Preface

> "Whenever you find that you are on the side of the majority, it is time to reform—(or pause and reflect)." —Mark Twain [Notebook, 1904]

Who was Sophie Germain, one of the first women known to achieve important original mathematical research, and how can her writings form the core of an introductory number theory course?[1]

Fortuitously, Germain's recently uncovered grand plan to prove Fermat's last theorem, one of the longest unsolved great problems in mathematics, dovetails with most of a first number theory course today. Thus studying her writings, and selections from other great mathematicians, can provide a complete and richly motivated story from the minds of those who founded modern number theory. We will meld an inquiry-oriented pedagogy with an overarching detective tale, based on Germain's never-published manuscripts and correspondence aiming to resolve Fermat's last theorem. The only student prerequisite is experience proving mathematical results, for instance an introduction to proofs course, along with curiosity and a drive for discovery.

My experiences developing the pedagogies of active learning [**67**, **68**] and student study directly from primary historical sources [**5**, **6**, **44**, **48**, **49**] led to a collaboration that uncovered Sophie Germain's impressive accomplishments toward proving Fermat's last theorem, unknown for the past two hundred years [**48**, **50**, **69**]. I eventually realized one could actually teach a beginning number theory course that primarily follows Germain's writings, in contrast to tackling her thinking only after such a course. Therefore this book largely follows Germain's own work from two centuries ago.

An inquiry pedagogy is natural and rich when studying primary sources. Such materials inevitably provoke thought about uncertainties, demand discussion, and often raise more questions than they answer. They also motivate us to understand the inventions of significant thinkers, and were written in a different context than the present, providing immediate multiple perspectives. For instance Sophie Germain was one of the first to wholeheartedly adopt Gauss's notion of congruence in her research, and we can see firsthand the value of its impact in how she uses it.

Additionally in this case, Sophie Germain was writing for the world's experts as her readers, quite literally for Gauss and Legendre, creating wonderful inquiry challenges today. She assumes her audience is already intimately familiar with many things, such as Fermat's theorem on power residues modulo a prime, which she simply utilizes

[1] While this book is intended for a number theory course, the richness of the related mathematical and social history welcomes cross-curricular listing, with appropriate mathematical prerequisite, by women's studies or history of science. See the citations in section 2.1.

without mention. Thus students must be detectives, divining what prior knowledge she is using as she works, and must develop ideas independently to remain abreast of her path. Our uncertainties about what she is doing lead us to pen "detective notes", questions the student should hypothesize on, or keep in mind for possible resolution as we go along.

By studying primary source excerpts throughout, we obtain a fully motivated experience from the minds of many of number theory's creators, including Euclid, Sunzi, Fermat, Euler, Lagrange, Legendre, Gauss, and Eisenstein, all orbiting Germain's work. Every development, inspiration, and problem emerges from a natural historical question, so no topic or result comes out of the blue. With a "just as needed" approach, phenomena and results arise with natural and timely urgency; for instance, rather than introducing something like Fermat's (little) theorem out of context, it arises here from endeavoring to understand and justify what Sophie Germain uses in her proofs.

Primary sources also naturally reveal multiple approaches through time. For instance, we experience different viewpoints from Euclid to Gauss on uniqueness of prime factorization and its application to fractions. And the genesis of Fermat's theorem appears first in his letters, followed by its proof by Leibniz, multiple proofs and generalization at the hands of Euler, a proof by Dirichlet in combination with Wilson's theorem, and a clever proof by Ivory that is favored today; while at the hands of Lagrange and Euler we see the original perspectives on proving Wilson's theorem. Further, for the existence of primitive roots for prime modulus, we see a rich evolution of multiple proofs through insights of Euler, Lagrange, Legendre, and Gauss. Our philosophy is that mathematics is as much about variety of ideas, techniques and strategies as about results.

How exactly is an inquiry pedagogy implemented in our setting? Students are carefully guided to discover and prove almost all results themselves in a sequence of scaffolded exploratory "tasks" with hints, fully integrated with the narrative. The difficulty of the inquiry tasks varies considerably; we sometimes refer to the level of challenge explicitly in a task, and we often scaffold a challenging task by breaking it into parts with appropriate guidance. The tasks are mandatory for progressing, and are fully relied on later, often without mention. On the other hand, "exercises" are optional, providing further enrichment, depth, and directions for continued study. Since the first two chapters are largely background, history, and broader context, the preponderance and pace of the mandatory tasks, in contrast to the optional exercises, accelerates starting in the third chapter. Tasks, exercises, and stated results often have a descriptive title, to assist readers in grasping and tracking the role and importance of each item during the inquiry process.

