MAT 311 Practice for Final Exam

Remark. If you are comfortable with all of the following problems, you will be very well prepared for the midterm. Some of the problems below are more difficult than a problem that would be asked on the midterm. But all of the problems will help you practice the skills and results from this part of the course.

Exam Policies. You must show up on time for all exams. Within the first 30 minutes of each exam, no students will be allowed to leave the exam room. No students arriving after the first 30 minutes will be allowed to take the exam. Students finishing within the last 10 minutes of the exam may be asked to remain until the exam is over and then follow special instructions for turning in their exams (for instance, students are often asked to turn in exams row-by-row).

If you have a university-approved reason for taking an exam at a time different than the scheduled exam (because of a religious observance, a student-athlete event, etc.), please contact your instructor as soon as possible. Similarly, if you have a documented medical emergency which prevents you from showing up for an exam, again contact your instructor as soon as possible.

For excused absences from a midterm, the usual policy is to drop the missed exam and compute the exam total using the other exams. In exceptional circumstances, a make-up exam may be scheduled for the missed exam. For an excused absence from the final exam, the correct letter grade can only be assigned after the student has completed a make-up final exam.

All exams are closed notes and closed book. Once the exam has begun, having notes or books on the desk or in view will be considered cheating and will be referred to the Academic Judiciary.

For all exams, you must bring your Stony Brook ID. The IDs may be checked against picture sheets.

It is not permitted to use cell phones, calculators, laptops, MP3 players, Blackberries or other such electronic devices at any time during exams. If you use a hearing aid or other such device, you should make your instructor aware of this before the exam begins. You must turn off your cell phone, etc., prior to the beginning of the exam. If you need to leave the exam room for any reason before the end of the exam, it is still not permitted to use such devices. Once the exam has begun, use of such devices or having such devices in view will be considered cheating and will be referred to the Academic Judiciary. Similarly, once the exam has begun any communication with a person other than the instructor or proctor will be considered cheating and will be referred to the Academic Judiciary.

Review Topics.
The final exam is cumulative. Here is a list of important topics from the course.

MAT 311 Number Theory **Jason Starr**
Final Exam, Chem 128, 11:15 AM – 1:45 PM **Spring 2011**
Friday, May 20th, 2011

---

(1) Know the division algorithm. Use the division algorithm to find the gcd of 2 (or more) integers.

(2) Know how to prove there are infinitely many primes. Know how to prove there are infinitely primes congruent to 3 modulo 4 (for instance).

(3) Know when an integer a is a *unit* modulo n. If so, be able to find an integer b such that ab is congruent to 1 modulo n.

(4) For a unit a modulo n, know what is the *order* of a modulo n. Be able to compute the order. Know the statements of Fermat's little theorem and Euler's theorem.

(5) Know the statement and uses of Wilson's theorem.

(6) Know when an integer is a sum of two squares.

(7) Know the statement of the Chinese Remainder Theorem. Know how to use the Chinese Remainder Theorem to find an integer with given residues modulo a sequence of (pairwise) relatively prime integers. Know how to use the Chinese Remainder Theorem to find the number of solutions of a polynomial congruence modulo a product of (pairwise) relatively prime integers, given the number of solutions modulo each factor.

(8) Know the definition of the Euler phi function. Know basic properties of the phi function. Be able to compute the phi function.

(9) Know the statement of Hensel's lemma. Be able to use Hensel's lemma to find solutions of a polynomial congruence modulo a power of a prime.

(10) Know what is a primitive root. Know for which integers n there exists a primitive root modulo n. Understand the significance for the group of units modulo n. For small integers n, know how to find a primitive root, including the algorithm for lifting a primitive root modulo p^e to a primitive root modulo p^{e+1}. Given one primitive root modulo n, know how to find all other primitive roots modulo n.

(11) Know the meanings of quadratic residue and quadratic nonresidue. Know the meaning of the Legendre symbol. Know the multiplicative property of the Legendre symbol. Know some direct criteria for computing the Legendre symbol.

(12) Know the statement of quadratic reciprocity, including the criteria for when -1 is a quadratic residue and when 2 is a quadratic residue.

(13) Know the relationship between primitive roots and quadratic nonresidues. Given one primitive root, be able to list all quadratic residues and all quadratic nonresidues in terms of that primitive root.

