Proofs
January-April, 2016

J. Randall Miller
jum385@psu.edu
IST 230 (Language, Logic & Discrete Mathematics)
Section 3, Dr. S. Rajtmajer

1. Prove or disprove (*make sure to show and clearly identify all steps and give justifications for each step)*:

To prove:

$\forall$ integers x, if $x + 1$ is even, then $x + 5$ is even.

****

Premises:

1. $\forall x \in$ integers, x is even $\leftrightarrow$ x mod $2 = 0$	definition of an even integer
2. $\forall x \in$ integers $\forall y \in$ integers,	
$(x \bmod y) \bmod y = x \bmod y$	theorem of modular arithmetic
3. $\forall x \in$ integers $\forall y \in$ integers $\forall z \in$ integers,	
$(x + y) \bmod z = (x \bmod z + y \bmod z) \bmod z$	theorem of modular arithmetic
4. $\forall x \in$ integers, $x + 0 = x$	identity element of addition
5. $\forall x \in$ integers $\forall y \in$ integers $\forall z \in$ integers,	
$(x + y) + z = x + (y + z)$	associative property of addition
6. $\forall x \in$ integers, $x = x$	reflexive property of identity
7. $\forall x \in$ integers $\forall y \in$ integers,	
$x = y \leftrightarrow y = x$	symmetric property of identity
8. $\forall x \in$ integers $\forall y \in$ integers $\forall z \in$ integers,	
$(x = y \rightarrow (y = z \rightarrow x = z))$	transitive property of identity
9. $\forall x \in$ integers $\forall y \in$ integers $\forall z \in$ integers,	
$x = y \rightarrow x + z = y + z$	by substitution into $x + z = x + z$
10. $1 + 4 = 5$	provable proposition in arithmetic
11. $4 \bmod 2 = 0$	provable proposition in arithmetic

****

Assume now an arbitrary integer a. For this a,

12. (a + 1) + 4 = a + (1 + 4) = a + 5	(5), instantiation; (10), substitution
13. ((a + 1) + 4) mod 2 = (a + 5) mod 2	(6), instantiation; (12), substitution
= ((a + 1) mod 2 + 4 mod 2) mod 2	(3), instantiation
= ((a + 1) mod 2 + 0) mod 2	(11), substitution
= ((a +1) mod 2) mod 2	(4), instantiation; substitution
= (a + 1) mod 2	(2), substitution
14. (a + 5) mod 2 = (a + 1) mod 2 →	
((a + 1) mod 2 = 0 → (a + 5) mod 2 = 0)	(8), instantiation
15. (a + 1) mod 2 = 0 → (a + 5) mod 2 = 0	(13), (14), *modus ponens*

J. Randall Miller
jum385@psu.edu
IST 230 (Language, Logic & Discrete Mathematics)
Section 3, Dr. S. Rajtmajer

But since a was arbitrary,

16. $\forall x \in$ integers,

$((x + 1) \bmod 2 = 0 \rightarrow (x + 5) \bmod 2 = 0)$ generalization of the arbitrary case

$\therefore$ $\forall x \in$ integers,

$x + 1$ is even $\rightarrow x + 5$ is even (1), with substitution of equivalents*

*skipping some explicit steps, and relying upon the validity of the form:

$$((A \rightarrow B) \wedge (A \leftrightarrow C) \wedge (B \leftrightarrow D)) \rightarrow (C \rightarrow D)$$

2. Prove that if n is an odd integer, then n^2 is an odd integer. State what method of proof you are using. At the beginning of each proof, state what you are assuming and what the proof will show.

To prove: $\forall n \in \mathbb{Z}\,[n \text{ is odd} \rightarrow n^2 \text{ is odd}]$. NOTE: Strictly speaking, the consequent of the quantified expression should instead be the conjunction $(n^2 \in \mathbb{Z} \wedge n^2 \text{ is odd})$. But the suppressed lefthand expression of this conjunction follows directly from the essential closure of the integers under multiplication, and its exemplification for an arbitrary integer a could be simply appended to result obtained in (6)-(10) below before that result is converted to a conditional and generalized. The proof given below will not be complicated by the explicit addition of these steps.

Method of proof: direct, from a theorem of modular arithmetic

Assumptions:

(1) $\forall x \in \mathbb{Z}\,[x \text{ is odd} \equiv x \bmod 2 = 1]$ adopted definition of an odd integer

(2) $\forall x \in \mathbb{Z}\ \forall y \in \mathbb{Z}\ \forall z \in \mathbb{Z}\,[(x * y) \bmod z = (x \bmod z * y \bmod z) \bmod z]$
a theorem of modular arithmetic

(3) $\forall x \in \mathbb{Z}\,[x * 1 = x]$ the identity element of multiplication

(4) $1 \bmod 2 = 1$ a particular fact of integer arithmetic

(5) $\exists x \in \mathbb{Z}\,[x \bmod 2 = 1 \wedge x = a]$ provisionally assumed for a named arbitrary *a*

Proof:

(6) $a^2 \bmod 2 = (a * a) \bmod 2$ { }, just expanding the square-notation

(7) $= (a \bmod 2 * a \bmod 2) \bmod 2$ { (2) }, an instantiation of the universal (2)

(8) $= (1 * 1) \bmod 2$ { (5), (2) }, by the provisional assumption (5)

(9) $= 1 \bmod 2$ { (5), (2), (3) }, instantiating (3) and substituting

(10) $= 1$ { (5), (2), (3), (4) }, by (4) and substitution

(11) $a \bmod 2 = 1 \rightarrow a^2 \bmod 2 = 1$ { (2), (3), (4) }, (5) from a premise to an if-clause

(12) $\forall n \in \mathbb{Z}\,[n \bmod 2 = 1 \rightarrow n^2 \bmod 2 = 1]$
{ (2), (3), (4) }, universal generalization of (11)

$\therefore$ $\forall n \in \mathbb{Z}\,[n \text{ is odd} \rightarrow n^2 \text{ is odd}]$ { (1), (2), (3), (4) }, substitution of equivalents

J. Randall Miller
jum385@psu.edu
IST 230 (Language, Logic & Discrete Mathematics)
Section 3, Dr. S. Rajtmajer

3. Prove that if a and b are positive real numbers, then $\boldsymbol{a + b \geq \sqrt{ab}}$.

To prove (in broad strokes):

$$\forall x \in \mathbb{R}\, \forall y \in \mathbb{R}\, [\, (x > 0 \wedge y > 0) \rightarrow x + y \geq \sqrt{xy}\,]$$

