MAT 311 Number Theory | Jason Starr
Midterm II | Spring 2011
Thursday April 14th, 2011

MAT 311 Practice for Midterm II

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 following are the most important new skills not already tested on Midterm I.

MAT 311 Number Theory — **Jason Starr**
Midterm II — **Spring 2011**
Thursday April 14th, 2011

---

(1) Know the statement of quadratic reciprocity, including the criteria for when -1 is a quadratic residue and when 2 is a quadratic residue. 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 value of p modulo a fixed integer.

(2) 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.

(3) 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.

(4) 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).

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

(6) Find all integral, binary quadratic forms with given non-square discriminant d which are reduced.

(7) 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 $a^2 + b^2 = c^8$.

(8) 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 $\gcd(a, b, c) = 1$.

(9) 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.

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

Practice Problems.

(1) In each of the following cases, determine the value of the given Legendre symbol.

$$\text{(i)}\ \left(\frac{3}{151}\right),\quad \text{(ii)}\ \left(\frac{151}{157}\right),\quad \text{(iii)}\ \left(\frac{-1}{157}\right),\quad \text{(iv)}\ \left(\frac{2}{157}\right),\quad \text{(v)}\ \left(\frac{6}{101}\right).$$

(2) Find all prime integers p such that -14 is a square modulo p. Do not forget about $p = 2$ and $p = 7$. For each prime where -14 is a square modulo p, is it also a square modulo p^2, resp. modulo p^3?

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

(i)
$$5x + 17y = 6$$

(ii)
$$112x - 35y = 41$$

(iii)
$$112x - 35y = 42$$

(iv)
$$112x - 35y = b, \quad b \text{ arbitrary}$$

(v)
$$6x + 10y + 15z = 29$$

(4) 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.

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

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

(5) For each of the matrices A from **Problem 4**, 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.

(6) 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 -7. What if the discriminant equals -9?

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

$$\text{(i) } 5x^2 - 4xy + 3y^2, \quad \text{(ii) } 3x^2 - xy - 3y^2, \quad \text{(iii) } 16x^2 - 17xy + 4x^2.$$

(8) Find all the positive definite, reduced, integral, binary quadratic forms which have discriminant -7. Next find all the positive definite, reduced, integral, binary quadratic forms which have discriminant -23. What is the class number $H(-23)$?

(9) Find the general form of a positive Pythagorean triple whose smallest coordinate is a prime integer.

(10) Find the general form of a primitive solution of the integral, Diophantine equation

$$x^4 + y^2 = z^2$$

such that x is odd.

(11) Find an invertible linear change of coordinates (with rational coefficients) that transforms the following ternary quadratic form to diagonal form.

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

Then use Legendre's theorem to determine whether or not this ternary quadratic form has a solution.

(12) Find an invertible linear change of coordinates (with rational coefficients) that transforms the following ternary quadratic form to diagonal form.

$$f(x, y, z) = (x^2 + yz) + 5(y^2 + xz) + 5(z^2 + xy).$$

Then use Legendre's theorem to determine whether or not this ternary quadratic form has a solution.