(14) Be able to use quadratic reciprocity and the Chinese Remainder Theorem to find necessary and sufficient conditions for a given integer m to be a quadratic residue modulo a varying odd prime p in terms of the residue of p modulo a fixed integer.

(15) Using elementary row and column operations over the integers, transform a given integer matrix into "block diagonal" form. Use this to find conditions for consistency of a linear system $AX = B$ in terms of linear congruences on the entries of B. For a consistent system, find the form of the general integer solution of the system.

(16) Know a necessary and sufficient condition for the existence of an integral, binary quadratic form with a given discriminant d and properly representing a given integer m.

(17) Know the meaning of positive definite, negative definite and indefinite. For a binary quadratic form with nonzero discriminant, know the relation between the sign of the discriminant and the type of the quadratic form. Know what this has to do with nontrivial real solutions of the binary quadratic form.

(18) Using quadratic reciprocity and the Chinese Remainder Theorem, determine all odd primes p which are properly represented by some integral, binary quadratic form with a given discriminant d (but possibly depending on p).

(19) For an integer, binary quadratic form whose discriminant is a square, know how to write the form in a special form.

(20) Use integer coefficient, linear variable changes with determinant $+1$ to find a reduced form of an integral, binary quadratic form with non-square discriminant d.

(21) Find all integral, binary quadratic forms with given non-square discriminant d which are reduced. Know how to find all which are positive definite, for instance. Know the meaning of the class number of d.

(22) Know the general form of a Pythagorean triple. Be able to use this to prove non-existence of a triple (a, b, c) of integers with both $a^4 + b^4 = c^2$ and $abc \neq 0$. Similarly, be able to use Pythagorean triples to find the general solution of equations such as $a^2 + b^2 = c^4$ or $a^2 + b^2 = c^8$.

(23) Know how to prove nonexistence of solutions of a Diophantine equation by reduction modulo some given integer n. Know, in principle, the method of "descent" for proving nonexistence of solutions of a Diophantine equation such as Fermat's equation for $n = 4$.

(24) For a ternary quadratic form with rational coefficients and nonzero discriminant, using an invertible linear variable change with rational coefficients, transform the quadratic form to "diagonal form" $g(ax^2 + by^2 + cz^2)$ where a, b, c are integers with $\gcd(a, b, c) = 1$.

(25) For a diagonal ternary quadratic form as above, use a further variable change to tranform to "Legendre diagonal form", $g(ax^2 + by^2 + cz^2)$ where a, b, c are integers such that abc is square-free.

(26) Use Legendre's theorem to determine when a Legendre diagonal ternary quadratic form has a nontrivial rational solution.

(27) Understand the connection between the hypotheses of Legendre's theorem and the existence of real solutions, resp. the existence of solutions modulo p^2 for every prime p dividing abc.

(28) Know which integers can be written as a sum of four squares. Given representations of integers m and n as sums of four squares, understand how to find a representation of mn as a sum of four squares.

(29) Know the division algorithm for polynomials with rational coefficient. Be able to find the greatest common divisor of two rational coefficient polynomials.

(30) Know the meaning of algebraic number and algebraic integer. Given two algebraic numbers, resp. algebraic integers, understand when the sum or product is also an algebraic number, resp. algebraic integer.

(31) Given a finite number field together with an ordered basis, for every element in the number field be able to compute a monic, rational coefficient polynomial satisfied by that element, the *characteristic polynomial*.

(32) Understand the meaning of the constant coefficient as well as the next-to-leading coefficient of the characteristic polynomial. Know some important properties of each of these coefficients involving two elements of the finite number field.

(33) Given the characteristic polynomial, assuming it is of small degree, be able to find the minimal polynomial of the element.

(34) Given a nonzero algebraic number, resp. algebraic integer, understand when the reciprocal is an algebraic number, resp. an algebraic integer.

(35) Know what is the ring of integers of a given finite number field. Understand, at least in principle, how to find the ring of integers.

(36) Be able to compute generators of the Abelian group of algebraic integers in a quadratic number field.

(37) Know the group of units in each imaginary quadratic number field.

(38) Know for which imaginary quadratic number fields, with the natural norm, the ring of integers is a Euclidean domain.

