

Chapter 1 Fermat

1

1.1 Fermat and his “Last Theorem.” Statement of the theorem. History of its discovery. **1.2 Pythagorean triangles.** Pythagorean triples known to the Babylonians 1000 years before Pythagoras. **1.3 How to find Pythagorean triples.** Method based on the fact that the product of two relatively prime numbers can be a square only if both factors are squares. **1.4 The method of infinite descent.** **1.5 The case $n=4$ of the Last Theorem.** In this case the proof is a simple application of infinite descent. General theorem reduces to the case of prime exponents. **1.6 Fermat’s one proof.** The proof that a Pythagorean triangle cannot have area a square involves elementary but very ingenious arguments. **1.7 Sums of two squares and related topics.** Fermat’s discoveries about representations of numbers in the form $n = x^2 + ky^2$ for $k = 1, 2, 3$. The different pattern when $k = 5$. **1.8 Perfect numbers and Fermat’s theorem.** Euclid’s formula for perfect numbers leads to the study of Mersenne primes $2^n - 1$ which in turn leads to Fermat’s theorem $a^p - a \equiv 0 \pmod{p}$. Proof of Fermat’s theorem. Fermat numbers. The false conjecture that $2^{32} + 1$ is prime. **1.9 Pell’s equation.** Fermat’s challenge to the English. The cyclic method invented by the ancient Indians for the solution of $Ax^2 + 1 = y^2$ for given nonsquare A . Misnaming of this equation as “Pell’s equation” by Euler. Exercises: Proof that Pell’s equation always has an infinity of solutions and that the cyclic method produces them all. **1.10 Other number-theoretic discoveries of Fermat.** Fermat’s legacy of challenge problems and the solutions of these problems at the hands of Lagrange, Euler, Gauss, Cauchy, and others.

Chapter 2 Euler

39

2.1 Euler and the case $n=3$. Euler never published a correct proof that $x^3 + y^3 \neq z^3$ but this theorem can be proved using his techniques. **2.2 Euler’s proof of the case $n=3$.** Reduction of Fermat’s Last Theorem in the case $n=3$ to the statement that $p^2 + 3q^2$ can be a cube (p and q relatively prime) only if there exist a and b such that $p = a^3 - 9ab^2$, $q = 3a^2b - 3b^3$.

2.3 Arithmetic of surds. The condition for p^2+3q^2 to be a cube can be written simply as $p+q\sqrt{-3}=(a+b\sqrt{-3})^3$, that is, $p+q\sqrt{-3}$ is a cube. Euler's fallacious proof, using unique factorization, that this condition is necessary for $p^2+3q^2=\text{cube}$. **2.4 Euler on sums of two squares.** Euler's proofs of the basic theorems concerning representations of numbers in the forms x^2+y^2 and x^2+3y^2 . Exercises: Numbers of the form x^2+2y^2 . **2.5 Remainder of the proof when $n=3$.** Use of Euler's techniques to prove $x^3+y^3\neq z^3$. **2.6 Addendum on sums of two squares.** Method for solving $p=x^2+y^2$ when p is a prime of the form $4n+1$. Solving $p=x^2+3y^2$ and $p=x^2+2y^2$.

Chapter 3 From Euler to Kummer

59

3.1 Introduction. Lagrange, Legendre, and Gauss. **3.2 Sophie Germain's theorem.** Sophie Germain. Division of Fermat's Last Theorem into two cases, Case I (x, y , and z relatively prime to the exponent p) and Case II (otherwise). Sophie Germain's theorem is a sufficient condition for Case I. It easily proves Case I for all small primes. **3.3 The case $n=5$.** Proof that $x^5+y^5\neq z^5$. The joint achievement of Dirichlet and Legendre. General technique is like Euler's proof that $x^3+y^3\neq z^3$ except that p^2-5q^2 a fifth power implies $p+q\sqrt{5}=(a+b\sqrt{5})^5$ only under the additional condition $5|q$. **3.4 The cases $n=14$ and $n=7$.** These proofs, by Dirichlet and Lamé respectively, are not explained here. To go further and prove Fermat's Last Theorem for larger exponents clearly requires new techniques. Exercise: Dirichlet's proof of the case $n=14$.

