Math 362 Information for the final exam

Work covered: Sections 1 – 19 (excluding 14 and excluding cryptography).

Theorems

You must know the statements of all the theorems and principles in Sections 1 – 19 that we covered, and be able to use them when needed.

- Suggestion: make a separate list of the statements of all the theorems, and learn them from your list.
- You should know the proofs of the following theorems.

Section 1: None

Section 2: Lemmas 2.1 – 2.6, Theorems 2.1, 2.2

Section 3: None

Section 4: None

Section 5: None

Section 6: None

Section 7: None

Section 8: Theorems 8.1 – 8.4

Section 9: Lemmas 9.1(a),(b), 9.2, Theorem 9.1

Section 10: (Numbering as in notes) Theorems 10.1, 10.2, 10.3, 10.6, Lemma 10.1, Corollary 10.2

Section 11: Theorems 11.1, 11.2, 11.5

Section 12: Theorem 12.3

Section 15: None

Section 16: Lemmas 16.1 – 16.4

Section 17: None

Section 18: (Numbering as in Notes) Lemmas 18.1 – 18.5, Corollaries 18.1, 18.2, Theorems 18.2, 18.3. (★ See summary below.)

Section 19: No proofs, but statements of theorems and facts (excluding of course the actual values of constants etc.)

★

Theorem 18.1 *The integer n can be written as the sum of two squares iff each prime $p \equiv 3 \pmod 4$ occurs to an even power in the p.p.d. of n.*

A: The integer n can be written as the sum of two squares.

B: Each prime p, where $p \equiv 3 \pmod 4$, occurs to an even power in the p.p.d. of n.

Thus Theorem 18.1 is "**A** $\Leftrightarrow$ **B**".

Theorem 18.2 *If p is prime, $p \equiv 3 \pmod 4$, and p occurs to an odd power in the prime-power decomposition of n, then n cannot be written as the sum of two squares.*

Thus Theorem 18.2 is "not **B** $\Rightarrow$ not **A**", which is the same as "**A** $\Rightarrow$ **B**".

Outline of proof of Theorem 18.2

1. Assume that $n = x^2 + y^2$ for some $x, y \in \mathbb{Z}$.

   Aim: Show that -1 is a quadratic residue of p, which is impossible as $p \equiv 3 \pmod 4$ and hence $(-1/p) = -1$.

2. Write $n = p^{2e+1}m$, where $e \geq 0$ and $\boxed{(p, m) = 1}$.

3. Factor out the powers of p common to x and y:

   (a) Let $(x, y) = d$, and say $d = p^k d_1$, where $k \geq 0$ and $(d_1, p) = 1$.

   (b) Let $x_1 = x/p^k$, $y_1 = y/p^k$ and $n_1 = n/p^{2k}$.

   (c) Then n_1 is an integer, $\boxed{n_1 = x_1^2 + y_1^2}$ and $\boxed{(x_1, y_1) = d_1.}$

4. Show that $p|n_1$, i.e., $\boxed{n_1 \equiv 0 \pmod p}$:

   (a) $n_1 = \frac{n}{p^{2k}} = p^{2e+1-2k}m$.

   (b) Since $(m, p) = 1$, $p^{2e+1-2k}$ is an integer. Therefore

   i. $2e + 1 \geq 2k$ and ii. $p^{2e+1-2k}|n_1$.

   (c) (i) plus a parity argument implies that $2e+1-2k \geq 1$, so from (ii) $p|p^{2e+1-2k}|n_1$.

5. Now show that $\boxed{(x_1, p) = 1}$.

6. Then the congruence $x_1 z \equiv y_1 \pmod{p}$ has a solution $z = u$, i.e., $\boxed{x_1 u \equiv y_1 \pmod{p}.}$

7. Substitute in (3)(c) and use (4) to obtain $x_1^2(1 + u^2) \equiv 0 \pmod{p}$.

8. Since $\boxed{(x_1, p) = 1}$, divide by x_1^2: $1 + u^2 \equiv 0 \pmod{p}$, i.e. $\boxed{u^2 \equiv -1 \pmod{p}.}$
   This gives the desired contradiction.

Lemma 18.5 Thue's Lemma. *Let p be prime and a an integer such that $(a, p) = 1$. Then the congruence $ax \equiv y \pmod{p}$ in two variables x and y is satisfied by $x = x_0, y = y_0$, where*

$$0 < |x_0| < \sqrt{p} \quad \textit{and} \quad 0 < |y_0| < \sqrt{p}.$$

Theorem 18.3 *If $p \equiv 1 \pmod{4}$ is prime, then p is representable as the sum of two squares.*

Outline of proof.

1. Since $p \equiv 1 \pmod{4}$, there exists an integer a satisfying $\boxed{a^2 \equiv -1 \pmod{p}.}$

2. For example, choose a to be the least residue of $\left(\frac{p-1}{2}\right)! \pmod{p}$.

3. Then $(a, p) = 1$ and by Thue's Lemma, $ax \equiv y \pmod{p}$ is satisfied by x_0, y_0 such that $0 < |x_0|, |y_0| < \sqrt{p}$, i.e., $\boxed{0 < x_0^2 + y_0^2 < 2p.}$

4. Use the congruence in (1) to deduce that $x_0^2 + y_0^2 \equiv 0 \pmod{p}$.

5. Thus there exists an integer k such that $x_0^2 + y_0^2 = kp$.

6. By (3) this is only possible if $k = 1$, so $p = x_0^2 + y_0^2$ and theorem is proved.

- Why does **B** $\Rightarrow$ **A** now follow from Theorem 18.3**?**

There are many ways in which these results may be asked – **and you will get at least one of them!**

Applications of Theorems

- Results about congruences and least residues.
- Solve linear and quadratic congruences.
- For a given integer n, determine $d(n),\ \sigma(n),\ \phi(n)$.
- Determine $\mathrm{ord}_m\, a$, for given integers a and m such that $(a, m) = 1$.
- Use Legendre symbols and the values of $(-1/p)$, $(2/p)$ to show that some integer a is a quadratic residue or nonresidue of a given prime.
- Find all primitive roots of a given integer (if it has any).
- Use Legendre symbols to (help) determine whether an integer is a primitive root of a given prime.
- Given integers c and n, determine whether c/n has a terminating decimal expansion, without calculating c/n. If it does have a terminating expansion, how many digits does the expansion have?
- Given integers c and n such that c/n does not have a terminating decimal expansion, determine the period of the decimal expansion of c/n without calculating c/n. What is the length of the non-periodical part of the expansion of c/n?
- Find a Pythagorean triangle (or all of them, fundamental and otherwise) with given hypotenuse or leg.
- Explain why there are no Pythagorean triangles (fundamental or not) with given hypotenuse or given leg.
- If $k = a^2 + b^2$ and $l = c^2 + d^2$, write kl as the sum of two squares.
- Determine whether a given integer n can be written as the sum of two squares, and if so, find such a sum, or several such sums.
- Show that there are no nontrivial integer solutions to equations such as $x^3+3y^3 = 9z^3$, etc.
- Use the representation of the integer n as the sum of two squares to find a Pythagorean triangle with hypotenuse of length n. (Thus combine the results of Sections 16 and 18.)
- More facts about prime numbers, e.g. the density of primes, arithmetic progressions, etc.