If a and b are any pair of arbitrarily-chosen positive real numbers then $\sqrt{a}$, $\sqrt{b}$, $\sqrt{ab}$ and $(\sqrt{a} - \sqrt{b})$ all exist and are real, and the distributive law of multiplication over addition with the collection and commutation of resulting terms permits one to posit the equality

(1) $(\sqrt{a} - \sqrt{b}) * (\sqrt{a} - \sqrt{b}) = \sqrt{a}^2 - 2\sqrt{ab} + \sqrt{b}^2 = a + b - 2\sqrt{ab}$

so that (adding the same term to both extremes of the equality, commuting terms and employing the definition of the square operator)

(2) $a + b = 2\sqrt{ab} + (\sqrt{a} - \sqrt{b})^2$

Now the square of any real number and in particular $(\sqrt{a} - \sqrt{b})^2$ is not negative, so subtracting the latter from the right-hand side of the preceding equation will validly yield the inequality

(3) $a + b \geq 2\sqrt{ab}$,

the allowance for the equality of both terms being needed for the case where $a = b$, and therefore $(\sqrt{a} - \sqrt{b})^2 = 0$.

The validity of the inequality must be preserved* if its possibly smaller right-hand member is divided by the positive integer 2, that is,

(4) $a + b \geq \sqrt{ab}$

* since our domain is the strictly positive rather than the non-negative real numbers we know that a and b are nonzero, and thus the '≥' could be replaced here with a '>'

But since a and b were arbitrarily-chosen with no special properties other than being severally real and greater than 0, we can generalize this result to

$\forall x \in \mathbb{R}\, \forall y \in \mathbb{R}\, [\, (x > 0 \wedge y > 0) \rightarrow x + y \geq \sqrt{xy}\,]$ *(QED)*

which is the result that was to be proven.

J. Randall Miller
jum385@psu.edu
IST 230 (Language, Logic & Discrete Mathematics)
Section 3, Dr. S. Rajtmajer

4. Prove that there is no smallest integer.

I will allow that the smallest integer, were it to exist, need not be smaller than itself, so that the proposition to be proven is

$$\neg\, \exists x \in \mathbb{Z}\, \forall y \in \mathbb{Z}\, [x \neq y \rightarrow x < y]$$

The proof will be a *reductio ad absurdum* that itself assumes the hypothesis that the just-given proposition negates, and then shows that this assumption leads directly to contradiction.

Note that the proposition to be demonstrated is in fact false for the domain $\mathbb{N}$ or $\mathbb{N} \cup \{0\}$. While the latter set, being recursively defined to be the smallest set that contains both the element 0 and the successor of every element of the set, is easily seen to be closed under the operation of addition, that same set is not closed, as is $\mathbb{Z}$, under the operation of subtraction.

The manner in which the proof proceeds depends upon how one should assume that $\mathbb{Z}$ has been defined in terms of the non-negative integers. If one assumes that $\mathbb{Z}$ has been recursively defined as the smallest set that contains all of the elements of $\mathbb{N} \cup \{0\}$ as well as the predecessor (rather than additive inverse) of every element of the set, then the proof becomes almost a *petitio principii*, although the explicit listing of several steps used to validly manipulate the existential quantifier will unfortunately lengthen it somewhat.

Provisionally assume the hypothesis that will be demonstrated to yield a contradiction:

(1) $\exists x \in \mathbb{Z}\, \forall y \in \mathbb{Z}\, [x \neq y \rightarrow x < y]$ $\{1\}$, provisional hypothesis

Designate some value of the variable x that is additionally supposed to satisfy the just-given hypothesis "a", so that we have, for this distinguished integer a: $a \in \mathbb{Z}$,

(2) $\forall y \in \mathbb{Z}\, [a \neq y \rightarrow a < y]$ $\{2\}$, premise

Finally, let us posit a second integer, named "b", and assume with respect to this b: $b \in \mathbb{Z}$ that it is equal to the predecessor of a:

(3) $b = a - 1$ $\{3\}$, premise

Instantiate the universal quantification contained in premise (2):

(4) $a \neq b \rightarrow a < b$ $\{2\}$, universal instantiation

and substitute for b in the result the value given to it in premise (3):

(5) $a \neq a - 1 \rightarrow a < a - 1$ $\{2, 3\}$, substitution of identicals

J. Randall Miller
jum385@psu.edu
IST 230 (Language, Logic & Discrete Mathematics)
Section 3, Dr. S. Rajtmajer

Adding the same quantity to both sides of the inequalities in the antecedent and consequence of this conditional will preserve its truth value (by a tautological chain of consequences of the properties of the identity relation, and the propositional substitution of equivalents); choose this quantity to equal the successor $-a + 1$ of the additive inverse of a, and the conditional (5) becomes:

(6) $1 \neq 0 \ \rightarrow 1 \ < 0$ $\{2, 3\}$, algebraic transformation

(proof abbreviated here by the omission of intermediate steps)**

which, since (7) $1 \neq 0$, leads to the straightforward falsehood:

(8) $1 < 0$ $\{2, 3\}$, (6) and (7) by *modus ponens*

Transform (3) from a premise to the antecedent of a conditional,

(9) $b = a - 1 \ \rightarrow \ 1 < 0$ $\{2\}$, (8) by premise deletion

generalize this proposition to a universal statement,

(10) $\forall y \in \mathbb{Z}\, [y = a - 1 \ \rightarrow \ 1 < 0\,]$ $\{2\}$, (9) by universal generalization

and transform the universal quantification in (10) to its corresponding existential form:

(11) $\exists y \in \mathbb{Z}\, [y = a - 1\,] \rightarrow \ 1 < 0$ $\{2\}$, (10) by quantifier manipulation

Now, finally, the proof can make use of the assumed definitional closure of the integer domain $\mathbb{Z}$ with respect to the predecessor operation on all of its elements

(12) $\forall x \in \mathbb{Z}\, \exists y \in \mathbb{Z}\, [y = x - 1\,]$ $\emptyset$, definitional property of $\mathbb{Z}$

which can be instantiated to the particular more relevant proposition

(13) $\exists y \in \mathbb{Z}\, [y = a - 1\,]$ $\emptyset$, instantiation of (12)

a result that in combination with (11) again produces the falsehood

(14) $1 < 0$ $\{2\}$, (11) and (13) by *modus ponens*

but this time as a consequence of the premise (2) alone. Transform this premise (2) to the antecedent of a conditional,

