the basic vocabulary of arithmetic and the predicate "divides", or "is divisible by".

ANSWER: Let a, b, c be integers. We say that c **is the least common multiple of** a **and** b if (i) c is a natural number, (ii) a divides c, (iii) b divides c, and (iv) if h is any natural number such that a divides h and b divides h, it follows that $c \leq h$.

IN SYMBOLIC NOTATION: if we write "LCM" for "least common multiple", then

$(\forall a \in \mathbb{Z})(\forall b \in \mathbb{Z})(\forall c \in \mathbb{Z})(c$ **is the LCM of** a **and** $b \Leftrightarrow$
$((c \in \mathbb{N} \wedge (c|a \wedge c|b)) \wedge (\forall h \in \mathbb{N})((a|h \wedge b|h) \Rightarrow c \leq h)))$.

Review Question 22. Define "coprime".

ANSWER: Let a, b be integers. We say that a and b are **coprime** if their greatest common divisor is 1.

Review Question 23. Define "absolute value" (of a real number). (The definition is given in the book, page 36.)

Review Question 24. Define "empty set". (This is done in the book, p. 71.)

Review Question 25. Define "subset". (This is done in the book, p. 71.)

Review Question 26. Define "power set". (This is done in the book, p. 74.)

Review Question 27. Define "union" (of two sets). (This is done in the book, p. 78.)

Review Question 28. Define "intersection" (of two sets). (This is done in the book, p. 78.)

Review Question 29. Define "difference" (of two sets). (This is done in the book, p. 78.)

Review Question 30. Define what it means for two sets to be "disjoint". (This is done in the book, p. 79.)

Review Question 31. Define "complement". (This is done in the book, p. 81.)

Review Question 32. Give a recursive (that is, inductive) definition of the "factorial" $n!$ of a natural number n. (This is done in the book, p. 98.)

Review Question 33. Give a recursive (that is, inductive) definition of the "n-th power" a^n, where a is a real number and n is a natural number.

ANSWER: Let a be a real number and let n be a natural number. Then (i) if $n = 1$ then $a^n = a$, (ii) if $n > 1$ then $a^n = a^{n-1} \cdot a$.

IN SYMBOLIC NOTATION:

$(\forall a \in \mathbb{Z})(\forall n \in \mathbb{Z})((n = 1 \Rightarrow a^n = a) \wedge n > 1 \Rightarrow a^n = a^{n-1} \cdot a)$.

Review Question 34. Define "Cartesian product". (This is done in the book, p. 132.)

Review Question 35. Define "relation". (This is done in the book, p. 133.)

Review Question 36. Define "relation from a set A to a set B". (This is done in the book, p. 133.)

Review Question 37. Define "domain" of a relation. (See the book, p. 135.)

Review Question 38. Define "range" of a relation. (See the book, p. 135.)

Review Question 39. Define "inverse" of a relation. (This is done in the book, p. 138.)

Review Question 40. Define "composite" of two relations. (This is done in the book, p. 139.)

Review Question 41. Define "function" from a set A to a set B; you are allowed to use the notions of relation and domain. (This is done in the book, p. 179.)

Review Question 42. Define "function" from a set A to a set B; you are ***not*** allowed to use the notions of relation, domain, or Cartesian product.

ANSWER: Let A, B be sets. A ***function*** from A to B is a set F such that (i) every member of F is an ordered pair (x, y) such that $x \in A$ and $y \in B$, (ii) for every member a of A there exists a $b \in B$ such that $(a, b) \in F$, (iii) whenever $(x, y) \in F$ and $(x, z) \in F$, it follows that $y = z$.

IN SYMBOLIC NOTATION:

$(\forall A)(\forall B)(\forall f)(f$ is a ***function*** $\Leftrightarrow$
$(f$ is a set$\wedge(\forall u)(u \in f \Rightarrow (\exists x)(\exists y)(u = (x, y) \wedge (x \in A \wedge y \in B)))) \wedge$
$(((\forall x)(x \in A \Rightarrow (\exists y)((x, y) \in f \wedge y \in B)) \wedge$
$(\forall x)(\forall y)(\forall z)(((x, y) \in f \wedge (x, z) \in f) \Rightarrow y = z))))$

Review Question 43. Prove that the sum of two even integers is even.

Review Question 44. Prove that the sum of two odd integers is even.

Review Question 45. Prove that the sum of an even integer and an odd integer is odd.

Review Question 46. Prove that if an integer x is odd then $x + 1$ is even. (This is done in the book, p. 32.)

Review Question 47. Prove that if a, b, c are integers, a divides b, and b divides c, then a divides c. (This is done in the book, p. 33.)

Review Question 48. Prove that if a, b, are natural numbers, a divides b, and b divides a, then $a = b$.