Students are guided to engage in inquiry like mathematicians: ask questions; carry out experiments; observe patterns, relationships, and phenomena; conjecture; prove or disprove; generalize. These practices produce deep engagement in rich mathematics, unified here within one overarching mathematical question. We also invite students to keep a running journal of their understanding, explaining how it assists their practice of being a mathematician; this is particularly relevant to the nonlinear aspects of learning via exploration of primary sources like Germain's.

Several features of the book enable multiple course paths of different length and emphasis, all centered around Sophie Germain's grand plan to prove Fermat's last theorem.

First and foremost, Germain's manuscripts and correspondence naturally traverse, albeit not in a typical order, all the standard topics in an introductory number theory course, except for systems of linear congruences and quadratic reciprocity. These latter two topics are fully addressed in section 6.3 and chapter 11, where we provide optional inquiry exploration via other primary historical sources. They, and all other optional sections not requisite to the direct trail following Germain, are labeled with a star (*), and may be incorporated as desired to round out a course.

Second, to grasp crucial number theory topics, and to comprehend the essence of Germain's work, the reader is not obligated to engage intimately the three Germain chapters after primitive roots (chapter 7), in which she carries out all the details of her plan. Even their titles and introductions will give a sense for how her plan proceeded and what the final upshot was.

Third, in several places we provide multiple approaches to a result, most notably for Euclid's lemma, Fermat's theorem, and existence of primitive roots. Not all the approaches need to be followed in detail.

Thus the briefest path, eminently suitable for a single term, is to follow the non-starred sections through chapter 7, waltz as lightly as desired through the three subsequent Germain chapters, and limit consideration of multiple approaches. The optional starred material on linear congruences or quadratic reciprocity may be added as desired. Longer options, ranging anywhere up to a year-long course, may include the three Germain chapters on her plan that succeed chapter 7 on primitive roots, and/or incorporate any optional starred sections.

The table of contents provides an overview of the number theoretic knowledge learned from Germain's plan as it unfolds over the first seven to ten chapters. Here, on the other hand, we will provide an overview of the three biggest optional topics supplementary to following Germain's plan, since they too feature primary sources (by others) to explore old ideas from special angles.

The first supplementary topic, mentioned above, begins with linear congruence equations and the Chinese remainder theorem governing specialized systems. We extend the exploration in historical context to fuller generality, not merely the well-known special case of pairwise relatively prime moduli. This leads to an inspiring solution formula for the general case, only discovered in 1952 by Oystein Ore.

The second supplementary topic, also mentioned above, is the quadratic reciprocity law and applications. Its origins are in Fermat's amazing claims about representability of primes by sums of squares, then Euler's study and discovery of patterns in prime divisors of quadratic forms to prove Fermat's claims, Legendre's formulation of the quadratic reciprocity law, and Lagrange's theory of descent for quadratic forms and representability of primes. While following their path, we present a spectacular proof of the law by Eisenstein that geometrizes one of Gauss's proofs; this is the only place in the book where we actually present a proof without guiding the student in self-discovery via tasks, and by this point in the book we generally expect readers to be able to fill in many details independently. Applications spill into the appendix.

A third supplementary topic, intended purely for enrichment, is in the appendix. It provides a hands-on investigation of why and how Fermat discovered his theorem on power residues modulo a prime, which underlies modern information security via the Rivest-Shamir-Adleman (RSA) cryptosystem. Fermat's trail deeply involves the search

for Mersenne primes, and is augmented here by applications to prime divisors of Fermat numbers and sums and differences of powers, utilizing the quadratic character of the number two and of Sophie Germain primes.

Finally, the introduction contains pictures of number theory cookies my students once spontaneously baked. Readers are invited to identify all the themes in the icing as they devour the book.

I hope you find number theory à la Sophie Germain as rewarding as I and my students have.

Acknowledgments. I owe heartfelt thanks to the encouragement and assistance of numerous people over many years, especially to my students Meredith Anderson and Kristina Brantley, and to many colleagues, friends and family, including Mai Gehrke, Tracy Hume, Richard Jones, Reinhard Laubenbacher, Eva McCarthy, Leanne Merrill, Ina Mette (for never-ending encouragement, enthusiasm, and patience), Dora Musielak, Owen Dell (staff alchemist), Alison and Rick Penfield, Pat Penfield, Doug Ravenel, Ed Rico, and Carol Walker. Their support and enthusiasm have nurtured this dream to fruition. I owe very special thanks to Steve Kennedy for excellent pedagogical suggestions for improvement, and to the series editorial board for many thoughtful and encouraging comments; also to Sarah Hagen and her students Alan Kappler and Samuel Goodman for numerous helpful and insightful comments throughout the book; and to Branwen Schaub for excellent advice based on studying both the mathematics and the intended inquiry pedagogy. Their recommendations have greatly improved the book. Finally, I have been so fortunate to be able to write this book using Scientific Workplace, the most wonderful software created for writing mathematics.

Corvallis, Oregon, 2022