

A MOORE EXPERIMENT—BASIC FACTS AND PROOFS

We will start with some notation and some assumptions. But first we have two rules of common sense (and common inference):

Common Sense Rule #1. If a statement is known for every a , then one can infer that it is known for any specific a —in other words one can choose (or select) the element to apply the sentence to.

Warning: In contrast if something is known for some a , then we are not free to choose to apply that sentence to a given specific x . For example, if it is known that $\forall a f(a) = 7$, then we know that $f(1) = 7$. On the other hand, if all we know is that $\exists a f(a) = 7$, then we cannot conclude that $f(1) = 7$.

Common Sense Rule #2. If we know that two things are equal, then we can freely substitute one for the other in any well-defined expression, and the two shall be equal too.

For example, if $a = b$ is known, then we know that $\frac{a+x}{y} = \frac{b+x}{y}$.

We will let \mathbb{R} denote the set of **real numbers**, which we will assume as given. We will also assume that we know how to add and multiply two of them, namely if $a, b \in \mathbb{R}$, then there are uniquely determined real numbers given by the sum of a and b , $a + b$, and by their product, $a \times b$.

ARITHMETIC

We will assume the following facts¹ about these operations:

A1	Addition is commutative.	$\forall a \forall b \ a + b = b + a$
A2	Addition is associative.	$\forall a \forall b \forall c \ a + (b + c) = (a + b) + c$
A3	0 is the identity.	$\forall a \ a + 0 = a$
A4	Additive inverses exist.	$\forall a \exists b \text{ such that } a + b = 0$

Things to be proven:

1. $0 + 0 = 0$ **Idempotency of the identity.**
2. $\forall a \forall x \forall y, \text{ if } a + x = a + y, \text{ then } x = y.$ **Cancellation.**

¹ Assumptions will always be boxed, and things to be proven are numbered.

3. $\forall a$, if $a + a = a$, then $a = 0$. **Uniqueness of idempotent.**
4. $\forall a \exists! b$ such that $a + b = 0$. **Uniqueness of inverse.**

The symbol $\exists!$ reads, there is exactly one. One proves uniqueness usually by taking two things that satisfy something, and proving that they are actually equal.

Definition. The b in 4 is then called $-a$, the negative of a . Define **subtraction** by $a - b = a + (-b)$.

5. $\forall a$, $-(-a) = a$. **Negative of negative.**

More assumptions

A5	Multiplication is commutative.	$\forall a \forall b \ a \times b = b \times a$
A6	Multiplication is associative	$\forall a \forall b \forall c \ a \times (b \times c) = (a \times b) \times c$
A7	Multiplication distributes over addition	$\forall a \forall b \forall c \ a \times (b + c) = (a \times b) + (a \times c)$

6. $\forall a$, $a \times 0 = 0$. **Zero annihilates**

A8	1 is the identity.	$\forall a \ a \times 1 = a$
A9	Multiplicative inverses exist.	$\forall a$ if $a \neq 0$, then $\exists b$ such that $a \times b = 1$

7. $1 \times 1 = 1$ **Idempotency of the identity.**

We will often use juxtaposition for multiplication: $ab = a \times b$.

8. $\forall a \forall x \forall y$, if $a \neq 0$, and $ax = ay$, then $x = y$. **Cancellation.**
9. $\forall a$, $a + a = 2a$. **2 is two**
10. $\forall a$, if $a \neq 0$ and $aa = a$, then $a = 1$. **Uniqueness of idempotent.**
11. $\forall a$, if $a = -a$, then $a = 0$.

Definition. aa is denoted by a^2 . Similarly, $a^2a = a^3$ by definition. This definition can be obviously extended.

12. $\forall a$ if $a \neq 0$, then $\exists! b$ such that $ab = 1$ **Uniqueness of inverse.**

The b in **12** is then called $\frac{1}{a} = a^{-1}$, the **reciprocal** of a .

Define **division** by $a \div b = ab^{-1} = a\left(\frac{1}{b}\right)$.

Unless necessary, the (universal) quantifiers will be tacitly implied rather than explicitly stated.

13. $(a^{-1})^{-1} = a$ Inverse of inverse.

14. $(-a)b = -(ab)$.

15. $a(-b) = -(ab)$.

16. $(-1)1 = -1$.

17. $(-1)(-1) = 1$. Minus times a minus.

18. $(-a)(-b) = ab$.