Review Question 49. Prove that if a, b, are integers, a divides b, and b divides a, then $a = b$.

Review Question 50. Prove that if a, b, c are integers, a divides b, and a divides c, then a divides $b - c$. (This is done in the book, p. 34.)

Review Question 51. Prove that if a and b are positive integers, and a divides b, then $a \leq b$.

Review Question 52. Prove that if a and b are integers, and a divides b, then $a \leq b$.

Review Question 53. Prove that if x is an odd integer, then $x^2 - 1$ is divisible by 8.

Review Question 54. Prove that if x is an integer, then $x^2 - 1$ is divisible by 8.

Review Question 55. Prove that $(\exists m \in \mathbb{Z})(\exists n \in \mathbb{Z})m^2 - n^2 = 50$.

Review Question 56. Prove that $(\exists m \in \mathbb{Z})(\exists n \in \mathbb{Z})m^2 - n^2 = 51$.

Review Question 57. Prove that $(\exists m \in \mathbb{Z})(\exists n \in \mathbb{Z})m^2 - n^2 = 52$.

Review Question 58. Prove that if n is an odd integer, then either $n = 4j + 1$ for some integer j, or $n = 4i - 1$ for some integer i. (This is done in the book, p. 35.)

Review Question 59. Prove that the sum of two rational numbers is rational.

Review Question 60. Prove that the sum of two irrational numbers is irrrational.

Review Question 61. Prove that the sum of a rational number and an irrational numbers is rational.

Review Question 62. Prove that the sum of a rational number and an irrational numbers is irrational.

Review Question 63. Prove that if a and b are positive real numbers, and $a < b$, then $b^2 - a^2 > 0$. (This is done in the book, p. 34.)

Review Question 64. Prove that if a and b are real numbers, and $a < b$, then $b^2 - a^2 > 0$.

Review Question 65. Prove that if x is a real number, then $-|x| \leq x$ and $x \leq |x|$. (This is done in the book, p. 36.)

Review Question 66. Prove that if x and y are real numbers, then $|x+y| \leq |x| + |y|$.

Review Question 67. Prove that if x and y are positive real numbers, then $\sqrt{x+y} \leq \sqrt{x} + \sqrt{y}$.

PROOF: Let $a = \sqrt{x}$, $b = \sqrt{y}$, $c = \sqrt{x+y}$. We want to prove that $c \leq a + b$. Assume that $c > a + b$. Then $c^2 > (a+b)^2$. But $c^2 = x + y$, and $(a+b)^2 = a^2 + 2ab + b^2 = x + y + 2ab = c^2 + 2ab$. Hence $c^2 < (a+b)^2$, contradicting the fact that $c^2 > (a+b)^2$.

Review Question 68. Prove that if x and y are positive real numbers, then $\sqrt{xy} \leq \frac{x+y}{2}$.

PROOF: $(\sqrt{x} - \sqrt{y})^2 = x + y - 2\sqrt{xy}$, and on the other hand $(\sqrt{x} - \sqrt{y})^2 \geq 0$. Hence $x + y - 2\sqrt{xy} \geq 0$. Therefore $x + y \geq 2\sqrt{xy}$, so $\frac{x+y}{2} \geq \sqrt{xy}$, and then $\sqrt{xy} \leq \frac{x+y}{2}$.

Review Question 69. Prove that if x is a positive real number, then $x + \frac{1}{x} \geq 2$.

FIRST PROOF (assuming you are allowed to use the result of the previous problem): Let $x \in \mathbb{R}$ be such that $x > 0$. Let $y = \frac{1}{x}$. Then $\sqrt{xy} \leq \frac{x+y}{2}$ (by the previous problem), so $2\sqrt{xy} \leq x + y$. But $xy = 1$, so $2 \leq x + y$, then $2 \geq x + \frac{1}{x} \geq 2$, so $x + \frac{1}{x} \geq 2$.

SECOND PROOF (assuming you are not allowed to use the result of the previous problem):

$$\begin{aligned} \left(x + \frac{1}{x}\right)^2 &= x^2 + \frac{1}{x^2} + 2x \cdot \frac{1}{x} \\ &= x^2 + \frac{1}{x^2} + 2 \end{aligned}$$

$$\begin{aligned} &= x^2 + \frac{1}{x^2} - 2 + 4 \\ &= x^2 + \frac{1}{x^2} - 2x \cdot \frac{1}{x} + 4 \\ &= \left(x - \frac{1}{x}\right)^2 + 4 \\ &\geq 4\,. \end{aligned}$$

Hence $x + \frac{1}{x} \geq 2$.

