

# Contents

**\* denotes optional material**

<b>Preface</b>	ix
<b>1 Introduction</b>	1
1.1 One theme, one unique researcher, and discovery detectives	2
1.2 How to use this book	3
1.3 Number theory cookies	4
<b>2 Sophie Germain, Number Theory, and Fermat's Last Theorem</b>	7
2.1 Sophie Germain, hidden mathematician	7
2.2 Number theory, queen of mathematics	10
2.3 Fermat's last theorem, puzzle of centuries	17
<b>3 Germain's Plan to Prove Fermat's Last Theorem</b>	21
3.1 The practice of being a detective	21
3.2 Residues	26
3.3 Primes in arithmetic progressions	29
3.4 Power residues	32
3.5 Consecutivity of power residues	35
<b>4 Fermat's Last Theorem for Exponent Four</b>	45
4.1 Pythagorean triples	45
4.2 Uniqueness of prime factorization	51
4.3 Euler's proof for exponent four	51
4.4 Proofs of Euclid's lemma on prime divisibility	58
4.4.1 Fermat's method of descent revisited	58
4.4.2 The Euclidean algorithm and Bézout equation	59
4.4.3 How did Euclid (try to) prove his lemma?	63
4.4.4 Integral linear combinations	68
4.5 Divisibility, powers, roots, and equivalences	69
<b>5 Germain's Grand Plan and a Letter to Gauss</b>	71
5.1 Inverse residues	71
5.2 Germain's claims in 1819 to Gauss	72
5.3 The grand plan understood	78
5.4 Large size of solutions "frightens the imagination"	79

<b>6</b>	<b>Congruence, Germain's Basic Lemma, Systems of Linear Congruences, and Higher Power Congruences</b>	81
6.1	Congruence and its properties	82
6.2	Germain's basic lemma	84
6.3	*Linear congruences and the Chinese remainder theorem	85
6.3.1	A single first degree congruence	85
6.3.2	Systems: The Chinese remainder theorem and an application	87
6.3.3	Generalizing the Chinese remainder theorem	92
6.4	*Higher power congruences, Wilson's theorem, Fermat's theorem, and $\sqrt{-1} \pmod p$ à la Dirichlet	96
<b>7</b>	<b>Primitive Roots</b>	99
7.1	Fermat's theorem	101
7.2	*The RSA cryptosystem	106
7.3	Orders of units and Euler's theorem	108
7.4	Lagrange's theorem on modular roots of polynomials	113
7.5	*Wilson's theorem à la Lagrange	115
7.6	Orders of units and counting roots of polynomials	116
7.7	Counting elements of each order with Euler	117
7.8	Primitive roots exist	118
7.9	*Wilson's theorem à la Euler	121
7.10	Powers, roots, orders, and Euler's criterion	121
<b>8</b>	<b>Germain Carrying out Her Grand Plan</b>	125
<b>9</b>	<b>Large Size of Solutions and Sophie Germain's Theorem</b>	137
<b>10</b>	<b>The Demise of the Grand Plan: A Letter to Legendre</b>	149
<b>11</b>	<b>*Prime Patterns in Quadratic Forms</b>	155
11.1	Fermat's amazing claims	155
11.2	Euler's discoveries on prime divisors of quadratic forms	156
11.3	The quadratic reciprocity law: Legendre, Gauss, and Eisenstein's geometric proof	161
11.4	Representing primes by quadratic forms: From Fermat via Euler to Lagrange	169
<b>A</b>	<b>*How Fermat Discovered his Theorem, and Other Divisibility Delights</b>	181
A.1	Perfect numbers, Mersenne numbers, and Fermat's discovery about primes	181
A.2	Fermat numbers and primes	190
A.3	Prime divisors of sums of powers	191
A.4	More on prime divisors of sums and differences of powers	192
	<b>References</b>	195
	<b>Credits</b>	199
	<b>Index</b>	201