COMPLEX ARITHMETIC

We let \mathbb{C} denote the set of complex numbers, $\{a + b\mathbf{i} \mid a, b \in \mathbb{R}\}$. We make the following assumptions:

C1	Uniqueness of form.	$\forall a \forall b \forall c \forall d$ if $a + b\mathbf{i} = c + d\mathbf{i}$, then $a = c$ and $b = d$.
-----------	----------------------------	---

Definition. Let $z, w \in \mathbb{C}$ with $z = a + b\mathbf{i}$ and $w = c + d\mathbf{i}$. Then

$$z + w = (a + c) + (b + d)\mathbf{i},$$

$$zw = (ac - bd) + (ad + cb)\mathbf{i}.$$

One can think of every real number as a complex number by simply letting $a = a + 0\mathbf{i}$.

19. $z + w = w + z$ Addition is commutative.

20. $z + (w + u) = (z + w) + u$ Addition is associative.

21. $z + 0 = z$ 0 is the identity.

22. $\forall z \exists w$ such that $z + w = 0$ **Additive inverses exist.**
23. $z \times w = w \times z$ **Multiplication is commutative.**
24. $z \times (w \times u) = (z \times w) \times u$ **Multiplication is associative**
25. $z \times (w + u) = (z \times w) + (z \times u)$ **Multiplication distributes over addition**
26. $z \times 0 = 0$ **Zero annihilates**
27. $z \times 1 = z$ **1 is the identity.**
28. If $z \neq 0$, then $\exists w$ such that $z \times w = 1$
Multiplicative inverses exist.

Definition. If $z = a + bi$, then the conjugate of z , \bar{z} is defined by $\bar{z} = a - bi$.

29. $\overline{z + w} = \bar{z} + \bar{w}$ **Conjugate of a sum is the sum of the conjugates.**
30. $\overline{z \times w} = \bar{z} \times \bar{w}$ **Conjugate of a product is the product of the conjugates.**
31. $\overline{\bar{z}} = z$ **Conjugate of conjugate.**

ORDER

In this section we return to the real numbers \mathbb{R} and we will look at some of the basic properties of order among them.

We will let \mathbf{P} denote the set of **positive real numbers**. For the time being there is no clear meaning to what this set is—but we will delineate its meaning by the assumptions we make about it. We let $\mathbf{N} = -\mathbf{P} = \{x \mid -x \in \mathbf{P}\}$, thus $x \in \mathbf{P}$ if and only if $-x \in \mathbf{N}$, and refer to this set as the set of **negative real numbers**.

01	the sum of two elements in \mathbf{P} is in \mathbf{P}	if $x, y \in \mathbf{P}$, then $x + y \in \mathbf{P}$
02	the product of two elements in \mathbf{P} is in \mathbf{P}	if $x, y \in \mathbf{P}$, then $xy \in \mathbf{P}$
03	\mathbf{P} and \mathbf{N} have nothing in common	$\mathbf{P} \cap \mathbf{N} = \emptyset$
04	every real number is either 0 or it belongs to \mathbf{P} or it belong to \mathbf{N}	$\mathbf{P} \cup \mathbf{N} \cup \{0\} = \mathbb{R}$

$x < y < z$ or $x < z < y$ or $y < x < z$ or $y < z < x$ or $z < y < x$ or $z < x < y$.

49. If $x < y$, then $x + z < y + z$. **Addition preserves order**
50. If $x < y$ and $z > 0$, then $xz < yz$. **Multiplication by positives preserves order**
51. If $x < y$ and $z < 0$, then $xz > yz$. **Multiplication by negatives reverses order**
52. If $x > 1$, then $x^2 > x$.
53. If $x > 0$ and $x < 1$, then $x^2 < x$.
54. If $x < 0$, then $x^3 < 0$.
55. If $x > 1$, then $0 < x^{-1} < 1$.
56. If $0 < x < y$, then $0 < y^{-1} < x^{-1}$. **Reciprocation**
57. If $0 > x > y$, then $0 > y^{-1} > x^{-1}$.

DIVISIBILITY

We start by considering several important subsets of the real numbers. We will let \mathbb{Z} denote the set of integers, $0, \pm 1, \pm 2, \pm 3, \dots$, while \mathbb{N} denotes the set of nonnegative integers, $0, 1, 2, 3, \dots$, in other words, if $n \in \mathbb{Z}$, then $n \in \mathbb{N}$ if and only if $n \geq 0$. The set \mathbb{Q} will denote the set of rational numbers which are ratios of two integers, $\frac{a}{b}$, where $a, b \in \mathbb{Z}$ and, of course, $b \neq 0$.