Review Question 70. Explain what is wrong with the following proof. CLAIM: If x is a real number and $x \neq 0$, then $x + \frac{1}{x} \geq 2$. PROOF: Squaring both sides of $x + \frac{1}{x} \geq 2$, we get $\left(x + \frac{1}{x}\right)^2 \geq 4$, that is, $x^2 + \frac{1}{x^2} + 2x \cdot \frac{1}{x} \geq 4$. But this is equivalent to $x^2 + \frac{1}{x^2} + 2 \geq 4$ (because $x \cdot \frac{1}{x} = 1$). Hence $x^2 + \frac{1}{x^2} \geq 2$, i.e., $x^2 + \frac{1}{x^2} - 2 \geq 0$, that is, $x^2 + \frac{1}{x^2} - 2x \cdot \frac{1}{x} \geq 0$, so $\left(x - \frac{1}{x}\right)^2 \geq 0$, which is true. Therefore $x + \frac{1}{x} \geq 2$.

Review Question 71. Prove that every natural number greater than 1 has a prime factor. You may use well-ordering or any form of induction you wish, but I recommend you use well-ordering. (This is done in the book, p. 114.)

Review Question 72. Prove that if p is prime and a, b are positive integers, then p divides the product ab if and only if p divides a or p divides b. (This is done in the book, 42, using the "fundamental theorem of arihtmetic" (FTA). I will acept this proof, even though we did not do the FTA in class. But I am also giving you below a proof that does not use the FTA.)

PROOF (without using the FTA): If p divides a, then we may pick an integer k such that $a = kp$. Then $ab = kbp$, so p divides ab. If p divides b, then we may pick an integer ℓ such that $b = \ell p$. Then $ab = \ell ap$, so p divides ab as well. Therefore, if p divides a or p divides b, then p divides ab. *(Notice that this is a proof by cases.)*

Now assume that p divides ab. We want to prove that p divides a or p divides b. If p divides a, then p divides a or p divides b, so we are done. Next consider the case when p does not divide a. We will prove that p divides b. Since p does not divide a and p is prime, the greatest common divisor of p and a is 1. This implies that we may pick integers m, n such that $ma + np = 1$. Multiplying both sides by b, we get $mab + npb = b$. Since p divides ab, we may pick an integer k such that $ab = kp$. Then $b = mab + npb = mkp + nbp = (mk + nb)p$, so p divides b. **END**

Review Question 73. Prove that the set of prime numbers is infinite. More precisely, prove that for every natural numb er N there exists a prime number p such that $p > N$. (This was done in class, and it's done in the book, p. 42.)

PROOF: Let N be a natural number. Let $M = N!$, and let $Q = M + 1$. Then $M+1$ is a natural number and $M+1 > 1$, so $M+1$ has a prime factor p. We will show that $p > N$. Suppose that $p \leq N$. Then $p|N!$. (*Reason: This is intuitively clear, because* $N!$ *is the product of all the natural numbers from* 1 *to* N*, and then* p *is one of these numbers, since* $p \leq N$*. Hence* $N!$ *is a product of natural numbers one of which is* p*, so* $p|N!$*. I will accept this argument. But here is a more rigorous proof: we fix* p*, and show using well-ordering that* $(\forall n \in \mathbb{N})(n \geq p \Rightarrow p|n!)$*. Call a natural number* n *"bad" if it is not true that* $n \geq p \Rightarrow p|n!$*. We want to show that there are no bad numbers. Assume there is one. Then by the well-ordering principle there is a smallest one. Call it* b*, so* b *is the smallest bad number. We observe that* b *cannot be* $< p$*, because if* $b < p$ *then the implication "*$b \geq p \Rightarrow p|b!$*" is true, so* b *is not bad, and this contradicts the fact that* b *is bad. So* $b \geq p$*. Then* $b! = (b-1)! \cdot b$*, by the inductive definition of the factorial. If* $b = p$ *then* $b! = (b-1)! \cdot p$*, so* $p|b!$*. If* $b > p$*, then* $b - 1$ *is a natural number which is not bad, since* b *is the smallest bad number. So the implication "*$b - 1 \geq p \Rightarrow p|(b-1)!$*" is true. Since* $b - 1 \geq p$*, it follows from Rule* $\Rightarrow_{use}$ *that* $p|(b-1)!$*. But then* $p|(b-1)! \cdot b$*, so* $p|b!$*. We have shown that* $p|b!$ *in both cases, when* $b = p$ *and* $b > p$*. So the implication "*$b \geq p \Rightarrow p|b!$*" is true in both cases. This shows that* b *is not bad, and we got a contradiction.*) So $p|M$. Since $p|M + 1$, it follows that $p|1$, which is impossible. So $p > N$. **END**.

Review Question 74. Explain what is wrong with the following "proof": Claim: $-2 = 2$. Proof: Assume that $-2 = 2$. Squaring both sides, we get $4 = 4$, which is true. So our assumption must be true. (This is discussed in the book, p. 58.)