Practice Problems.

(1) In each of the following cases, for the given pair $(m,n) \neq (0,0)$ of integers, find the greatest common divisor $c > 0$. Find the integers m/c and n/c. Find integers u and v such that c equals $um + vn$. Given integers (x,y), know a necessary and sufficient condition in terms of c such that there exists an integer z with $z \equiv x \pmod{m}$ and $z \equiv y \pmod{n}$. Assuming the condition is true, find a formula for one particular such integer z, and know how to describe the general such integers in terms of a particular integer.

(a) $(m,n) = (114, 91)$.
(b) $(m,n) = (51, 85)$.
(c) $(m,n) = (-56, 92)$.
(d) $(m,n) = (72, 54)$.
(e) $(m,n) = (b^3, (b+1)^3)$, where b is an arbitrary integer.

(2) For each of the following sequences $(n_1, \ldots, n_r)$ of pairwise relatively prime integers, find a formula for a particular integer z such that

$$z \equiv x_1 \pmod{n_1}, \ldots, \ z \equiv x_r \pmod{n_r},$$

for a variable sequence of residues $(x_1, \ldots, x_r)$. Finally, for the given sequence of residues $(a_1, \ldots, a_r)$, find the integer z as above with smallest absolute value.

(a) $(n_1, n_2, n_3) = (1, 2, 3)$, $(a_1, a_2, a_3) = (0, 1, 2)$.
(b) $(n_1, n_2, n_3) = (4, 9, 25)$, $(a_1, a_2, a_3) = (1, 1, 1)$.
(c) $(n_1, n_2, n_3, n_4) = (16, 27, 25, 7)$, $(a_1, a_2, a_3, a_4) = (-1, 1, -1, 1)$.
(d) $(b, b+1, b(b+1)+1)$, $(a_1, a_2, a_3) = (1, 0, 0)$, where b is an arbitrary integer.

(3) Prove that there are infinitely many primes congruent to 5 modulo 6.

(4) For the following list $a_1, \ldots, a_r$ of integers and for the following list $n_1, \ldots, n_s$ of positive integers, determine precisely which integers a_i are invertible modulo n_j. In each such case, find an integer $b_{i,j}$ such that $b_{i,j}a_i \equiv 1 \pmod{n_i}$.

$$(n_1, n_2, n_3, n_4, n_5)) = (8, 27, 25, 49, 51), \quad (a_1, a_2, a_3, a_4) = (1, 2, 3, 4).$$

(5) In each of the following cases, determine $\phi(n)$.

$$n = 2, \ n = 7, \ n = 16, \ n = 14, \ n = 105, \ n = 75.$$

(6) In each of the following cases, say whether or not the given integer n is a sum of two squares. When it is a sum of two squares, find integers a and b such that $a^2 + b^2$ equals n.

$$n = 0, \ n = 1, \ n = 4, \ n = 19, \ n = 29, \ n = 49, \ n = 61.$$

(7) In each of the following cases, find all solutions of the polynomial congruence $f(x) \equiv 0$ modulo the two given relatively prime integers a and b. Then find all solutions modulo the integer ab.

(a) $f(x) = 7$, $(a, b) = (2, 7)$.
(b) $f(x) = 3x - 1$, $(a, b) = (2, 5)$.
(c) $f(x) = x^2$, $(a, b) = (8, 9)$.
(d) $f(x) = x^6 - 1$, $(a, b) = (7, 13)$.
(e) $f(x) = x^6 + 1$, $(a, b) = (7, 13)$.

(8) In each of the following cases, for the given polynomial $f(x)$, given prime p, and given integer a_1, say whether or not the given integer a_1 is a solution of $f(x) \equiv 0 \pmod{p}$. Further, say whether or not a is a critical point of $f(x)$ modulo p. If not, give formulas for solutions a_2, resp. a_3, of $f(x) \equiv 0 \pmod{p^2}$, resp. of $f(x) \equiv 0 \pmod{p^3}$, which are congruent to a_1 modulo p.

(a) $f(x) = 7$, $p = 2$, $a_1 = 3$.
(b) $f(x) = 3x - 1$, $p = 5$, $a_1 = 2$.
(c) $f(x) = x^2$, $p = 3$, $a_1 = 1$.
(d) $f(x) = x^6 - 1$, $p = 7$, $a_1 = 3$.
(e) $f(x) = x^6 + 1$, $p = 13$, $a_1 = 2$.