D1	The sum of two integers is an integer.	\mathbb{Z} is closed under addition: if $n, m \in \mathbb{Z}$, then $m + n \in \mathbb{Z}$
D2	The product of two integers is an integer	\mathbb{Z} is closed under multiplication: if $n, m \in \mathbb{Z}$, then $mn \in \mathbb{Z}$
D3	The negative of an integer is an integer	\mathbb{Z} is closed under negation: if $m \in \mathbb{Z}$, then $-m \in \mathbb{Z}$

58. The difference of two integers is an integer, in other words, \mathbb{Z} is closed under subtraction.
59. The sum of two nonnegative integers is a nonnegative integer, in other words, \mathbb{N} is closed under addition.

60. **The product of two nonnegative integers is a nonnegative integer**, in other words, \mathbb{N} is closed under multiplication.
61. Let $\frac{a}{b}, \frac{c}{d}$ be rational numbers, then $\frac{a}{b} = \frac{c}{d}$ if and only if $ad = bc$.
62. **The sum of two rationals is a rational**; in other words, \mathbb{Q} is closed under addition.
63. **The difference of two rationals is a rational**; in other words, \mathbb{Q} is closed under subtraction.
64. **The product of two rationals is a rational**; in other words, \mathbb{Q} is closed under multiplication.
65. **The quotient of two rationals is a rational**; in other words, \mathbb{Q} is closed under division.
66. If $m \in \mathbb{N}$ and $m \neq 0$, then $m \geq 1$.
67. If $m \in \mathbb{Z}$ and $m > 1$, then $\frac{1}{m} \notin \mathbb{Z}$.

Definition. Let a and b be integers with a nonzero. We say a **divides** b if $ax = b$ for some integer x . In symbols, $a | b$ reads a divides b . If a divides b then we say a **is a divisor of** b , or equivalently, b **is a multiple of** a .

68. Let a and b be integers with a nonzero. Then, $a | b$ if and only if $\frac{b}{a} \in \mathbb{Z}$.

Throughout assume a and b are positive integers.

69. $a | a$. **Reflexivity**
70. If $a | b$ and $b | a$, then $a = b$. **Antisymmetry**
71. If $a | b$ and $b | c$, then $a | c$. **Transitivity**
72. 1 is a divisor of a . **Minimum**
73. If 1 is a multiple of a , then $a = 1$.

74. 0 is a multiple of a . Maximum
75. If $a \mid b$, then $a \leq b$.
76. Suppose a is a multiple of n , then so is ab .
77. $a \mid b$ if and only if $-a \mid b$.
78. $a \mid b$ if and only if $-a \mid -b$.
79. Suppose a and b are multiples of n . Then $ax + by$ is also a multiple of n for any integers x and y .

Definition. Let a and b be integers. A positive integer n is a **common divisor** of a and b if it divides both of them, *i.e.*, $n \mid a$ and $n \mid b$. If d is a common divisor of a and b , then d is called a **greatest common divisor (g.c.d)** if and only $d \geq n$ for any common divisor n of a and b .

80. The g.c.d. of a and b , if it exists, is uniquely determined.

Given the last proposition, we can now refer to ~~the~~ versus **a** g.c.d.

81. The g.c.d. of a and 0 exists and it equals a .

Due to the last proposition, we will concentrate on nonzero integers from now on. We will axiomatize the existence of the g.c.d.

D4	Any two positive integers have a g.c.d.	$\exists d \ d = \text{g.c.d.}(a, b)$
----	---	---------------------------------------

We will use $a \wedge b$ to denote the $\text{g.c.d.}(a, b)$

82. $a \wedge b = b \wedge a$.
83. $a \wedge b = (a - nb) \wedge b$ for any integer n .

Definition. Two integers a and b are **relatively prime** if their g.c.d. is 1, $a \wedge b = 1$.

84. a and 1 are relatively prime.
85. If a is relatively prime to a and a is nonnegative, then $a = 1$.
86. If a is a multiple of b , and a and n are relatively prime, then so are b and n .

D5	The g.c.d. is a linear combination.	$\exists x \exists y \ x, y \in \mathbb{Z}$ such that $a \wedge b = xa + yb$
----	-------------------------------------	---

87. The g.c.d. is a multiple of any common divisor: if n is a common divisor of a and b , then $n \mid a \wedge b$.
88. If d is a common divisor of a and b , and $d = xa + yb$ for some integers x and y , then $d = a \wedge b$.
89. Let $a, b \in \mathbb{Z}$. Then $a \wedge b = 1$ if and only if there exist integers x and y such that $xa + yb = 1$.
90. If $a \wedge n = 1$, then $a^k \wedge n = 1$ for any positive integer k .
91. If $a \wedge n = 1$, then $a^k \wedge n^j = 1$ for any positive integers k and j .