(15) $\forall y \in \mathbb{Z}\, [a \ \neq y \ \rightarrow a \ < y] \ \rightarrow \ 1 < 0$ $\emptyset$, from (14) by premise deletion

generalize over the arbitrary instance a, which is not mentioned in any premise of (15),

(16) $\forall x \in \mathbb{Z}\, [\forall y \in \mathbb{Z}\, [x \ \neq y \ \rightarrow x \ < y] \ \rightarrow \ 1 < 0\,]$

$\emptyset$, universal generalization of (15)

and then transform the universal quantification in (16) to its corresponding existential form:

(17) $\exists x \in \mathbb{Z}\, \forall y \in \mathbb{Z}\, [x \ \neq y \ \rightarrow x \ < y] \ \rightarrow \ 1 < 0$ $\emptyset$, (10) by quantifier manipulation

J. Randall Miller
jum385@psu.edu
IST 230 (Language, Logic & Discrete Mathematics)
Section 3, Dr. S. Rajtmajer

With (17) we now have our recurring falsehood as a straightforward consequence of the premise (1) that we set out to disprove:

(18) $1 < 0$ $\{1\}$, (1) and (17) by *modus ponens*

But since $1 \geq 0$ is tautologically true this contrary proposition is also deducible from the same premise (1):

(19) $1 \nless 0$ $\{1\}$, truth of arithmetic

So finally this contradiction permits us to assert *simpliciter*:

(20) $\neg\exists x \in \mathbb{Z}\, \forall y \in \mathbb{Z}\, [x \neq y \rightarrow x < y]$, *QED*

$\{1\} \sim \{\neg 20\}$ *or* $\emptyset$, a *reductio ad absurdum*

**Upon this description of the algebraic transformation of (5) into (6) it seems that its proof might also require invocation of an axiom or theorem that the additive inverse of any element of $\mathbb{Z}$ itself exists as an element of $\mathbb{Z}$, a second assumption that comes dangerously close to being a *petitio principii*. But the transformation can be recast to require only the assumption about the definitional properties of $\mathbb{Z}$ to which the proof is already committed. Take as previously established the set of theorems schematized by:

$$\forall x \in \mathbb{Z}\, \forall y \in \mathbb{Z}\, \forall z \in \mathbb{Z}\, [x\, R\, y \leftrightarrow (x+z)\, R\, (y+z)]$$

where 'R' stands for any of the binary relational operators '=', '≠ ', '≤ ', ' >',..., etc. Now instantiate this form for '≠' and '<' with $x = 1$, $y = 0$, and $z = b$, the last being an integer already supposed in premise (3) of the proof to be equal to the predecessor $a - 1$ of a, and there result from straightforward arithmetic two equivalences that can be substituted into (5) to give (6). The supposition (3) is finally eliminated from the premise set of the proof by the sequence of steps in (8)-(14) that explicitly invoke the closure of $\mathbb{Z}$ under the predecessor operation.

5. Prove that if x and y are real numbers, then max(x,y)+min(x,y)=x+y.

To prove: $\forall x \in \mathbb{R}\, \forall y \in \mathbb{R}\, [max(x,y) + min(x,y) = x + y]$

Assumptions:

(1) $\forall x \in \mathbb{R}\, \forall y \in \mathbb{R}\, [x \leq y \vee y \leq x]$ $\emptyset$, total ordering of the real-number domain by '≤'

(2) $\forall x \in \mathbb{R}\, \forall y \in \mathbb{R}\, [(min(x,y) = x \leftrightarrow x \leq y) \wedge (min(x,y) = y \leftrightarrow y \leq x)]$

$\emptyset$, a definition of $\min()$

(3) $\forall x \in \mathbb{R}\, \forall y \in \mathbb{R}\, [(max(x,y) = x \leftrightarrow y \leq x) \wedge (max(x,y) = y \leftrightarrow x \leq y)]$

$\emptyset$, a definition of $\max()$

J. Randall Miller
jum385@psu.edu
IST 230 (Language, Logic & Discrete Mathematics)
Section 3, Dr. S. Rajtmajer

The following may not be necessary to the proof, but makes it evident that $\min()$ and $\max()$ are both functions, as is doubtless intended:

(4) $\forall x \in \mathbb{R}\, \forall y \in \mathbb{R}\, [(x \leq y \wedge y \leq x) \rightarrow x = y]$

$\emptyset$, antisymmetry of '≤'

The proof will be a direct one that exhausts the consequences of a dilemma. Most (although not all) of the intermediate deductive steps are made explicit and separately listed, so that the proof is prolix.

Arbitrarily select two real numbers named "a" and "b"; assume in the first instance that

(5) $a \leq b$ $\{5\}$, provisional premise

Instantiating (2), detaching the left-hand member of its conjunction, and reading its biconditional from right to left gives:

(6) $a \leq b \rightarrow min(a, b) = a$ $\emptyset$, instantiation of definition

Instantiating (3), detaching the right-hand member of its conjunction, and reading its biconditional from right to left gives:

(7) $a \leq b \rightarrow max(a, b) = b$ $\emptyset$, instantiation of definition

Use of the provisional assumption (5) with (6) and (7) yields—

(8) $min(a, b) = a, max(a, b) = b$ $\{5\}$, *modus ponens*

—which equalities can substituted into the reflexive identity $b + a = b + a$ to give the result

(9) $max(a, b) + min(a, b) = b + a$ $\{5\}$, substitution

(10) $= a + b$ $\{5\}$, algebraic transformation

where in the final step (10) I have taken the liberty of making an immediate application of the commutative property of real-number addition. Changing (5) from a provisional premise to the antecedent of a conditional produces

(11) $a \leq b \rightarrow max(a, b) + min(a, b) = a + b$

$\emptyset$, premise deletion

The case for $b \leq a$ will now be developed in steps exactly parallel to steps (5)-(11) above; the reader who wishes to spare herself some tedium can proceed directly to step (17).

