Semester Review

The final exam will be cumulative, with more emphasis on the later material (after Spring Break; material beginning in Chapter 14). This is an outline of content covered throughout the semester. For your reference, the content listed in the Test Review (up to Chapter 13) is reprinted here.

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 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 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.

We introduced the *Riemann zeta-function* $\zeta(s)$, and its *Euler factorization*. We introduced the *Riemann Hypothesis*, which conjectures that the 'nontrivial' complex solutions of $\zeta(s) = 0$ all have the form $s = ½ + it$. Without a course in complex analysis (Math 4320 should suffice), I wouldn't expect you to fully understand this statement; nevertheless because of the importance of the Riemann Hypothesis (generally considered to be the most significant unsolved problem in mathematics), we felt that some discussion of

this question was appropriate. The importance of $\zeta(s)$, as we indicated, is that the statistical properties of the distribution of prime numbers, are governed by the behavior of $\zeta(s)$ near the 'critical line' $Im(s) = ½$ in the complex plane. As a more accessible demonstration of the significance of $\zeta(s)$, we explained in class that for two 'sufficiently large' integers m and n chosen at random, the probability that *m* and *n* are relatively prime is $1/\zeta(2) = 6/\pi^2$. An introduction to the Riemann zeta-function and its role in describing statistical properties of the distribution of prime numbers, is found in https://ericmoorhouse.org/handouts/needles_and_numbers.pdf. This handout also gives an outline of Euler's heuristic derivation of the identity $1/\zeta(2) = 6/\pi^2$. (If you want to see a more rigorous derivation, this is given in https://ericmoorhouse.org/handouts/basel.pdf; but you are not responsible for this derivation.)

Chapter 12 includes Euclid's proof that there are infinitely many primes. The stronger result that there are infinitely many primes congruent to 3 mod 4 is also proved. *Dirichlet's Theorem* is stated. You should know what this theorem says: Every arithmetic progression of the form $a, a+m, a+2m, \ldots$ (where $gcd(a,m) = 1$) contains infinitely many primes; but you are not responsible for the proof. A supplementary discussion of the proof (which you are *not* responsible for) is found in https://ericmoorhouse.org/handouts/dirichlet.pdf.

Chapter 13 includes a statement (but no proof) of the *Prime Number Theorem*. *Goldbach's Conjecture* is presented.

Chapter 14 introduces Mersenne primes. The largest known primes have this form. I mentioned the popularity of searching for new (and especially larger) Mersenne primes; for the latest news on this effort, see https://www.mersenne.org/. We omit the Fermat primes (which appear only in the exercises).

Chapter 15 defines perfect numbers and presents Euler's characterization of all even perfect numbers in terms of Mersenne primes. Two open problems arise: Are there infinitely many Mersenne primes (or equivalently, are there infinitely many even perfect numbers)? And are there any odd perfect numbers?

Chapter 16 explains how to most efficiently perform modular exponentiation (i.e. compute $a^k \bmod m$) for large a, k, m. This method uses the binary representation of k, and involves repeatedly squaring mod m. This is the most efficient general procedure known for performing modular exponentiation for large values of k and m, unless the factorization of m is known (in which case Fermat's Little Theorem may be useful to simplify the work required). We explained in class how this approach works, with some small explicit examples; and in larger examples, we have left the work to software. We demonstrated the Mathematica command `PowerMod[a,k,m]` which implements this algorithm.

Omit Chapter 17.

Chapter 18 covers RSA public key encryption. We have covered this in class, as well as the Diffie-Hellman scheme for secure key exchange over an open channel. We also discussed the use of RSA encryption for achieving both secrecy and authentication simultaneously.

Omit Chapter 19.