Upper Case Greek	Lower Case Greek	Name	Roman Symbol
A	α	alpha	A
B	β	beta	B
X	χ	chi	C
Δ	δ	delta	D
E	ε	epsilon	E
Φ	ϕ	phi	F
Γ	γ	gamma	G
H	η	eta	H
I	ι	iota	I
	φ	alternate phi	j
	ϑ	alternate sigma	J
K	κ	kappa	K
Λ	λ	lambda	L
M	μ	mu	M
N	ν	nu	N
O	\omicron	omicron	O
Π	π	pi	P
Θ	θ	theta	Q
P	ρ	rho	R
Σ	σ	sigma	S
T	τ	tau	T
Y	υ	upsilon	U
ζ	ϖ		V
Ω	ω	omega	W
Ξ	ξ	xi	X
Ψ	ψ	psi	Y
Z	ζ	zeta	Z
Other alphabets			
Hebrew	\aleph	aleph	
Fraktur	\mathfrak{C}	c	C
	\mathfrak{F}	f	F
	\mathfrak{G}	g	G
	\mathfrak{K}	k	K
	\mathfrak{M}	m	M
	\mathfrak{P}	p	P
	\mathfrak{S}	s	S
	\mathfrak{T}	t	T
	\mathfrak{A}	a	A

INDEX

2-path, 111, 112

3-path, 111

A

a is congruent to b , 93

a is joined to b , 108

addition preserves order, 133

addition, 6, 128, 131

adjacency matrix, 108, 110, 118

algebra of congruences, 94

anagram, 87

and, 12, 13, 38, 40, 46

antisymmetric, 111, 118

antisymmetry, 112, 133, 135

argument, 4, 7

arithmetic progressions, 18

arrow, 108

assignment, 64

associative, 73, 128, 131

asymptotic, 124

asymptotics, 124

at least, 70

at most, 70

average, 58

B

balls, 82

Bernoulli's inequality, 24

big-Oh, 125

bijection, 70

binomial coefficients, 27

Binomial Theorem, 31, 84

birthday, 63, 64, 69, 76, 77

black box, 63

block triangular form, 109

buckets, 82

C

calendar, 103

cancellation, 129

Cardano, 48

cardinality, 32, 63

Cartesian, 3, 4, 66

casting-out-nines, 95

ceiling, 74

Chinese Remainder Theorem, 102

choosing, 46

clock, 89

codomain, 63, 69

committee, 46

commutative, 73, 128, 131

complement, 35

complete graph, 106

complete set of residues, 96

complex number, 3, 4, 6

complex numbers, 130

components, 114

composition, 72

conditional probability, 62

conditional, 10

congruence, 93

congruences, 94

congruent, 93

conjugate, 5, 131

connected, 114, 115, 116

contrapositive, 12, 22

converse, 11, 22

counter-clockwise, 90

counting function, 74

counting numbers, 1

counting, 65

cross, 40, 66

cube, 22

cubes, 92

cycle, 111, 115

D

D'Alembert, 50

decimal expansion, 89

decimal, 2

DeMoivre's Theorem, 8

DeMorgan's Laws, 13

denominator, 1

dice, 47

difference, 17

digraph, 108, 110

direct product, 66

directed graph, 108

disjoint, 34, 35

distance, 3

distributes, 129, 131

distributive law, 38

distributivity, 24
 divides, 135
 divisor, 44, 135
 domain, 63, 68
 dominoes, 56, 59
 double counting, 32
 dual notion, 120

E

edges, 105
 element, 33
 ellipsis, 17
 empty set, 33
 equal, 33
 equally feasible outcomes, 48, 57
 equals added to equals, 94
 equals multiplied by equals, 94
 equivalence class, 113
 equivalence relation, 113
 Euler, 24
 Euler's constant, 127
 Every horse is white., 14
 Existence of Cycles, 115
 expectation, 59
 expected value, 58

F

factorial, 23, 43
 Fermat prime, 32
 Fermat, 57
 Fibonacci numbers, 100
 Fibonacci sequence, 25
 Fibonacci, 92
 first counting principle, 34
 floor, 74
 for every a, 128
 for every, 14, 69
 fractional part, 75
 function, 63
 functions & equivalence relations, 114

G

g.c.d, 135
 Galileo, 47
 Gauss, 3, 6, 8, 18, 93, 124
 graph, 66, 108, 111
 greatest common divisor, 135

Gregorian Calendar, 103

H

Hasse diagram, 119
 hexagesimals, 2
 Hindu-Arabic, 1
 House of Representatives, 46