(12) $b \leq a$ $\{12\}$, provisional premise

Instantiating (2), detaching the right-hand member of its conjunction, and reading its biconditional from right to left gives:

(13) $b \leq a \rightarrow min(a, b) = b$ $\emptyset$, instantiation of definition

J. Randall Miller
jum385@psu.edu
IST 230 (Language, Logic & Discrete Mathematics)
Section 3, Dr. S. Rajtmajer

Instantiating (3), detaching the left-hand member of its conjunction, and reading its biconditional from right to left gives:

(14) $b \leq a \rightarrow max(a,b) = a$ ∅, instantiation of definition

Use of the provisional assumption (12) with (13) and (14) yields—

(15) $min(a,b) = b, max(a,b) = a$ $\{12\}$, *modus ponens*

—which equalities can substituted into the reflexive identity $a + b = a + b$ to give the result

(16) $max(a,b) + min(a,b) = a + b$ $\{12\}$, substitution

Changing (12) from a provisional premise to the antecedent of a conditional produces

(17) $b \leq a \rightarrow max(a,b) + min(a,b) = a + b$
∅, premise deletion

The total ordering of the real-number domain by '≤' can now be invoked with particular respect to the selected numbers a and b:

(18) $a \leq b \vee b \leq a$ ∅, instantiation of (1)

By the valid rule of inference known as the constructive dilemma (11), (17) and (18) can be combined to produce the redundant disjunction

(19) $max(a,b) + min(a,b) = a + b \vee max(a,b) + min(a,b) = a + b$
∅, constructive dilemma

which of course may be simplified, as an instance of what our textbook calls the idempotent law, to

(20) $max(a,b) + min(a,b) = a + b$ ∅, simplification

Since a and b are arbitrary save for the proviso that they both belong to the real-number domain, (20) may be generalized to:

(21) $\forall x \in \mathbb{R}\, \forall y \in \mathbb{R}\, [max(x,y) + min(x,y) = x + y]$, *QED*

∅, universal generalization

which is the desired result.

6. Prove that for any $n \geq 2$, 4 evenly divides $3^{2n} - 1$.

To prove: $\forall n \in \mathbb{N}\, \exists m \in \mathbb{N}\, [n \geq 2 \rightarrow 3^{2n} - 1 = 4m]$

If the proposition is true for all $n \geq 1$ it will *ipso facto* be true for all $n \geq 2$. And in fact we have

(1) $3^{2*1} - 1 = 9 - 1 = 8 = 4 * 2$ ∅, arithmetic and substitution

J. Randall Miller
jum385@psu.edu
IST 230 (Language, Logic & Discrete Mathematics)
Section 3, Dr. S. Rajtmajer

Now suppose that for two natural numbers k and q

(2) $3^{2k} - 1 = 4q$ $\{2\}$, inductive hypothesis

It will prove useful to immediately transform this to

(3) $3^{2k} = 4q + 1$ $\{2\}$, adding 1 to both terms

For the successor $k + 1$ of k algebra yields

(4) $3^{2(k+1)} - 1 = 3^{2k+2} - 1$ $\emptyset$, distributive law

(5) $= 3^{2k} * 3^2 - 1$ $\emptyset$, law of exponents

(6) $= (4q + 1) \cdot 9 - 1$ $\{2\}$, substituting from (3) and from $3^2 = 9$

If we apply the distributive law to (6) and then collect, arrange and factor the resulting terms we have $3^{2(k+1)} - 1$

(7) $= 36q + 8 = 4 \cdot (9q + 2) = 4q'$, with $q' = 9q + 2$

$\{2\}$, from (6) by algebra

We can now transform (2) from a premise to the antecedent of a conditional,

(8) $3^{2k} - 1 = 4q \rightarrow 3^{2(k+1)} - 1 = 4q'$ $\emptyset$, premise deletion

Because $q \in \mathbb{N}$ and $\mathbb{N}$ is closed under the operations of multiplication and addition we know, moreover, that $q' \in \mathbb{N}$; and since k does not appear among any premises of (8), we may generalize (8) to the universal proposition:

(9) $\forall n \in \mathbb{N} \left[\exists m \in \mathbb{N} \left[3^{2n} - 1 = 4m\right] \rightarrow \exists m' \in \mathbb{N} \left[3^{2(n+1)} - 1 = 4m'\right]\right]$

$\emptyset$, successive existential and universal generalizations

After (1) is similarly generalized to

(10) $\exists m \in \mathbb{N} \left[3^{2*1} - 1 = 4m\right]$ (1), existential generalization

the combination of (9) and (10) produces by the principle of mathematical induction the desired result:

$$\forall n \in \mathbb{N}\ \exists m \in \mathbb{N} \left[\ 3^{2n} - 1 = 4m\right], \textit{QED}$$

The weaker statement proposed in the formulation of this question is evidently a direct consequence of the foregoing.

7. Prove or disprove: For all integers x, if x+2 is even, then 3x+5 is odd.

The proposition is true, and it appears that its direct proof by means of theorems of modular arithmetic will be more straightforward than a proof, for example, by mathematical induction. So this proof will make use of the definitional axioms:

J. Randall Miller
jum385@psu.edu
IST 230 (Language, Logic & Discrete Mathematics)
Section 3, Dr. S. Rajtmajer

(1) $\forall x \in \mathbb{Z}\,[x\ is\ even\ \leftrightarrow_{def} x\ mod\ 2 = 0]$ ∅, definition

(2) $\forall x \in \mathbb{Z}\,[x\ is\ odd\ \leftrightarrow_{def} x\ mod\ 2 = 1]$ ∅, definition

in terms of which the proposition to be proven becomes**

To prove:

$$\forall x \in \mathbb{Z}\,[(x+2)\ mod\ 2 = 0 \rightarrow (3x+5)\ mod\ 2 = 1]$$

In adopting definition (2) above I have already made implicit use of (or obviated) the disjunction that either $x\ mod\ 2 = 0$ or $x\ mod\ 2 = 1$ for any integer x; provable general theorems and particular facts of arithmetic that also comprise the presuppositions of this proof include the following

Assumptions:

(3) $\forall x \in \mathbb{Z}\,\forall n \in \mathbb{N}\,[(x\ mod\ n)\ mod\ n = x\ mod\ n]$ ∅, theorem of modular arithmetic

(4) $\forall x \in \mathbb{Z}\,\forall y \in \mathbb{Z}\,\forall n \in \mathbb{N}\,[(x+y)\ mod\ n = (x\ mod\ n + y\ mod\ n)\ mod\ n]$

∅, theorem of modular arithmetic

(5) $\forall x \in \mathbb{Z}\,\forall y \in \mathbb{Z}\,\forall n \in \mathbb{N}\,[(x * y)\ mod\ n = (x\ mod\ n * y\ mod\ n)\ mod\ n]$