(9) For each of the following integers n, say whether or not the multiplicative group $(\mathbb{Z}/n\mathbb{Z})^\times$ is cyclic. If so, find one generator, say how many generators there are, and give a formula for finding all generators in terms of the particular generator.

$$n = 13,\ n = 14,\ n = 8,\ n = 27,\ n = 257.$$

(10) For each of the following integers n, list all units modulo n which are quadratic residues. Then list all units modulo n which are quadratic nonresidues.

$$n = 5,\ n = 7,\ n = 8,\ n = 9,\ n = 10,\ n = 257.$$

(11) Compute each of the following Legendre symbols directly, without using quadratic reciprocity.

$$\left(\frac{2}{3}\right),\ \left(\frac{3}{7}\right),\ \left(\frac{-1}{11}\right),\ \left(\frac{2}{11}\right),\ \left(\frac{6}{19}\right),\ \left(\frac{-9}{23}\right)$$

(12) Compute each of the following Legendre symbols by any method, including quadratic reciprocity.

$$\left(\frac{2}{11}\right),\ \left(\frac{7}{53}\right),\ \left(\frac{14}{53}\right),\ \left(\frac{30}{53}\right),\ \left(\frac{53}{257}\right),\ \left(\frac{-2}{257}\right)$$

(13) In each of the following cases, for the given integer a, find a necessary and sufficient condition for a variable odd prime p (not dividing a) that a is a quadratic residue modulo p in terms of a congruence involving p modulo a fixed integer n (not varying with p).

$$a = 7,\ a = 13,\ a = 91,\ a = 44,\ a = 27.$$

(14) In each of the following cases, determine whether or not the system is consistent. If it is consistent, find the general solution.

(i)
$$7x + 15y = 9$$

(ii)
$$84x - 39y = 41$$

(iii)
$$84x - 39y = 42$$

(iv)
$$84x - 39y = b, \quad b \text{ arbitrary}$$

(v)
$$15x + 21y + 35z = 14$$

(15) For each of the following matrices A, find invertible, square matrices with integer entries U and V such that UAV is defined and is in block diagonal form.

$$\text{(i) } A = \begin{bmatrix} 2 & 0 \\ 3 & -1 \end{bmatrix}, \quad \text{(ii) } A = \begin{bmatrix} 2 & 0 & 0 \\ 0 & -5 & 0 \\ 3 & 0 & -1 \end{bmatrix}, \quad \text{(iii) } A = \begin{bmatrix} 5 & 10 \\ 9 & 3 \\ 4 & -7 \end{bmatrix},$$

$$\text{(iv) } A = \begin{bmatrix} 1 & 1 & -3 & 2 \\ 5 & 5 & -3 & 10 \\ 2 & 2 & 0 & 4 \end{bmatrix}, \quad \text{(v) } A = \begin{bmatrix} 1 & 2 & 3 \\ 1 & 4 & 9 \\ 1 & 3 & 6 \end{bmatrix},$$

(16) For each of the matrices A from **Problem 15**, find necessary and sufficient conditions on a column vector B so that there exists a column vector X with integer entries solving the linear system $AX = B$. Assuming the system is consistent, find the general integer solution of the system.

(17) In each of the following cases, for the given integer d, find necessary and sufficient conditions on a prime p such that it is properly represented by an integral, binary quadratic form with discriminant equal to d.

$$d = 1, \ d = 2, \ d = -4, \ d = -3, d = -60.$$

(18) In each of the following cases, find an "admissible" linear change of coordinates that transforms the given binary quadratic form to reduced form.

$$\text{(i) } 6x^2 - 5xy + 3y^2, \quad \text{(ii) } 3x^2 - 3xy - 3y^2, \quad \text{(iii) } 17x^2 - 18xy + 4x^2.$$

(19) For each of the following integers d, find all the positive definite, reduced, integral, binary quadratic forms which have discriminant d. In particular, compute the class number $H(d)$.

$$d = -3,\ d = -4,\ d = -8,\ d = -11.$$

(20) For each of the cases from **Problem 19**, find a necessary and sufficient condition on an odd prime p not dividing d such that p is properly represented by a positive definite, reduced, integral, binary quadratic form with discriminant d. Can you determine which form represents which prime p in terms of the residue class of p modulo $4d$?