I

idempotency, 129
 idempotent, 129
 identity, 128, 129, 131
 if and only if, 12
 if...then, 21, 23
 image, 74
 in parallel, 101
 in series, 102
 Incas, 1
 inclusion-exclusion principle, 39, 81
 inclusive, 13
 increasing function, 64
 induction, 20
 influence network, 109
 injective, 67
 in order, 117
 input, 63
 integers, 2
 intersection, 33
 inverse image, 73
 inverses, 128, 131
 irrational, 2
 irreflexive, 110, 118
 Irreflexivity, 112, 133
 ISBN, 96, 97

L

l.c.m., 101
 least common multiple, 101
 Leibniz, 50
 length, 4, 7
 Liar's Paradox, 16
 loop, 110

M

main diagonal, 111
 mapping, 64
 maps to, 63

mathematical induction, 20
 matrices, 9
 matrix multiplication, 63, 65
 matrix, 106, 123
 maximal, 120
 maximum, 120, 135
 minimal, 120
 minimum, 120, 135
 minus times a minus, 130
MISSISSIPPI, 87
 mod 11, 96, 97
 mod 9, 95
 mod function, 91
 modulus, 4, 94
 multinomial coefficients, 86
 Multinomial Theorem, 87
 multiple choice, 51
 multiple, 21, 22, 39, 135
 multiplication by positives preserves
 order, 133
 multiplication, 7, 129, 131

N

n choose *k*, 27
 natural numbers, 1
 negation, 13
 negative numbers, 2
 negative real, 132
 negative, 129
 network, 108
 Newton's expression, 30
 nodes, 105
n - set, 27, 32
 number of Edges, 115
 number of Functions, 66
 numerator, 1

O

odd, 22
 odds, 58, 77
 one-to-one correspondence, 70
 one-to-one, 67, 72
 onto functions, 80
 onto, 68, 72, 78, 80
 ontoness, 68, 69
 operator, 64
 or, 12, 13, 39, 40, 46
 order, 117

ordered pairs, 110
 ordered-pair, 107
 outcomes, 48
 output, 63

P

parallelogram law, 6
 partial order, 118
 partition, 34, 113, 114, 121
 partitions, 82, 122
 Pascal, 57
 Pascal's recursion, 28
 Pascal's triangle, 29, 30
 path, 111
 permutation, 70, 71, 72
 Petersen graph, 106, 107
 pigeon hole II, 71
 pigeon-hole principle, 70
 poker, 52
 polar form, 7
 polar, 4
 poset, 118
 positive integers, 1
 positive rationals, 1
 positive real numbers, 132
 postorder, 117
 power set, 65, 121
 preorder, 117
 president, 67
 Prime Number Theorem, 124
 prime, 11, 24, 37, 98, 100
 principle of inclusion-exclusion, 37
 probability, 50, 51
 probability, 76
 product of two sets, 40
 pronouns, 10
 property, 32
 Ptolemy's theorem, 4
 pure imaginary, 6
 Pythagorean theorem, 3

R

range, 64, 69
 rational numbers, 2
 real numbers, 2, 65, 128
 reciprocating, 8
 recursion, 25
 recursive, 25

reflexive, 110, 118
 reflexivity, 132, 135
 relation, 105, 108
 relatively prime, 99, 136
 restriction, 68
 Roberval, 57
 root a tree, 116
 roots of unity, 9
 round, 74
 round-down, 74
 round-off, 74
 round-up, 74
 rule of product, 43
 rule of sum, 34

S

Scheherazade, 89
 second counting principle, 43
 selections, 84
 self-referral, 16
 senate, 46
 sentence, 10
 sequence, 17
 series, 17
 set, 32, 108
 size, 34
 slower, 125
 squares, 92
 squaring, 65, 69, 74
 standard clock, 90
 Stirling number of the second kind, 79
 Stirling Recursion, 80
 Stirling's Formula, 124, 127
 subset, 33, 41
 suit, 52
 sum, 17, 26
 surjective, 68
 symmetric, 110, 111

T

the average of a sum, 59
 there exists a horse that is white., 14
 there exists, 14
 Thousand Nights and a Night, 89
 total order, 118, 132
 transformation, 64
 transitive, 112, 118
 transitivity, 93, 133, 135

transpose, 110
 tree diagram, 40
 tree, 111, 114, 116
 triangular numbers, 18, 21
 True-False, 51, 52
 two things are equal, 128

U

U.S. Congress, 46
 union, 33, 34
 unit circle, 4

V

Venn diagrams, 33, 35
 vertices, 105, 113

W

whole numbers, 2

X

$x \bmod n$, 91
 x modulo 6, 91
 x modulo n , 91

Z

zero, 1