

Exam 1 material

I. Be able to state:

1. Division Algorithm (2.1)
2. GCD Theorem (2.3)
3. Relatively Prime Theorem (2.4)
4. Fundamental Theorem of Arithmetic & canonical form corollary (3.2 & corollary)
5. Dirichlet's Theorem (3.7)
6. Definition of multiplicative inverse
7. If $ca \equiv cb \pmod{n}$, then $a \equiv b \pmod{n/d}$, where $d = \gcd(c, n)$. (4.3)
8. Chinese Remainder Theorem (4.8)
9. Fermat's Little Theorem & Corollary (5.1)
10. Result from Theorem 5.5 (quadratic congruence)

II. Be able to state and prove:

1. Euclid's Lemma (2.5)
2. There exists an infinite number of primes of the form $4k + 3$. (3.6)
3. Wilson's Theorem (5.4) (there are two proofs: the original one and one in the section §8.2 on primitive roots for primes, you only need to know one of them).

III. Know:

1. Definitions from chapters 1-5.
2. Conditions under which linear diophantine equations can be solved, how to find them and how many solutions exist.
3. Divisibility conditions (section 4.3)
4. Euclidean Algorithm
5. Techniques from homework problems.

Exam 2 material

I. Be able to state:

1. How to calculate σ, τ, μ and ϕ . In particular, Theorems 6.2 & 7.3
2. τ and σ are a multiplicative functions (Theorem 6.3)
3. Theorem 7.5: Euler's Theorem
4. Theorem 8.3 (on the order of $a^h \pmod{n}$)
5. Corollary to 8.4 (If n has a primitive root, then it has exactly $\phi(\phi(n))$ of them.)
6. Lagrange's Theorem (Theorem 8.5)

7. Theorem 8.6 (If p is a prime number and $d \mid p - 1$, then there are exactly $\phi(d)$ incongruent integers having order d modulo p .) & corollary on the number of primitive roots of primes.
8. Theorem 9.2 on properties of the Legendre symbol.
9. Theorem 9.6 (on the calculation of $(2/p)$) and the corollary (stating that for p an odd prime, $(2/p) = (-1)^{(p^2-1)/8}$).

II. Be able to state and prove:

1. Theorem 7.6 Gauss' Theorem
2. Theorem 8.1: If $a^k \equiv 1 \pmod{n}$, then the order of $a \pmod{n}$ divides k .
3. Theorem 9.1: Euler's Criterion

III. Know:

1. Definitions of
 - (a) a multiplicative function,
 - (b) the number theoretic functions σ, τ, ϕ, μ ,
 - (c) the *order* of an integer modulo n ,
 - (d) a *primitive* root of an integer n ,
 - (e) a quadratic residue and a quadratic non-residue of n ,
 - (f) the Legendre symbol (a/p) for p an odd prime,
2. Know how to calculate $a^n \pmod{m}$ using Euler's Theorem for large n .
3. Know how to find all elements of a given order given a primitive root of n .
4. Know how to find all solutions (and when they exist) to $x^d \equiv 1 \pmod{n}$.
5. Practice manipulation of Legendre symbols using theorem 9.2 & corollaries.
6. Know how to find solutions to $ax^2 + bx + c \equiv 0 \pmod{p}$ for p an odd prime.
7. Techniques from homework.

After exam 2 material

I. Be able to state:

1. Law of Quadratic Reciprocity (Theorem 9.9)
2. Corollaries 1 & 2 to the Law of Quadratic Reciprocity on the relationship between (p/q) and (q/p) .
3. Theorem 9.10 on the calculation of $(3/p)$.
4. Know the possible prime divisors of M_p (Theorems 11.5 & 11.6)
5. Pepin's test (Theorem 11.10)
6. Any rational number can be written as a finite simple continued fraction. (Theorem 15.1)

7. The value of the k -th convergent of a finite simple continued fraction is $C_k = p_k/q_k$. (Theorem 15.2) (so you need to know definitions of p_k and q_k .)

II. Be able to state and prove

1. The Euclid-Euler Theorem (Theorem 11.1)
2. Perfect numbers end in 6 or 8. (Theorem 11.2)
3. $p_k q_{k-1} - q_k p_{k-1} = (-1)^{k-1}$ and therefore p_k and q_k are relatively prime. (Theorem 15.3 & Corollary)

III. Know:

1. Definitions of
 - (a) perfect numbers
 - (b) Mersenne numbers and Mersenne primes
 - (c) amicable numbers
 - (d) Fermat numbers and Fermat primes
2. How to compute Legendre symbols (a/p) for any odd prime p and any integer a using law of quadratic reciprocity and the values of $(2/p)$ and $(-1/p)$.
3. Algorithm for finding infinite continued fraction representation of an irrational number (Theorem 15.7).
4. Finding the unique irrational number represented by a periodic infinite continued fraction. (For example, example 15.4 determining the unique irrational number represented by the infinite continued fraction $x = [3; 6, \overline{1}, 4]$)
5. Techniques from homework