Review Question 75. Prove the *division theorem*: If a, b are integers and $b > 0$ then there exist integers q, r such that $a = bq + r$ and $0 \leq r < b$. (This is done in the notes, p. 101. It is also done in the book, p. 115, under the aditional assumption that $b \leq a$.)

Review Question 76. Prove that if a and b are integers, and a greatest common divisor of a and b exists, then it is unique.

PROOF: We show that, if d and $\tilde{d}$ are two greatest commoon divisors of a and b, then $d = \tilde{d}$. Since $\tilde{d}$ is a GCD of a and b, $\tilde{d}$ is a common divisor of a

and b, i.e., $\tilde{d}$ divides a and b. Since d is a GCD of a and b, d is greater than or equal to any common divisor of a and b, so in particular $d \geq \tilde{d}$. A similar argument shows that $\tilde{d} \geq d$. Hence $\tilde{d} = d$. **END**.

Review Question 77. Prove that if a and b are integers, and at least one of them is not zero, then the greatest common divisor d of a and b is an integer linear combination of a and b, that is, there exist integers x, y such that $xa + yb = d$. (This was done in class, and it is also done in the book, p. 115, under the aditional assumption that $a \in \mathbb{N}$ and $b \in \mathbb{N}$.)

Review Question 78. Prove that if r is a rational number then there exist integers m, n such that $n \neq 0$, $r = \frac{m}{n}$, and m, n are coprime.

PROOF: Since r is rational, there exist integers μ, ν such that $\nu \neq 0$ and $r = \frac{\mu}{\nu}$. Let d be the greatest common divisor of μ and ν. Then $d|\mu$, so we may pick $m \in \mathbb{Z}$ such that $\mu = md$. Also, $d|\nu$, so we may pick $n \in \mathbb{Z}$ such that $\nu = nd$. Then $n \neq 0$ (because $\nu \neq 0$ and $\nu = nd$) and $r = \frac{\mu}{\nu} = \frac{md}{nd} = \frac{m}{n}$. Let us show that m and n are coprime. Let g be the greatest common divisor of m and n. Then we may pick $k \in \mathbb{Z}$ amd $\ell \in \mathbb{Z}$ such that $m = kg$ and $n = \ell g$. Then $\mu = kgd$ and $\nu = \ell gd$. So $gd|\mu$ and $gd|\nu$. Therefore $gd \leq d$, since d is the greatest common divisor of μ and ν. Hence $g = 1$, because if $g > 1$ then $gd > d$. So m and n are indeed coprime. **END**.

Review Question 79. Prove that if p is a prime number then $\sqrt{p}$ is irrational.

PROOF: Let $r = \sqrt{p}$. Suppose r is rational. Pick integers m, n such that $r = \frac{m}{n}$ and m and n are coprime. Then $p = r^2 = \frac{m^2}{n^2}$, so $pn^2 = m^2$. It follows that $p|m^2$. Since p is prime and p divides the product $m \cdot m$, it follows that p divides one of the factors, so $p|m$. Pick $k \in \mathbb{Z}$ such that $m = kp$. Then $m^2 = k^2p^2$, so $pn^2 = k^2p^2$, and then $n^2 = k^2p$. Hence $p|n^2$. Since p is prime and p divides the product $n \cdot n$, it follows that p divides one of the factors, so $p|n$. We have thus shown that $p|m$ and $p|n$. So p is a common divisor of m and n. Since m and n are coprime, their greatest common divisor is 1. So $p \leq 1$. But p is prime, so $p > 1$. We have shown that $p \leq 1$ and $p > 1$. This is a contradiction, showing that r is irrational.

Review Question 80. Prove that $\sqrt{15}$ is irrational.

PROOF: Let $r = \sqrt{15}$. Suppose r is rational. Pick integers m, n such that $r = \frac{m}{n}$ and m and n are coprime. Then $15 = r^2 = \frac{m^2}{n^2}$, so $15\,n^2 = m^2$. It follows that $3|m^2$. Since 3 is prime and 3 divides the product $m \cdot m$, it follows

that 3 divides one of the factors, so $3|m$. Pick $k \in \mathbb{Z}$ such that $m = 3k$. Then $m^2 = 9k^2$, so $15n^2 = 9k^2$, and then $5n^2 = 3k^2$. Hence $3|5n^2$. Since 3 is prime and 3 divides the product $5 \cdot n \cdot n$, it follows that 3 divides one of the factors, so $3|5$ or $3|n$. Since $\sim 3|5$, we can conclude that $3|n$. We have thus shown that $3|m$ and $3|n$. So 3 is a common divisor of m and n. Since m and n are coprime, their greatest common divisor is 1. So $3 \leq 1$. But $3 > 1$. So $3 \leq 1 \wedge 3 > 1$. This is a contradiction, showing that r is irrational. **END**.

