Test Review

The following outline covers just the content covered roughly prior to the Spring Break, this being the material that will be represented on the Test, scheduled for 7:30-8:50am, Monday, April 9. This content includes lecture material from Chapters 1-12 and related handouts, as listed (and linked) below.

See https://ericmoorhouse.org/handouts/integers.pdf for basic notation/properties/results on integers, including divisibility, the *Division Algorithm*, congruences, and modular arithmetic. We covered (or reviewed) *Euclid's Algorithm* in its extended form. (Recall: Given integers a and b, not both zero, the algorithm shows how to compute $g = \gcd(a, b)$, and how to find r, s such that $ra + sb = g$.) This allowed us to compute the inverse of *a* mod *m* (whenever $\gcd(a, m) = 1$); it also leads to *Euclid's Lemma* (the theorem that if a prime p divides ab, then $p|a$ or $p|b$). This in turn yields the *Fundamental Theorem of Arithmetic*: Every integer $n > 1$ has a unique factorization as a product of primes. This content is largely covered in **Chapters 5-8** of the textbook; but I have covered this material very quickly, treating it as **review**, because it is also covered in prerequisite courses.

Chapter 1 introduces some of the basic problems of number theory, including some open problems (such as the *Twin Prime Conjecture* and *Goldbach's Conjecture*), and some problems that have been solved (such as *Fermat's Last Theorem*). We mentioned some other themes and open problems in number theory, but we omitted the discussion of triangular numbers.

Chapter 2 gives a classification of primitive Pythagorean triples. For a slightly different presentation of this topic, see our class handout https://ericmoorhouse.org/courses/4550/pythagoras.pdf. Another approach to the same theorem is to classify rational points on the unit circle, as in **Chapter 3**; but this you may treat as supplementary.

Chapter 4 covers a little more of the interesting history of Fermat's Last Theorem than I presented in class but is highly recommended reading, particularly as it describes Sophie Germain's contributions.

Chapters 5-8: review (see above).

Chapter 9 includes Fermat's Little Theorem, which we covered.

Chapter 10 introduces Euler's 'totient' function $\phi(n)$, and derives a generalization of Fermat's Little Theorem known as Euler's Formula.

Chapter 11 describes some properties of $\phi(n)$, indicating how $\phi(n)$ may be computed if the factorization of n is known. The *Chinese Remainder Theorem* also appears: If $gcd(m, n) = 1$ and r, s are integers, there is an integer x satisfying $x \equiv r$ mod m and $x \equiv s$ mod n; and this value of x is unique mod mn.

Chapter 12 includes Euclid's proof that there are infinitely many primes. It also shows that the sequence of prime numbers has gaps of arbitrarily large size.

In connection with the Fundamental Theorem of Arithmetic, further context was supplied by comparing the situation with more general rings of the form $\mathbb{Z}[\sqrt{d}]$ where factorization is not necessarily unique, as

we showed. Moreover, such rings can have a differing number of units (invertible elements) and when $d < 0$, the units correspond to integer solutions of Pell's Equation $x^2 - dy^2 = \pm 1$.

In our prerecorded lecture of February 19, we introduced *Continued Fractions*. This topic can be found in Chapters 47-48 but the presentation there is much more technical than what we need. I will ask you to have covered instead our class version. The applications of the continued method include

- Recognition of rationals and quadratic irrationals from their decimal approximations. If you prefer a pdf version of this, see https://ericmoorhouse.org/handouts/cf.pdf
- Computation of the solutions of Pell's equation. This is especially useful for finding the fundamental solution when d is large.
- Later (not yet) we will introduce a modern method of integer factorization using continued fractions.

We also spent some time discussing which numbers are expressible as a sum of two squares (or three squares, or $x^2 + dy^2$ or etc. The full answer to the question of two squares is not given until later (Chapters 24-25) but by now we have a taste of this question, and its connection with integer factorization. Also (on February 24) we discussed the use of the theta series $\theta(x) = \sum_{n=-\infty}^{\infty} x^{n^2} = 1 + 2x + 2x^4 + 2x^9 + \cdots$ which provides a way to count the number of ways of writing an integer in such a form.