Chapter 4 Kummer's theory of ideal factors

76

4.1 The events of 1847. Lamé's "proof" of Fermat's Last Theorem. Liouville's objection. Cauchy's attempts at a proof. Kummer's letter to Liouville. Failure of unique factorization. Kummer's new theory of ideal complex numbers. **4.2 Cyclotomic integers.** Basic definitions and operations. The norm of a cyclotomic integer. The distinction between "prime" and "irreducible." Division using the norm. **4.3 Factorization of primes $p\equiv 1 \pmod{\lambda}$.** Derivation of necessary and sufficient conditions for a cyclotomic integer to be a prime factor of such a prime p . **4.4 Computations when $p\equiv 1 \pmod{\lambda}$.** Explicit factorizations of such primes for small values of p and λ . Kummer's factorizations for $\lambda\leq 19$ and $p\leq 1000$. Impossibility of factorization when $\lambda=23$ and $p=47$. The idea behind Kummer's "ideal" prime factors. **4.5 Periods.** The conjugation $\sigma:\alpha\rightarrow\alpha^\gamma$ corresponding to a primitive root $\gamma \pmod{\lambda}$. A cyclotomic integer is made up of periods of length f if and only if it is invariant under σ^e where $ef=\lambda-1$. **4.6 Factorization of primes $p\not\equiv 1 \pmod{\lambda}$.** If f is the exponent of $p \pmod{\lambda}$ and if $h(\alpha)$ is any prime factor of p then the periods of length f are all congruent to integers $\pmod{h(\alpha)}$. This makes it easy to test cyclotomic integers made up of periods for divisibility by $h(\alpha)$. **4.7 Computations when $p\not\equiv 1 \pmod{\lambda}$.** Explicit factorizations for small values of p and λ . **4.8 Extension of the divisibility test.** Testing arbitrary cyclotomic integers—not just those made up of periods—for divisibility by a given prime cyclotomic integer $h(\alpha)$. **4.9 Prime divisors.** The tests for divisibility by prime factors exist in all cases, even those in which there is no prime factor. This is the basis for the definition of "ideal" prime factors or prime divisors. Inadequacy of Kummer's original proof of the basic proposition. **4.10 Multiplicities and the exceptional prime.** Definition of the multiplicity

with which a prime divisor divides a cyclotomic integer. The one prime divisor $(1 - \alpha)$ of λ . **4.11 The fundamental theorem.** A cyclotomic integer $g(\alpha)$ divides another $h(\alpha)$ if and only if every prime divisor which divides $g(\alpha)$ divides $h(\alpha)$ with multiplicity at least as great. **4.12 Divisors.** Definition of divisors. Notation. **4.13 Terminology.** A divisor is determined by the set of all things that it divides. "Ideals." **4.14 Conjugations and the norm of a divisor.** Conjugates of a divisor. Norm of a divisor as a divisor and as an integer. There are $N(A)$ classes of cyclotomic integers mod A . The Chinese remainder theorem. **4.15 Summary.**

Chapter 5 Fermat's Last Theorem for regular primes 152

5.1 Kummer's remarks on quadratic integers. The notion of equivalence of divisors. Kummer's allusion to a theory of divisors for quadratic integers $x + y\sqrt{D}$ and its connection with Gauss's theory of binary quadratic forms. **5.2 Equivalence of divisors in a special case.** Analysis of the question "Which divisors are divisors of cyclotomic integers?" in a specific case. **5.3 The class number.** Definition and basic properties of equivalence of divisors. Representative sets. Proof that the class number is finite. **5.4 Kummer's two conditions.** The types of arguments used to prove Fermat's Last Theorem for the exponents 3 and 5 motivate the singling out of the primes λ for which (A) the class number is not divisible by λ and (B) units congruent to integers mod λ are λ th powers. Such primes are called "regular." **5.5 The proof for regular primes.** Kummer's deduction of Fermat's Last Theorem for regular prime exponents. For any unit $e(\alpha)$, the unit $e(\alpha)/e(\alpha^{-1})$ is of the form α^r . **5.6 Quadratic reciprocity.** Kummer's theory leads not only to a proof of the famous quadratic reciprocity law but also to a derivation of the statement of the law. Legendre symbols. The supplementary laws.