Review Question 81. Is the following proof correct? Explain?

CLAIM: $\sqrt{15}$ is irrational.

PROOF: $\sqrt{15} = \sqrt{3} \cdot \sqrt{5}$. Furthermore, $\sqrt{3}$ is irrational, and $\sqrt{5}$ is irrational. So the product $\sqrt{15}$ is irrational as well. **END**.

Review Question 82. Prove that $\sqrt{18}$ is irrational.

Review Question 83. Prove that every integer is even or odd. (In symbolic notation: $(\forall n \in \mathbb{Z})(n$ is even $\vee\, n$ is odd. Or, if you prefer, you could also say $(\forall n \in \mathbb{N})((\exists k \in \mathbb{Z})(n = 2k) \vee (\exists k \in \mathbb{Z})(n = 2k + 1))$.) (NOTE: This is done in the notes, p. 80, for natural numbers. The proof for general integers is only a little bit longer, because most of the work is already there in the proof for natural numbers.

PROOF: First, we are going to prove that $(\forall n \in \mathbb{N})(n$ is even $\vee\, n$ is odd). We will prove this by contradiction. Call a natural number n "bad" if it is not true that n is even $\vee\, n$ is odd, i.e., if n is neither even nor odd. Call n "good" if it is not bad. We want to prove that there are no bad natural numbers. So we assume that the desired conclusion is not true. This means that there exists a bad natural number. If we apply Axiom NZ12 to the predicate "u is neither even nor odd" , since there exists a $u \in \mathbb{N}$ for which the predicate is true, Axiom NZ12 tells us that there exists a smallest bad u. Pick a smallest bad natural number, and call it a. Then $a \in \mathbb{N}$, a is bad, and there is no $b \in \mathbb{N}$, such that b is bad and $b < a$. Can a be 1? No, because 1 is odd, so 1 is good. So $a > 1$. Then $a - 1 \in \mathbb{N}$. Could $a - 1$ be even? No, because if $a - 1$ was even, then a would be odd so a would be good. Could $a - 1$ be odd? No, because if $a - 1$ was odd, then a would be even, so a would be good. So $a - 1 \in \mathbb{N}$ and $a - 1$ is neither even nor odd So $a - 1$ is bad, and we have reached a contradiction because $a - 1$ is bad, and a is the smallest bad number. This concludes the proof that $(\forall n \in \mathbb{N})(n$ is even $\vee\, n$ is odd). We will prove this by

We now prove that $(\forall n \in \mathbb{Z})(n \text{ is even} \vee n \text{ is odd})$. Let $n \in \mathbb{Z}$ be arbitrary. Then $n > 0$ or $n = 0$ or $n < 0$. If $n > 0$, then $n \in \mathbb{N}$, so we already know that n is even $\vee\, n$ is odd. If $n = 0$ then n is even (because $n = 2 \cdot 0$) so n is even $\vee\, n$ is odd. If $n < 0$ then $-n > 0$, so $-n$ is even $\vee -n$ is odd. If $-n$ is even then n is even as well. If $-n$ is odd then n is odd. In both cases, n is even $\vee\, n$ is odd. **END.**i

Review Question 84. Prove that $(\forall x \in \mathbb{R})x \cdot 0 = 0$

PROOF: Let $a \in \mathbb{R}$ be arbitrary. Then $a \cdot 0 = a \cdot 0$ because $(\forall x)x = x$. Also, $0 + 0 = 0$, because of Axiom ZO1. So $a \cdot 0 = a \cdot (0 + 0)$. On the other hand, $a \cdot (0 + 0) = a \cdot 0 + a \cdot 0$, by Axiom DIS. Hence $a \cdot 0 = a \cdot 0 + a \cdot 0$.

Let $\alpha = a \cdot 0$. Then $\alpha = \alpha + \alpha$. On the other hand, $\alpha = \alpha + 0$ by ZO1, and $\alpha - \alpha = 0 \Leftrightarrow \alpha = \alpha + 0$ by Sub2. Hence $\alpha - \alpha = 0$. But then

$$0 = \alpha - \alpha = (\alpha + \alpha) - \alpha = \alpha + (\alpha - \alpha) = \alpha + 0 = \alpha\,,$$

so $a \cdot 0 = 0$. Since a was arbitrary, we have shown that $(\forall x \in \mathbb{R})x \cdot 0 = 0$. **END**

Review Question 85. Prove that an integer cannot be both even and odd. (In symbolic notation: $(\forall n \in \mathbb{Z})(\sim (n \text{ is even} \wedge n \text{ is odd}))$.)

