SECOND MIDTERM REVIEW

1. Overall Info

The exam is 50 minutes; there will once again be a combination of 'computational' problems and more theoretical proofs. The format will be similar to the first test, probably with a little more computation than before. Knowing the proofs and computations in the text and your homework will be most valuable. There will be indications of how much each problem is worth, so that you can pace yourself. This exam covers Chapters 3, 4, and 6, as well as the sections of 5 and 7 which we did.

2. Chapter 3

Be able to define divisor, divisible, common divisor, greatest common divisor, relatively prime, prime, and composite; be able to give examples of each, or to calculate them. Know how to prove some, and use all, of the various theorems about divisors in the first section. Be able to give some primes, and say how you got them. Recall material related to twin triple primes.

3. Chapter 4

Know the division algorithm, both the (full) statement and how to use it. Be able to say in a general way how the Well-Ordering Principle was used in its proof. Know how to use the Euclidean algorithm, and its statement; also be able to say how we use Thm. 3.8 in its proof and how it implies Thm. 4.4. Be able to state the Fundamental Theorem of Arithmetic and use it to find GCDs, as well as explain why 1 is not a prime.

4. Chapter 6

Know all about congruences - what they are, how they work, what a residue class is, what the set of residues is. Be able to do modulo arithmetic $\mathbb{Z}_m$. Also, be able to prove some of the very small Theorems 6.1, 6.2, and 6.3 which we used to define modulo arithmetic. Be able to define a group, and give some examples; given a non-group, be able to tell why it isn't one. Know the idea behind Theorem 6.6. Know how to find the group $U(m)$. Be able to find the order of an element or group I give you; be able to define and identify a cyclic group.

5. Chapters 5 and 7

Be conversant with the definitions of both $\sigma(n)$ and $\tau(n)$, and be able to calculate them for prime powers and for any number given in prime decomposition. Know the idea behind the formulas. Be able to tell what the highest power of 2 and 5 that divides a number is, as well as whether a number is divisible by 3, 7, 9, 11, or 13. Be able to give the rationale behind these methods. Know how check digits work, and be able to do explicit examples for ISBNs. Know how the non-Abelian group we constructed works (we called it D_6 and used triangle symmetry for it), including how to get an example showing it is not commutative.

6. Useful Review Problems

Note: not all these were assigned; they are just useful. First be sure you know how to solve assigned exercises; if there is an area you are weak in, being able to solve these will help you.

Practice Problems 3.2, 3.3, 3.5, 3.11 (we did this in class)
Exercises 3.1, 3.2, 3.7, 3.12
Practice Problems 4.1, 4.3, and 4.4
Exercises 4.1, 4.3, 4.4, and 4.20
Practice Problems 6.2, 6.6, 6.8, 6.9, and 6.10
Exercises 6.1, 6.5, 6.6, 6.8, 6.12, 6.19, and 6.21
Practice Problems 5.2, 5.5, 7.1, 7.2, 7.10
Exercises 5.4, 5.7, 7.1, 7.10, 7.11, Problem in HW about D_6