Chapter 6 Determination of the class number 181

6.1 Introduction. The main theorem to be proved is Kummer's theorem that λ is regular if and only if it does not divide the numerators of the Bernoulli numbers $B_2, B_4, \dots, B_{\lambda-3}$. **6.2 The Euler product formula.** Analog of the formula for the case of cyclotomic integers. The class number formula is found by multiplying both sides by $(s-1)$ and evaluating the limit as $s \downarrow 1$. **6.3 First steps.** Proof of the generalized Euler product formula. The Riemann zeta function. **6.4 Reformulation of the right side.** The right side is equal to $\zeta(s)L(s, \chi_1)L(s, \chi_2) \cdots L(s, \chi_{\lambda-2})$ where the χ 's are the nonprincipal characters mod λ . **6.5 Dirichlet's evaluation of $L(1, \chi)$.** Summation by parts. $L(1, \chi)$ as a superposition of the series for $\log(1/(1 - \alpha^j))$, $j = 1, 2, \dots, \lambda - 1$. Explicit formulas for $L(1, \chi)$. **6.6 The limit of the right side.** An explicit formula. **6.7 The nonvanishing of L -series.** Proof that $L(1, \chi) \neq 0$ for the χ 's under consideration. **6.8 Reformulation of the left side.** In the limit as $s \downarrow 1$, the sum of $N(A)^{-s}$ over all divisors A in a divisor class is the same for any two classes. Program for the evaluation of their common limit. **6.9 Units: The first few cases.** Explicit derivation of all units in the cases $\lambda = 3, 5, 7$. Finite-dimensional Fourier analysis. Implicit derivation of the units in the case $\lambda = 11$. Second factor of the class number. **6.10 Units: The general case.** Method for finding, at least in principle, all units. Sum over all principal divisors written in terms of a sum over a certain set of cyclotomic integers. **6.11 Evaluation of the integral.** Solution of a problem in integral calculus. **6.12**

Comparison of the integral and the sum. In the limit to be evaluated, the sum can be replaced by the integral. **6.13 The sum over other divisor classes.** Proof that, in the limit, the sum over any two divisor classes is the same. **6.14 The class number formula.** Assembling of all the pieces of the preceding sections to give the explicit formula for the class number. **6.15 Proof that 37 is irregular.** Simplifications of the computation of the first factor of the class number. Bernoulli numbers and Bernoulli polynomials. **6.16 Divisibility of the first factor by λ .** Generalization of the techniques of the preceding section to show that λ divides the first factor of the class number if and only if it divides the numerator of one of the Bernoulli numbers $B_2, B_4, \dots, B_{\lambda-3}$. **6.17 Divisibility of the second factor by λ .** Proof that λ divides the second factor of the class number only if it also divides the first factor. **6.18 Kummer's lemma.** (A) implies (B). **6.19 Summary.**