Chapters 20,21,22 introduce the notion of *squares* and *nonsquares* mod p for an odd prime p, which play a role similar to squares (i.e. positives) and nonsquares (i.e. negatives) in the real numbers. Here p is an odd prime. Note that we speak simply of squares and nonsquares, rather than quadratic residues and nonresidues as in the textbook. The *Legendre symbol* is introduced, and its multiplicativity is shown. *Euler's Criterion* for evaluating the Legendre symbol, is shown. You are responsible for the statement of the *Law of Quadratic Reciprocity* (Chapter 23), in particular knowing how to compute the Legendre symbol

in special (small) cases; but you are not responsible for the proof. (The textbook uses primitive roots in its proof. We offer an alternative proof using Gauss sums, which we feel is more natural: https://ericmoorhouse.org/handouts/reciprocity.pdf, but you are not responsible for these methods or the proofs.)

Chapter 24 shows that an odd prime p is expressible as a sum of two squares, iff p is congruent to 1 mod 4. A descent algorithm is presented for actually finding integers a, b such that $p = a^2 + b^2$. This algorithm was presented in class (see the worksheet of April 11) implemented using Mathematica. The main theorem of Chapter 24 amounts to the observation that this algorithm always works. In our proofs (and in our implementation of the descent algorithm) we refer explicitly to the arithmetic of *Gaussian integers* (complex numbers of the form $a + bi$ where a, b are ordinary integers) which results in shorter descriptions than those in the textbook, which instead writes out everything in longhand using real and imaginary parts. We find here an illustration of *Hadamard's Principle: The shortest route between two truths in the real domain, passes through the complex domain*.

Chapter 25 finally answers a question raised early in the semester: We determine exactly which integers are expressible as a sum of two squares. We stated the result (Theorem 25.1) but only gave part of the proof.

Chapter 26 explains mathematical induction, which I assume you all know, so I did not present this. Omit Chapters 27,28,29 also.

Chapter 30 verifies Fermat's Last Theorem in the case of exponent 4, using Fermat's own idea of 'infinite descent'. Actually, more is shown: the equation $x^4 + y^4 = z^2$ has no positive integer solutions. We finally covered this proof during our last lecture.

Omit Chapter 31.

Chapter 32 covers Pell's Equation. This topic overlaps significantly with the subject of Continued Fractions, which appears in the **online Chapters 47 and 48**. The online chapters are found at https://www.math.brown.edu/~jhs/frintonlinechapters.pdf. We offered a much more basic treatment of these topics in our pre-recorded lecture of February 19. We described

- How to compute the continued fraction expansion of a real number from its decimal representation. See **online chapter 47** but omit the technical details of pages 419-422. Note the sequence of *continued fraction convergents* which are defined here.
- How to recognize rationals and quadratic irrationals from their continued fraction expansions, which are terminating (in the case of rationals) or periodic (in the case of quadratic irrationals). See https://ericmoorhouse.org/handouts/cf.pdf for further worked examples. Note that computing the continued fraction expansion of a rational number m/n in lowest terms, is equivalent to computing $gcd(m, n) = 1$; the sequence of quotients in Euclid's algorithm gives the sequence of terms in the continued fraction expansion.
- We introduced Pell's equation; see **Chapter 32**. Theorem 32.1, which we stated without proof, guarantees the existence of (infinitely many) solutions of Pell's equation whenever the coefficient $D > 1$ is a squarefree integer. We phrased the equation in terms of the norm map $\mathrm{N}(a + b\sqrt{D}) = a^2 - Db^2$ which satisfies $N(\alpha)N(\beta) = N(\alpha\beta)$. We worked through several explicit examples in class.
- We mentioned that the continued fraction convergents to a real number α are in some sense the 'most efficient' rational approximations to α. The optional Chapter 33 makes this notion more precise.
- We showed how to solve Pell's equation $x^2 - Dy^2 = 1$ using the continued fraction convergents of $\sqrt{D}$. An example for small D was worked out in detail. Our justification for this method was

heuristic: solutions of Pell's equation give rational numbers x/y which are good rational approximations to D; so it is reasonable that the method of continued fractions would find these solutions. For proofs and details, see the optional Chapter 48.

- On April 30, we presented a Mathematica worksheet demonstrating the first modern factorization algorithm, CFRAC (the Continued Fraction method) which makes use of continued fraction convergents to quadratic irrationals $\sqrt{kn}$ as a way to come up with solutions of $x^2 \equiv y^2 \bmod n$ and thereby a factorization of n.