∅, theorem of modular arithmetic

(6) $\forall x \in \mathbb{Z}\ [x + 0 = x]$ ∅, identity element of addition

(7) $\forall x \in \mathbb{Z}\ [x * 1 = x]$ ∅, identity element of multiplication

(8) $0\ mod\ 2 = 0 \wedge 1\ mod\ 2 = 1 \wedge 2\ mod\ 2 = 0 \wedge 3\ mod\ 2 = 1 \wedge 4\ mod\ 2 = 0 \wedge 5\ mod\ 2 = 1$

∅, a few conjoined facts of arithmetic

****

Taking "k" as the name of some arbitrarily selected integer, let us introduce first the supposition

(9) $(k+2)\ mod\ 2 = 0$ {9}, premise introduction

Now by the above-cited principles of modular arithmetic

(10) $(k+2)\ mod\ 2 = (k\ mod\ 2 + 2\ mod\ 2)\ mod\ 2$ ∅, universal instantiation of (4)

(11) $= (k\ mod\ 2 + 0)\ mod\ 2$ ∅, decomposing (8) and substituting

(12) $= (k\ mod\ 2)\ mod\ 2$ ∅, instantiating (6) and substituting

(13) $= k\ mod\ 2$ ∅, instantiating (3) and substituting

so that by substituting (13) into (9) it appears that from (9) there is deducible the proposition that

(14) $k\ mod\ 2 = 0$ {9}, substitution of identicals

Again by the postulated principles of modular arithmetic

J. Randall Miller
jum385@psu.edu
IST 230 (Language, Logic & Discrete Mathematics)
Section 3, Dr. S. Rajtmajer

(15) $(3k+5)\ mod\ 2 = (3k\ mod\ 2 + 5\ mod\ 2)\ mod\ 2$ ∅, a universal instantiation of (4)

(16) $= \big((3\ mod\ 2 * k\ mod\ 2)\ mod\ 2 + 5\ mod\ 2\big)\ mod\ 2$

∅, instantiating (5) and substituting

(17) $= \big((1 * k\ mod\ 2)\ mod\ 2 + 1\big)\ mod\ 2$ ∅, decomposing (8) and substituting

(18) $= \big((k\ mod\ 2)\ mod\ 2 + 1\big)\ mod\ 2$ ∅, instantiating (7) and substituting

(19) $= (k\ mod\ 2 + 1)\ mod\ 2$ ∅, instantiating (3) and substituting

Because of the special property of k posited in premise (9) we can substitute (14) into (19) to obtain an equality having the (not generally valid) categorical form

(20) $(3k+5)\ mod\ 2 = (0+1)\ mod\ 2$ $\{9\}$, substitution of identicals

(21) $= 1\ mod\ 2$ $\{9\}$, instantiating (6) and substituting

(22) $= 1$ $\{9\}$, decomposing (8) and substituting

The singular proposition (9) can now be deleted from the set of premises and instead made the explicit antecedent of a valid conditional whose consequent is the categorical equality expressed in the preceding (22):

(23) $(k+2)\ mod\ 2 = 0 \rightarrow (3k+5)\ mod\ 2 = 1$ ∅, (22) with premise transformation

But since "k" denotes an arbitrarily selected integer and does not appear in any member of the current premise set we can replace every occurrence of it in (23) with a universally quantified variable:

(24) $\forall x \in \mathbb{Z}\ [(x+2)\ mod\ 2 = 0 \rightarrow (3x+5)\ mod\ 2 = 1]$ ∅, universal generalization of (23)

By the working definitions (1) and (2) the foregoing is equivalent to:

(25) $\forall x \in \mathbb{Z}\ [(x+2)\ is\ even \rightarrow (3x+5)\ is\ odd]$ *(QED)*

which is the proposition that was to be proven.

**Stating the problem in these terms suggests a possibly quicker and more elegant means of proof, by way of proving the slightly stronger proposition

$$\forall x \in \mathbb{Z}\ [(x+2) \not\equiv (3x+5)\ mod\ 2]$$

which is stronger than the proposition given for proof because it also entails its (likewise valid) converse. Such a proof might nevertheless be shorter because it need only show the validity of the formula:

$$2 \nmid \big((3x+5) - (x+2)\big)$$

J. Randall Miller
jum385@psu.edu
IST 230 (Language, Logic & Discrete Mathematics)
Section 3, Dr. S. Rajtmajer

which is immediately apparent to intuition when the subtraction on the right-hand side of the relation is performed, and the resulting difference is expressed as

$$2 * (x + 1) + 1$$

This has the form of the Euclidean division algorithm for the divisor 2, the quotient $(x + 1) \in \mathbb{Z}$, and the positive nonzero remainder $1 < 2$.

8. Prove that if an integer n is positive and a perfect square, then $n + 2$ is not a perfect square.

I. The overall structure of a direct proof, in broad outline, is as follows:

a. Since the positive integer $n + 2 > n$, if $n + 2$ is a perfect square it is necessarily an element of the intersection of the set of all integers greater than n and the set of all perfect squares.

b. Since $\mathbb{N}$ is well-ordered and the set of all perfect squares greater than n is a subset of $\mathbb{N}$, there exists an element of this latter set that is its *least element*, *i.e.*, that is smaller than every other element of the set. If $n + 2$ is a perfect square it must therefore be equal to or greater than this least element of the set.

c. There is a bijection or one-to-one correspondence given by the function $y = f(x) = x^2$ (or equivalently by its inverse $x = f^{-1}(x^2) = \sqrt[2]{y}$) between the natural numbers $\mathbb{N}$ and the set of all nonzero perfect squares, such that according to the correspondence the elements of the latter set can be arranged like (and paired off with) the elements of $\mathbb{N}$, in a monotonically increasing sequence: that is, $y_2 > y_1$ and follows y_1 in the sequence if, and only if, $\sqrt[2]{y_2} > \sqrt[2]{y_1}$.

d. In the well-ordering of $\mathbb{N}$ the least element of the subset of positive integers that contains all of those integers that are $> x$ is x's immediate successor $x + 1$. Because of the existence of the one-to-one mapping just described above in (c), it must therefore be the case that if $n \in \mathbb{N}$ is a nonzero perfect square, the least element of the set of all perfect squares that are greater than n will be equal to $\left(\sqrt[2]{n} + 1\right)^2 = n + 2\sqrt[2]{n} + 1$.

e. The first nonzero positive perfect square is 1, and its corresponding root $\sqrt[2]{n} = 1$, the smallest element of $\mathbb{N}$, so that $\forall n \in \{y: \exists x[x \in \mathbb{N} \wedge y = x^2]\}\left[n + 2\sqrt[2]{n} + 1 \ \geq n + 3\right]$. Therefore the number $n + 2 \ \ngeq n + 2\sqrt[2]{n} + 1 =$ the least perfect square that is $> n$, which entails, according to (b) above, that $n + 2$ cannot be a perfect square.