Chapter 7 Divisor theory for quadratic integers

245

7.1 The Prime divisors. Determination of what the prime divisors must be if there is to be a divisor theory for numbers of the form $x + y\sqrt{D}$. Modification of the definition of quadratic integers in the case $D \equiv 1 \pmod{4}$. **7.2 The divisor theory.** Proof that the divisors defined in the preceding section give a divisor theory with all the expected properties. Equivalence of divisors. **7.3 The sign of the norm.** When $D > 0$ the norm assumes negative as well as positive values. In this case a divisor with norm -1 is introduced. **7.4 Quadratic integers with given divisors.** Unlike the cyclotomic case, for quadratic integers there is a simple algorithm for determining whether a given divisor is principal and, if so, of finding all quadratic integers with this divisor. It is, in essence, the cyclic method of the ancient Indians. Proof of the validity of the algorithm in the case $D < 0$. Exercises: Use of 2×2 matrices to streamline the computations of the cyclic method. **7.5 Validity of the cyclic method.** Proof in the case $D > 0$. Computation of the fundamental unit. **7.6 The divisor class group: examples.** Explicit derivation of the divisor class group for several values of D . **7.7 The divisor class group: a general theorem.** Proof that two divisors are equivalent only if application of the cyclic method to them yields the same period of reduced divisors. This simplifies the derivation of the divisor class group. **7.8 Euler's theorems.** Euler found empirically that the way in which a prime p factors in quadratic integers $x + y\sqrt{D}$ depends only on the class of $p \pmod{4D}$. He found other theorems which simplify the determination of the classes of primes $\pmod{4D}$ which split and the classes which remain prime. These theorems, unproved by Euler, imply and are implied by the law of quadratic reciprocity. **7.9 Genera.** Gauss's necessary conditions for two divisors to be equivalent. Character of a divisor class. Resulting partition of the divisor classes into genera. **7.10 Ambiguous classes.** Definition. Proof that the number of ambiguous classes is at most half the number of possible characters. **7.11 Gauss's second proof of quadratic reciprocity.** Proof that at most half of the possible characters actually occur. Gauss's deduction, from this theorem, of quadratic reciprocity.

Chapter 8 Gauss's theory of binary quadratic forms

305

8.1 Other divisor class groups. When D is not squarefree the definition of the divisor class group needs to be modified. Orders of quadratic integers.

Equivalence relative to an order. The divisor class group corresponding to an order. Exercises: Euler's convenient numbers. **8.2 Alternative view of the cyclic method.** Interpretation of it as a method for generating equivalent binary quadratic forms. Method for finding representations of given integers by given binary quadratic forms. **8.3 The correspondence between divisors and binary quadratic forms.** Proper equivalence of binary quadratic forms. The one-to-one correspondence between proper equivalence classes of properly primitive forms (positive when $D > 0$) and divisor classes for the order $\{x + y\sqrt{D} : x, y \text{ integers}\}$. **8.4 The classification of forms.** Extension of the theorem of Section 7.7 to the case where D is not squarefree. **8.5 Examples.** Derivation of the divisor class group in several cases. **8.6 Gauss's composition of forms.** How Gauss defined the product of two classes of binary quadratic forms without using divisor theory. **8.7 Equations of degree 2 in 2 variables.** Complete solution, essentially due to Lagrange, of $ax^2 + bxy + cy^2 + dx + ey + f = 0$.

Chapter 9 Dirichlet's class number formula 342

9.1 The Euler product formula. Analog in the case of quadratic integers. Splitting into cases for various types of D . **9.2 First case.** The case $D < 0$, $D \not\equiv 1 \pmod{4}$, D squarefree. Derivation of the class number formula. Examples. **9.3 Another case.** The case $D > 0$, $D \not\equiv 1 \pmod{4}$, D squarefree. Derivation. Examples. **9.4 $D \equiv 1 \pmod{4}$.** Modifications required when $D \equiv 1 \pmod{4}$, D squarefree. **9.5 Evaluation of $\Sigma(\frac{D}{n})\frac{1}{n}$.** This term of the class number formula can be evaluated using the technique of Section 6.5. Fourier transform of the character $(\frac{D}{n}) \pmod{4D}$ is a multiple of itself. Use of this fact to reduce the formula. Exercises: Dirichlet's further reductions of the formula in the case $D < 0$, D squarefree. The sign of Gaussian sums and its relation to this formula. **9.6 Suborders.** Generalization of the class number formula to the case where D is not squarefree and, more generally, to divisor class groups corresponding to arbitrary orders of quadratic integers. **9.7 Primes in arithmetic progressions.** Dirichlet's proof that $an + b$ represents an infinity of primes when b is relatively prime to a . Use of the class number formula to prove $L(1, \chi) \neq 0$ for all real characters $\chi \pmod{a}$.

Appendix: The natural numbers 372

A.1 Basic properties. Addition and multiplication. Euclidean algorithm. Congruence modulo a natural number. Chinese remainder theorem. Solution of $ax \equiv b \pmod{c}$. Fundamental theorem of arithmetic. Integers. **A.2 Primitive roots mod p .** Definition. Proof that every p has a primitive root.

Answers to exercises	381
Bibliography	403
Index	409