PROOF: Let n be arbitrary. Suppose n is even and n is odd. Then we may pick integers k, ℓ such that $n = 2k$ and $n = 2\ell + 1$. It follows that $2k = 2\ell + 1$, so $1 = 2(k - \ell)$. So $\frac{1}{2} = k - \ell$. Therefore $\frac{1}{2}$ is an integer.

We now prove that $\frac{1}{2}$ is not an integer. For this purpose, we show that $0 < \frac{1}{2}$ and $\frac{1}{2} < 1$. If it wasn't true that $0 < \frac{1}{2}$, then we would have $0 \geq \frac{1}{2}$ (Axiom Or4), so $\frac{1}{2} \leq 0$ (Axiom Or3), so either $\frac{1}{2} < 0$ or $\frac{1}{2} = 0$ (Axiom Or2). If $\frac{1}{2} < 0$ then we can multiply both sides by 2 and conclude from Axiom Or8 that $1 < 0$. (Reason: first, $2 > 0$ because NZ4 tells us that $1 \in \mathbb{N}$, NZ8 then implies that $1 + 1 \in \mathbb{N}$, so $2 \in \mathbb{N}$ because $2 = 1 + 1$. And then NZ10 tells us that $2 > 0$. So the application of Or8 is justified. Second, $2 \cdot \frac{1}{2} = 1$ by Axiom Div2. Third, $2 \cdot 0 = 0$ because $\forall x \in \mathbb{R})x \cdot 0 = 0$.) But Axiom NZ4 tells us that $1 \in \mathbb{N}$, and $NZ10$ then implies that $1 > 0$. So $1 > 0 \wedge 1 < 0$, contradicting Axiom Or5. Hence the possibility that $\frac{1}{2} < 0$ is excluded, because it leads to a contradiction. If $\frac{1}{2} = 0$ then we can multiply both sides by 2 and conclude that $1 = 0$. Since $1 \in \mathbb{N}$, it follows that $0 \in \mathbb{N}$. But then NZ10 tells us that $0 > 0$, and this contradicts Or5 (because $0 \geq 0$, since $0 = 0$). So the possibility that $\frac{1}{2} = 0$ is also excluded, because it leads to a contradiction. Hence $\frac{1}{2} > 0$.

Since $\frac{1}{2} > 0$, we can add $\frac{1}{2}$ to both sides and conclude that $\frac{1}{2} + \frac{1}{2} > \frac{1}{2}$, i.e., that $1 > \frac{1}{2}$. (Why is $\frac{1}{2} + \frac{1}{2} = 1$? Because

$$\frac{1}{2} + \frac{1}{2} = \frac{1}{2} \times 1 + \frac{1}{2} \times 1 = \frac{1}{2} \times (1 + 1) = \frac{1}{2} \times 2\,,$$

and we have already shown that $\frac{1}{2} \times 2 = 1$.)

So $0 < \frac{1}{2}$ and $\frac{1}{2} < 1$. But Axiom NZ11 tells us that there are no integers x such that $0 < x$ and $x < 1$. Hence $\frac{1}{2}$ is not an integer.

So we have shown that (a) if some integer was both even and odd then it would follow that $\frac{1}{2}$ is an integer, and (b) $\frac{1}{2}$ is not an integer. Our conclusion then follows. **END.**

Review Question 86. Prove that if A is a set then the empty set is a subset of A.

Review Question 87. Prove that if A is a set then $A \subseteq A$.

Review Question 88. Prove that if A, B are sets then $A \subseteq B \Leftrightarrow A = A \cap B$.

Review Question 89. Prove that if A, B are sets then $A \subseteq B \Leftrightarrow B = A \cup B$.

Review Question 90. Prove that if A, B are sets then $(A \cup B) \cap A = A$.

Review Question 91. Prove that if A, B, C are sets, $A \subseteq B$, and $B \subseteq C$, then $A \subseteq C$.

Review Question 92. Prove that if A, B, C, D are sets, $A \cup B \subseteq C \cup D$, $A \cap B = \emptyset$, and $C \subseteq A$, then $B \subseteq D$.

Review Question 93. Prove that if A, B are sets then $\mathcal{P}(A \cap B) = \mathcal{P}(A) \cap \mathcal{P}(B)$.

Review Question 94. Prove that if A, B are sets then $\mathcal{P}(A \cup B) = \mathcal{P}(A) \cup \mathcal{P}(B)$.

Review Question 95. Explain what is wrong with the following "proof." In particular, indicate which is the first step in the proof that is either false or meaningless, and explain why. Is the claim true? CLAIM: If A, B are sets such that $A \times B = B \times A$ then $A = B$. PROOF: Suppose $A \times B = B \times A$. Since $A \times B = \{(a, b) : a \in A, b \in B\}$, and $B \times A = \{(b, a) : b \in B, a \in A\}$, the fact that $A \times B = B \times A$ implies that $(a, b) = (b, a)$. So $a = b$. Since $a \in A$, it follows that $a \in B$. So $a \in A \Rightarrow a \in B$. Hence $A \subseteq B$. Similarly, $B \subseteq A$. Hence $A = B$.

