

Contents

0	Introduction	1
	Number Theory and Mathematical Thinking	1
	Note on the approach and organization	2
	Methods of thought	3
	Acknowledgments	4
1	Divide and Conquer	7
	Divisibility in the Natural Numbers	7
	Definitions and examples	7
	Divisibility and congruence	9
	The Division Algorithm	14
	Greatest common divisors and linear Diophantine equations	16
	Linear Equations Through the Ages	23
2	Prime Time	27
	The Prime Numbers	27
	Fundamental Theorem of Arithmetic	28
	Applications of the Fundamental Theorem of Arithmetic	32
	The infinitude of primes	35
	Primes of special form	37
	The distribution of primes	38
	From Antiquity to the Internet	41
3	A Modular World	43
	Thinking Cyclically	43
	Powers and polynomials modulo n	43
	Linear congruences	48

	Systems of linear congruences: the Chinese Remainder Theorem	50
	A Prince and a Master	51
4	Fermat's Little Theorem and Euler's Theorem	53
	Abstracting the Ordinary	53
	Orders of an integer modulo n	54
	Fermat's Little Theorem	55
	An alternative route to Fermat's Little Theorem	58
	Euler's Theorem and Wilson's Theorem	59
	Fermat, Wilson and ... Leibniz?	62
5	Public Key Cryptography	65
	Public Key Codes and RSA	65
	Public key codes	65
	Overview of RSA	65
	Let's decrypt	66
6	Polynomial Congruences and Primitive Roots	73
	Higher Order Congruences	73
	Lagrange's Theorem	73
	Primitive roots	74
	Euler's ϕ -function and sums of divisors	77
	Euler's ϕ -function is multiplicative	79
	Roots modulo a number	81
	Sophie Germain is Germane, Part I	84
7	The Golden Rule: Quadratic Reciprocity	87
	Quadratic Congruences	87
	Quadratic residues	87
	Gauss' Lemma and quadratic reciprocity	91
	Sophie Germain is germane, Part II	95
8	Pythagorean Triples, Sums of Squares, and Fermat's Last Theorem	99
	Congruences to Equations	99
	Pythagorean triples	99
	Sums of squares	102
	Pythagorean triples revisited	104
	Fermat's Last Theorem	104
	Who's Represented?	106
	Sums of squares	106

Sums of cubes, taxicabs, and Fermat’s Last Theorem	107
9 Rationals Close to Irrationals and the Pell Equation	109
Diophantine Approximation and Pell Equations	109
A plunge into rational approximation	110
Out with the trivial	114
New solutions from old	115
Securing the elusive solution	116
The structure of the solutions to the Pell equations	117
Bovine Math	119
10 The Search for Primes	123
Primality Testing	123
Is it prime?	123
Fermat’s Little Theorem and probable primes	124
AKS primality	126
Record Primes	127
A Mathematical Induction: The Domino Effect	129
The Infinitude Of Facts	129
Gauss’ formula	129
Another formula	131
On your own	132
Strong induction	133
On your own	134
Index	135
About the Authors	139