I believe that a more detailed and formally stricter proof than I have just sketched out might well require use of principles of set theory and second-order formal logic beyond my limited skills in first-order quantificational /propositional logic, so I haven't attempted it here.*

II. But a less demanding proof by the technique of *reductio ad absurdum* may yet be available:

J. Randall Miller
jum385@psu.edu
IST 230 (Language, Logic & Discrete Mathematics)
Section 3, Dr. S. Rajtmajer

a. Suppose that two arbitrary positive integers a and $a+2$ are perfect squares. By algebra their difference $2 = \left(\sqrt[2]{a+2} + \sqrt[2]{a}\right) * \left(\sqrt[2]{a+2} - \sqrt[2]{a}\right)$. Now by provisional hypothesis $\sqrt[2]{a+2}$ and $\sqrt[2]{a}$ are both integers, so that their sum and their difference must be integers, too; moreover their sum must be greater than their difference since $a > 0$.

b. But the difference $= 2$ of the two presumed perfect squares is itself the first prime number, so that its only distinct integral factors are 2 and 1; setting the sum of the roots equal to the greater factor, and the difference of the roots equal to the lesser, yields:

$$\sqrt[2]{a+2} + \sqrt[2]{a} = 2$$

$$\sqrt[2]{a+2} - \sqrt[2]{a} = 1$$

Solving this pair of equations by successive addition and subtraction of the one from the other gives $\sqrt[2]{a+2} = 3/2$ and $\sqrt[2]{a} = 1/2$; although this result satisfies the condition that $(3/2)^2 = (1/2)^2 + 2$, it contradicts the hypothesis that a and $a+2$ are perfect squares— *i.e.*, that their roots are both of them integers.

c. Because we can deduce from the hypothesis that a and $a+2$ are both perfect squares the contrary conclusion that neither of them is, we have proven the result that either a or $a+2$ is not a perfect square. So then if a is a perfect square, $a+2$ is not ($(p \vee q) \rightarrow (\neg p \longrightarrow q)$).

d. Since $'a'$ names some arbitrarily selected positive integer and does not appear in any premises of the foregoing result, we may universally generalize the result to

$$\forall n \in \mathbb{N}\left[\exists j \in \mathbb{N}[n = j^2] \rightarrow \forall k \in \mathbb{N}[n+2 \neq k^2]\right] \text{ (}QED\text{)}$$

* A few of the more significant propositions stated in or presupposed by paragraphs (c)-(d) of section I might be deduced from more fundamental ones in the manner shown here. First, from the group of natural-number theorems pertaining to the ordering of products, all of them having the schematic form

$$\forall x \in \mathbb{N}\ \forall y \in \mathbb{N}\ \forall z \in \mathbb{N}[xRy \leftrightarrow xzRyz]$$

obtain by successive instantiations, for example, $a < b \leftrightarrow aa < ba$ and $a < b \leftrightarrow ab < bb$; then commute ba to ab, instantiate the transitive property of the ordering relation to obtain the equivalence $a < b \leftrightarrow aa < bb$, and universally generalize the result.

From this schematic result it is not difficult, although a little tedious, to show that the least perfect square that is greater than n must be equal to the square of the immediate successor $\left(\sqrt[2]{n} + 1\right)$ of its square root. By definition this perfect square cannot be $\leq n$, and so cannot be the square of any integer $\leq \sqrt[2]{n}$, from the result just obtained; but since the immediate successor $\left(\sqrt[2]{n} + 1\right)$ of $\sqrt[2]{n}$ is the least element of the set of the integers greater than $\sqrt[2]{n}$, if the least perfect square that is

J. Randall Miller
jum385@psu.edu
IST 230 (Language, Logic & Discrete Mathematics)
Section 3, Dr. S. Rajtmajer

greater than n were to be the square of some integer other than $\left(\sqrt[2]{n}+1\right)$ it would necessarily be the square of an integer greater than $\left(\sqrt[2]{n}+1\right)$, and as such would have to be greater than the square of $\left(\sqrt[2]{n}+1\right)$, even though this latter square is itself greater than n (because its square root is greater than $\sqrt[2]{n}$). This last circumstance violates the supposition that the provisionally presumed alternative is the least perfect square that is greater than n.

9. Prove that any postage of 8 cents or more can be made from 5 cent or 3 cent stamps.

The proposition to be proven can be formalized as

To prove:

$$\forall n \in \mathbb{N} \cup \{0\}\ \exists j \in \mathbb{N}\ \cup \{0\}\, \exists k \in \mathbb{N} \cup \{0\}\, [n \geq 8 \rightarrow n = 3j + 5k]$$

The proof will proceed by mathematical induction, *** but requires the use of a lemma that will itself, in steps (1)-(11), be directly proved first:

Lemma:

$$\forall n \in \mathbb{N} \cup \{0\}\ \forall j \in \mathbb{N}\ \cup \{0\}\, \forall k \in \mathbb{N} \cup \{0\}\, [(n \geq 8 \wedge n = 3j + 5k) \rightarrow (j \geq 3 \vee k \geq 1)]$$

Suppose three integers a, b and c within the domain $\mathbb{N} \cup \{0\}$ that satisfy the relation

(1) $a = 3b + 5c$ $\{1\}$, premise introduction

Suppose further that

(2) $\neg(b \geq 3 \vee c \geq 1)$ $\{2\}$, premise introduction

or in other words (using a few facts about small integers) that

(3) $b \leq 2\ \wedge\ c = 0$ $\{2\}$, DeMorgan's law

Detaching the terms of the conjunction (3), making use of the zero property of multiplication and identity substitutions to obtain $5c = 0$ and $a = 3b$, and then multiplying both sides of the inequality $b \leq 2$ by the positive integer 3 to obtain $3b \leq 2 * 3$, we have, using the arithmetical fact that $2 * 3 = 6$,

(4) $a \leq 6$ $\{1, 2\}$, algebraic transformation of (1)

or, making use of the transitive property of the ordering relationship and the fact that $6 < 8$,