Review Question 96. Explain what is wrong with the following "proof." In particular, indicate which is the first step in the proof that is either false or meaningless, and explain why. Is the claim true? CLAIM: If A, B are nonempty sets such that $A \times B = B \times A$ then $A = B$. PROOF: Suppose $A \times B = B \times A$. Since $A \times B = \{(a, b) : a \in A, b \in B\}$, and $B \times A = \{(b, a) : b \in B, a \in A\}$, the fact that $A \times B = B \times A$ implies that $(a, b) = (b, a)$. So $a = b$. Since $a \in A$, it follows that $a \in B$. So $a \in A \Rightarrow a \in B$. Hence $A \subseteq B$. Similarly, $B \subseteq A$. Hence $A = B$.

WARNING: Of the claims in the following eight questions (97 to 104), about half (I don't want to tell you exactly how many) are true and the remaining ones are false. Pay a lot of attention, and apply the rules with great care, for otherwise you are likely to make a serious mistake. **Almost all the people who did Problems 94 and 95 in the homework got them wrong.**

Review Question 97. Prove that if A, B are sets such that $A \times B = B \times A$, then $A = B$.

Review Question 98. Prove that if A, B are nonempty sets that satisfy the identity $A \times B = B \times A$, then $A = B$.

Review Question 99. Prove that if A, B, C, D are sets such that $A \times B = C \times D$ then $A = C$ and $B = D$.

Review Question 100. Prove that if A, B, C, D are nonempty sets such that $A \times B = C \times D$ then $A = C$ and $B = D$.

Review Question 101. Prove that if A, B, C, D are sets such that $A \times B = C \times D$ and B and D are nonempty, then $A = C$.

Review Question 102. Prove that if A, B, C, D are sets such that $A \times B = C \times D$ and A and C are nonempty, then $A = C$.

Review Question 103. Prove that if A, B, C, D are sets such that $A \times B = C \times D$ and A and B are nonempty, then $A = C$.

Review Question 104. Prove that if A, B, C, D are sets such that $A \times B = C \times D$ and A and D are nonempty, then $A = C$.

Review Question 105. Prove that if A, B, C are sets, $f : A \mapsto B$, and $g : B \mapsto C$, then the composite relation $g \circ f$ is a function from A to C.

Review Question 106. Define what it means for a function to be ***onto*** (that is, ***surjective***). (This is done in the book, page 198.)

Review Question 107. Prove that the composite of two surjective functions is surjective. That is, prove that if A, B, C are sets, $f : A \mapsto B$ is onto, and $g : B \mapsto C$ is onto, then $g \circ f$ is onto. (This is stated as an Exercise in the book, page 206.)

PROOF: Assume that A, B, C are sets, $f : A \mapsto B$ is onto, and $g : B \mapsto C$ is onto. Let $h = g \circ f$. To prove that h is onto, we want to prove that $(\forall z \in C)(\exists x \in A)h(x) = z$. Let $c \in C$ be arbitrary. Using the fact that g is onto, pick $b \in B$ such that $g(b) = c$. Then, using the fact that f is onto, pick $a \in A$ such that $f(a) = b$. Then $h(a) = g(f(a)) = g(b) = c$. So $h(a) = c$, and then $(\exists x \in A)h(x) = c$. Since c was an arbitrary member of C, we have shown that $(\forall z \in C)(\exists x \in A)h(x) = z$. **END.**

Review Question 108. Prove that if the composite of two functions is surjective, then the first function is surjective. ("First" means "the one that is applied first". That is, when we look at a composite function, $g \circ f$, the "first" one is f.) That is, prove that if A, B, C are sets, $f : A \mapsto B$, $g : B \mapsto C$, and $g \circ f$ is onto, then f is onto.

Review Question 109. Prove that if the composite of two functions is surjective, then the second function is surjective. That is, prove that if A, B, C are sets, $f : A \mapsto B$, $g : B \mapsto C$, and $g \circ f$ is onto, then g is onto.

Review Question 110. Define what it means for a function to be ***one-to-one*** (that is, ***injective***). (This is done in the book, page 201.)

Review Question 111. Prove that the composite of two injective functions is injective. That is, prove that if A, B, C are sets, $f : A \mapsto B$ is one-to-one, and $g : B \mapsto C$ is one-to-one, then $g \circ f$ is one-to-one. (This is proved in the book, page 202, Theorem 4.11.)