(21) Does there exist a Pythagorean triple (x, y, z) such that xy is a square integer?

(22) In each of the following cases, find an invertible linear change of coordinates (with rational coefficients) that transforms the given ternary quadratic form to diagonal form. Then use Legendre's theorem to determine whether or not this quadratic form has a solution.

$$f(x, y, z) = (x^2 + yz) + 3(y^2 + xz) + 4(z^2 + xy),$$

$$g(x, y, z) = x^2 - y^2 + 2xz + z^2,$$

$$h(x, y, z) = x^2 + y^2 + z^2 - 2xy - 2xz - 2yz.$$

(23) In each of the following cases, for the given polynomials $(f(x), g(x)) \neq (0, 0)$ with integer coefficients, find the monic greatest common divisor polynomial $c(x)$ as polynomials with rational coefficients. Find the polynomials $f(x)/c(x)$ and $g(x)/c(x)$. Find polynomials $u(x)$ and $v(x)$ with rational coefficients such that $c(x)$ equals $u(x)f(x) + v(x)g(x)$. Finally, find a polynomial with integer coefficients $F_1(x)$, resp. $G_1(x)$, which is a scalar multiple of $f(x)/c(x)$, resp. $g(x)/c(x)$, and such that $F(x)/F_1(x)$ has integer coefficients, resp. $G(x)/G_1(x)$ has integer coefficients.

(a) $f(x) = x + 2$, $g(x) = 2x + 1$.
(b) $f(x) = x^3 + x^2 + x + 1$, $g(x) = x + 1$.
(c) $f(x) = x^3 + x^2 + x + 1$, $g(x) = x^5 + x^4 + x^3 + x^2 + x + 1$.
(d) $f(x) = (x^3 + x)^3$, $g(x) = f'(x) = 3(x^3 + x)^2(3x^2 + 1)$.

(24) For each of the following nonzero algebraic numbers α, find the minimal polynomial $m_\alpha(x)$ of α. Then describe $1/\alpha$ as $f(\alpha)$ for some polynomial $f(x)$ with rational coefficients. Finally, find the minimal polynomial for $1/\alpha$, and find the minimal polynomial for $\alpha - (1/\alpha)$.

(a) $\alpha = 1$.
(b) $\alpha = \sqrt{7}$.
(c) $\alpha = \sqrt[3]{7}$.
(d) $\alpha = \sqrt[3]{7} + 2\sqrt[3]{49}$.
(e) $\alpha = \sqrt{2} + \sqrt{3}$.

(25) For each of the following pairs of algebraic numbers (α, β), find the minimal polynomial of $\alpha + \beta$ and find the minimal polynomial of $\alpha \cdot \beta$.

(a) $(\alpha, \beta) = (1, 2)$.
(b) $(\alpha, \beta) = (\sqrt[3]{7}, \sqrt[3]{7})$.
(c) $(\alpha, \beta) = (\sqrt[3]{7}, \sqrt{3})$.
(d) $(\alpha, \beta) = (\sqrt{2} + \sqrt{3}, \sqrt{3} + \sqrt{6})$.

(26) For each of the following nonzero algebraic numbers α, determine whether or not α is an algebraic integer. When it is an algebraic integer, determine all positive integers n which can be written in the form $\alpha \cdot \beta$ for some choice of algebraic integer β. Finally, for the least positive integer n_1 which can be written in this form, find an algebraic integer β such that $\alpha \cdot \beta$ equals n_1. In particular, say whether or not α is a unit, and if so, find a formula for the multiplicative inverse.

(a) $\alpha = (-1 + \sqrt{2})/2$.
(b) $\alpha = (-1 + \sqrt{3})/2$.
(c) $\alpha = \sqrt{2} + \sqrt{3}$.
(d) $\alpha = \sqrt[3]{81}/3$.

(27) For each of the following squarefree integers m, find the general form of an algebraic integer in $\mathbb{Q}(\sqrt{m})$. When m is negative, describe the group of units in the ring of integers.

$$m = 2,\ m = -1,\ m = -3,\ m = -5.$$