(5) $a < 8$ $\{1, 2\}$, from (4) and $6 < 8$

Deleting (1) from the premise set to make it the antecedent of a conditional, we have

(6) $(a = 3b + 5c) \rightarrow a < 8$ $\{2\}$, premise deletion/transformation

This conditional (6) is equivalent by the laws of propositional logic to the disjunction

(7) $a < 8\ \vee \neg(a = 3b + 5c)$ $\{2\}$, disjunctive equivalent of (6)

J. Randall Miller
jum385@psu.edu
IST 230 (Language, Logic & Discrete Mathematics)
Section 3, Dr. S. Rajtmajer

which in turn is equivalent by DeMorgan's law (with $\neg\neg p \equiv p$) to

(8) $\neg(a \geq 8 \ \wedge \ a \ = \ 3b + 5c)$ $\{2\}$, DeMorgan's law applied to (7)

Deleting (2) from the premise set and making it the premise of a conditional,

(9) $\neg(b \geq 3 \vee c \geq 1) \rightarrow \neg(a \geq 8 \ \wedge \ a \ = \ 3b + 5c)$

$\emptyset$, premise deletion/transformation

which is equivalent (again with $\neg\neg p \equiv p$) to its contraposition:

(10) $(a \geq 8 \ \wedge \ a \ = \ 3b + 5c) \rightarrow \ (b \geq 3 \vee c \geq 1)$

$\emptyset$, the contraposition of (9) for (9)

Now since the three integers a, b and c, apart from the proviso of their membership in the domain $\mathbb{N} \cup \{0\}$, are completely arbitrary, and no longer appear in any proposition that is a member of the premise set, we may replace every occurrence of the name of each in (10) with a distinct variable that is the subject of a universal quantification:

(11) $\forall n \in \mathbb{N} \cup \{0\} \ \forall j \in \mathbb{N} \ \cup \{0\} \forall k \in \mathbb{N} \cup \{0\} \ [(n \geq 8 \wedge n = 3j + 5k) \rightarrow (j \geq 3 \vee k \geq 1)]$

$\emptyset$, universal generalization of (10)

(11) is the lemma needed for the core proof by mathematical induction, to which we now turn.

First, remark that

(12) $8 = 3 * 1 + 5 * 1$ $\emptyset$, fact of arithmetic

and therefore

(13) $\exists j \in \mathbb{N} \ \cup \{0\} \ \exists k \in \mathbb{N} \cup \{0\} \ [8 = 3j + 5k]$ $\emptyset$, existential generalization of (12)

Suppose next that for some three integers named a, b and c within the domain $\mathbb{N} \cup \{0\}$ we have

(14) $a \geq 8 \ \wedge \ a \ = \ 3b + 5c$ $\{14\}$, inductive hypothesis

Consider first the case of (14) in combination with the additional hypothesis that

(15) $b \geq 3$ $\{15\}$, provisional premise introduction

The preceding supposition allows us to add 1 to both terms of the righthand clause of the conjunction (14) by replacing b with $b' \coloneqq b - 3$ and c with $c' \coloneqq c + 2$, while all variables still remain confined to the required domain; we can also add 1 to the lefthand term of the other, lefthand clause, since if $a \geq 8$ then *ipso facto* so is $a + 1$:

J. Randall Miller
jum385@psu.edu
IST 230 (Language, Logic & Discrete Mathematics)
Section 3, Dr. S. Rajtmajer

(16) $a + 1 \geq 8 \ \wedge \ a + 1 \ = \ 3(b - 3) + 5(c + 2) = 3b' + 5c'$, with $a + 1,\ b'$and $c' \in \ \mathbb{N} \cup \{0\}$
$\{14, 15\}$; closure, distributive law and
$3 * -3 + 5 * 2 = \ -9 + 10 = 1$

Deleting (15) from the premise set yields the conditional (with $b'$and c' as defined above)

(17) $b \geq 3 \rightarrow (a + 1 \geq 8 \ \wedge \ a + 1 \ = \ 3b' + 5c')$ $\{14\}$, from (16) by premise deletion

Similarly we may consider the case which combines (14) with the alternate hypothesis that

(18) $c \geq 1$ $\{18\}$, provisional premise introduction

The preceding supposition allows us to add 1 to both terms of the righthand clause of the conjunction (14) by replacing b with $b'' \coloneqq b + 2$ and c with $c'' \coloneqq c - 1$; and again the fact that $a \ \geq 8 \rightarrow \ a + 1 \geq 8$ lets us increment the lefthand term of its lefthand clause, too:

(19) $a + 1 \geq 8 \ \wedge \ a + 1 \ = \ 3(b + 2) + 5(c - 1) = 3b'' + 5c''$, with $a + 1,\ b'',\ c'' \in \ \mathbb{N} \ \cup \{0\}$
$\{14, 18\}$; closure, distributive law and
$3 * 2 + 5 * -1 = \ 6 + -5 = 1$

Deleting (18) from the premise set now yields the conditional (with $\mathrm{b}''$and c'' as defined above)

(20) $c \geq 1 \rightarrow (a + 1 \geq 8 \ \wedge \ a + 1 \ = \ 3b'' + 5c'')$ $\{14\}$, from (19) by premise deletion

An appropriate instantiation of the lemma proved above in (1)-(11) above gives

(21) $(a \geq 8 \ \wedge \ a \ = \ 3b + 5c) \rightarrow (b \geq 3 \vee c \geq 1)$ $\emptyset$, universal instantiation of (11)

And (21) and (14) together produce by *modus ponens* the consequence

(22) $b \geq 3 \vee c \geq 1$ $\{14\}$, (14) and (21), by *modus ponens*

(17), (20) and (22) in turn yield by constructive dilemma (with some elimination of redundancy and minor re-arrangement of sub-propositions):

(23) $a + 1 \geq 8 \ \wedge \ (a + 1 \ = \ 3b' + 5c' \ \vee \ a + 1 \ = 3b'' + 5c'')$, where
$b' \coloneqq b - 3, c' \coloneqq c + 2, b'' \coloneqq b + 2, c'' \coloneqq c - 1,$
$a + 1,\ b',\ c',\ b'', c'' \in \mathbb{N} \ \cup \{0\}$
$\{14\}$, (17), (20) and (23), constructive dilemma

The inductive premise (14) can now be removed from the premise set and made the antecedent of a conditional of which the consequent is (23), *i.e.*,