Review Question 112. Prove that if the composite of two functions is injective, then the first function is injective. That is, prove that if A, B, C are sets, $f : A \mapsto B$, $g : B \mapsto C$, and $g \circ f$ is one-to-one, then f is one-to-one.

Review Question 113. Prove that if the composite of two functions is injective, then the second function is surjective. That is, prove that if A, B, C are sets, $f : A \mapsto B$, $g : B \mapsto C$, and $g \circ f$ is one-to-one, then g is one-to-one.

Review Question 114. Define what it means for a function to be a ***one-to-one correspondence*** (that is, a ***bijection***) (This is done ine book, page 203.)

Review Question 115. Prove that the composite of two bijections is a bijection. That is, prove that if A, B, C are sets, $f : A \mapsto B$ is a bijection, and $g : B \mapsto C$ is a bijection, then $g \circ f$ is a bijection from A to C. (This is proved in the book, page 202, Theorem 4.11.)

Review Question 116. Prove that if the composite of two functions is bijective, then the first function is bijective. That is, prove that if A, B, C are sets, $f : A \mapsto B$, $g : B \mapsto C$, and $g \circ f$ is a bijection, then f is a bijection.

Review Question 117. Prove that if the composite of two functions is bijective, then the second function is bijective. That is, prove that if A, B, C are sets, $f : A \mapsto B$, $g : B \mapsto C$, and $g \circ f$ is a bijection, then g is a bijection.

Review Question 118. Define what it means for two sets to have ***the same cardinality*** (that is, to be ***equivalent***, or to be ***in one-to-one correspondence***), using the basic vocabulary of arithmetic, the basic vocabulary of set theory, the concepts of "ordered pair" and "function", and nothing else. (In particular, if in your definition you are going to use other concepts, such as "onto function", "one-to-one-function", or "bijection", then you have to define them first.)

Review Question 119. Prove that if A is a set then there does not exist an onto map $f : A \mapsto \mathcal{P}(A)$.

PROOF: Suppose an onto map $f : A \mapsto \mathcal{P}(A)$ exists. Pick one and call it F, so $F : A \mapsto \mathcal{P}(A)$ is onto. define a set S by letting $S = \{a \in A : a \notin F(a)\}$. Since F is onto, we may pick an $s \in A$ such that $F(s) = S$. Since $F(s) = S$, and $S = F(s)$, it follows that $s \notin F(s)$, so $s \notin S$. But the fact that $s \notin F(s)$ implies that $s \in S$. So $s \in S \wedge s \notin S$, which is a contradiction. Hence f does not exist.

Review Question 120. Define what it means for a set to be ***finite***, using the basic vocabulary of arithmetic, the basic vocabulary of set theory, the concepts of "ordered pair" and "function", and nothing else. (In particular, if in your definition you are going to use other concepts, such as "onto function", "one-to-one-function", "bijection", or "having the same cardinality", you have to define them first.)

Review Question 121. Define what it means for a set to be ***infinite***, using the basic vocabulary of arithmetic, the basic vocabulary of set theory, the concepts of "ordered pair" and "function", and nothing else. (In particular, if in your definition you are going to use other concepts, such as "onto function", "one-to-one-function", "bijection", "having the same cardinality", or "finite set", then you have to define them first.)

Review Question 122. Define what it means for a set to be ***infinite***, using the basic vocabulary of arithmetic, the basic vocabulary of set theory, the concepts of "ordered pair" and "function", and nothing else. (In particular, if in your definition you are going to use other concepts, such as "onto function", "one-to-one-function", "bijection", "having the same cardinality", or "finite set", then you have to define them first.)

Review Question 123. Define what it means for a set to be ***denumerable***, using the basic vocabulary of arithmetic, the basic vocabulary of set theory, the concepts of "ordered pair" and "function", and nothing else. (In particular, if in your definition you are going to use other concepts, such as "onto function", "one-to-one-function", "bijection", or "having the same cardinality", then you have to define them first.)

Review Question 124. Define what it means for a set to be ***countable***, using the basic vocabulary of arithmetic, the basic vocabulary of set theory, the concepts of "ordered pair" and "function", and nothing else. (In particular, if in your definition you are going to use other concepts, such as "onto function", "one-to-one-function", "bijection", or "having the same cardinality", then you have to define them first.)

Review Question 125. Prove that the set $\mathbb{Z}$ of all integers is denumerable.

Review Question 126. Prove that set $\mathbb{Q}$ of all rational numbers is denumebrable.

Review Question 127. Prove that the interval $I = \{x \in \mathbb{R} : 0 < x < 1\}$ is uncountable.

Review Question 128. Prove that the set $\mathbb{R}$ of all real numbers is uncountable. (You are allowed to use the fact that a subset of a countable set is countable.)