J. Randall Miller
jum385@psu.edu
IST 230 (Language, Logic & Discrete Mathematics)
Section 3, Dr. S. Rajtmajer

(24) $(a \geq 8 \wedge a = 3b + 5c) \rightarrow \big(a + 1 \geq 8 \wedge (a + 1 = 3b' + 5c' \vee a + 1 = 3b'' + 5c'')\big)$

$\emptyset$, from (23) by premise deletion

Simultaneous universal and existential generalizations of (24) can now be performed to finally yield a proposition having the desired form of the principal conditional of our inductive proof. To produce (25) I have also made use of the fact that after $aRb \vee aRc$ has been transformed by existential generalization to $\exists x[aRx] \vee \exists y[aRy]$ the variables x and y are placeholder "dummy referents" and the two expressions in which they appear are synonymous, so that the disjunction reduces by the idempotent law to $\exists x[aRx]$:

(25) $\forall n \in \mathbb{N} \cup \{0\}\ \exists j \in \mathbb{N} \cup \{0\}\ \exists k \in \mathbb{N} \cup \{0\}\ \exists j' \in \mathbb{N} \cup \{0\}\ \exists k' \in \mathbb{N} \cup \{0\}$:

$[(n \geq 8 \rightarrow n = 3j + 5k) \rightarrow (n + 1 \geq 8 \rightarrow n + 1 = 3j' + 5k')]$

$\emptyset$, universal/existential generalization of (24)

By the principle of mathematical induction (25) and (13) together entail the final result that:

(26) $\forall n \in \mathbb{N} \cup \{0\}\ \exists j \in \mathbb{N} \cup \{0\}\ \exists k \in \mathbb{N} \cup \{0\}\ [n \geq 8 \rightarrow n = 3j + 5k]$ (*QED*),

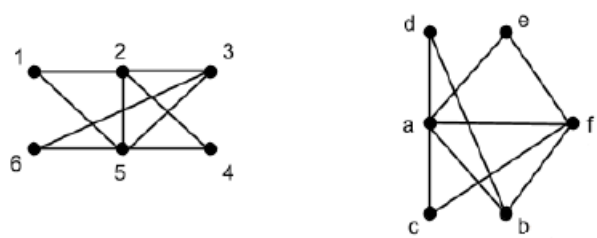
the proposition that was to be proven.

***The proof by mathematical induction has the shortcoming of not showing how, for any given postage $n \geq 8$, to construct that postage from 3-cent and 5-cent stamps. This shortcoming would be avoided by a proof that instead just gave an algorithm for constructing that postage in any case, and demonstrated its adequacy to the enumeration of these cases; such an algorithm is summarized in:

n mod 3	number of 3-cent stamps	number of 5-cent stamps
0	n div 3	0
1	n div 3 – 3	2
2	n div 3 – 1	1

The construction is not always the only one that would work: people who prefer to use a smaller number of stamps can always substitute 3 * (n div 15) 5-cent stamps for 5 * (n div 15) 3-centers.

10. Prove that these two graphs are isomorphic:



J. Randall Miller
jum385@psu.edu
IST 230 (Language, Logic & Discrete Mathematics)
Section 3, Dr. S. Rajtmajer

I will define**** two undirected graphs $G_{numbered} = \{V_{numbered}, E_{numbered}\}$ and $G_{lettered} = \{V_{lettered}, E_{lettered}\}$ to be isomorphic to one another if and only if there exist reciprocal functions $func: V_{numbered} \to V_{lettered}$ and $func^{-1}: V_{lettered} \to V_{numbered}$ such that

$$\forall x_i \in V_{numbered} \forall x_j \in V_{numbered} \left[\{x_i, x_j\} \in E_{numbered} \leftrightarrow \{func(x_i), func(x_j)\} \in E_{lettered}\right]$$

or equivalently, given the requirement that $(func^{-1} \circ func)(x) = x$,

$$\forall y_i \in V_{lettered} \forall y_j \in V_{lettered} \left[\{y_i, y_j\} \in E_{lettered} \leftrightarrow \{func^{-1}(y_i), func^{-1}(y_j)\} \in E_{numbered}\right]$$

The object of this proof then becomes to show that a bijection like this exists. I do so by exhibiting one such bijection; a mapping that satisfies the necessary condition is, I assert:

$$func = \{(1, e), (2, f), (3, b), (4, c), (5, a), (6, d)\}$$

It will be easiest to verify that the defined bijection satisfies the necessary condition and thus that the two graphs are isomorphic if the visual representations of the two undirected graphs in question are replaced with matrix representations in which each vertex of a graph is associated both with a row *i* and a column *j*, and matrix element $a_{ij} = 1$ or $a_{ij} = 0$ according respectively as to whether the pair of vertices $\{v_i, v_j\} \in E$ or $\{v_i, v_j\} \notin E$. Since the graphs are undirected the constructed matrices will be symmetric; such a representation of $G_{numbered}$ is:

vertex:	1	2	3	4	5	6	degree:
1	0	1	0	0	1	0	2
2	1	0	1	1	1	0	4
3	0	1	0	0	1	1	3
4	0	1	0	0	1	0	2
5	1	1	1	1	0	1	5
6	0	0	1	0	1	0	2
degree:	2	4	3	2	5	2	18

and the representation of $G_{lettered}$ whose row and column order corresponds to the mapping of vertices $\{(1, e), (2, f), (3, b), (4, c), (5, a), (6, d)\}$ is:

vertex:	e	f	b	c	a	d	degree:
e	0	1	0	0	1	0	2
f	1	0	1	1	1	0	4
b	0	1	0	0	1	1	3
c	0	1	0	0	1	0	2
a	1	1	1	1	0	1	5
d	0	0	1	0	1	0	2
degree:	2	4	3	2	5	2	18

J. Randall Miller
jum385@psu.edu
IST 230 (Language, Logic & Discrete Mathematics)
Section 3, Dr. S. Rajtmajer

Inspection suffices to confirm that each of the foregoing matrices represents the corresponding graph depicted visually in the problem statement, and is identical to the other. *QED.*

****As I hope was evident from the context, I am using a subscripted 'V' to refer to an undirected graph G's set of vertices, and a subscripted 'E' to refer to its set of edges. The described bijection guarantees that the two vertex sets will be of the same size, but the given definition of isomorphism does not require that a bijection that satisfies its condition be unique, as the mapping may happen to be in the example proof given above; between two different but isomorphic representations of a regular graph there may well be many such bijections.