MAT 312/AMS 351: Applied Algebra

·Home
·Course Info
·Schedule
·Homework
·Exams
·Projects

Welcome to MAT 312/AMS 351

This course is an introduction to algebraic structures with a heavy emphasis on applications. On the algebra side, we will study algebraic properties of integers and such structures as sets and groups. On the applied side, we will discuss public key cryptography and error correcting codes. The course also provides a good opportunity to learn how to read and write rigorous proofs.

These pages will be updated regularly throughout the semester. For specific course-related information, go to the Course info page. Other pages here contain the (tentative) course schedule, home assignments, a list of suggested projects, and exam reviews.

MAT 312/AMS 351: Applied Algebra

Lecture

MF 12:50-2:10pm, Physics P116

Recitations

Section R01: Tu 12:50-1:45pm, SB Union 236
Section R02: W 11:45-12:40pm, Harriman Hall 108

Instructor

Alexander Retakh
Office: Math Tower 4-108
E-mail: retakh@math.sunysb.edu
Office Hours: M 2:30-3:30pm, W 1:00-2:00pm, or by appointment

TA

Yusuf Mustopa
E-mail: mustopa@math.sunysb.edu
Office Hours: M 3-4pm in Math Tower 2-116, T 4-6pm in Math Learning Center, or by appointment

Required text

Numbers, Groups and Codes by J. F. Humphreys & M. Y. Prest, 2nd edition
(On reserve in Math/Physics library)

Exams

Midterm 1
Friday, October 13, in-class

Midterm 2
Mid-November, date TBA; in-class

Final Exam
Friday, December 22, 11:00am-1:30pm

Make-up policy: The university policy is that makeup examinations are given only for work missed due to **unforseeable circumstances** beyond the student's control.

Homework

Homework is a fundamental part of this course, and you will have to work hard on the assigned problems in order to succeed. Assignments will be announced in class, posted on the web and will be **collected in class on Friday** of the following week. **Late homework will not be accepted**.

Projects

You are encouraged to do an individual special project or participate in a group special project. These may include learning a topic in algebra not covered in this course, writing a computer program for an algorithm, or doing a historical report on the subject (or person) discussed in this course. A suggested list of topics is available but you may propose a subject yourself. The exact topic and scope of your project will be determined after a consultation with the instructor. **You must present the final proposal in writing by October 30. All projects are due on December 4.**

GRADING

Your course grade will be computed as follows: homework 20%, two in-class midterms 25% each, and the final exam 30%. The lowest homework grade will be dropped before calculating the average. Participation in a project may contribute up to extra 10% of your grade. In borderline cases, class participation (both lectures and recitations) will be taken into account.

HELP OUTSIDE CLASS

The Math Learning Center is located in Math Tower S-240A and offers free help to any student requesting it. It also provides a locale for students wishing to form study groups.

AMERICANS WITH DISABILITIES ACT

If you have a physical, psychological, medical or learning disability that may impact your course work, please contact Disability Support Services, ECC (Educational Communications Center) Building, room 128, (631) 632-6748. They will determine with you what accommodations are necessary and appropriate. (Note that we cannot make special arrangements for students with disabilities except for those determined by DSS.) All information on and documentation of a disability condition should be supplied to me in writing at the earliest possible time.

STONY
BROOK
UNIVERSITY

MAT 312/AMS 351: Applied Algebra

·Home
·Course Info
·Schedule
·Homework
·Exams
·Projects

Course Schedule (*italic=tentative*)

WEEK OF	SECTIONS	NOTES
9/6-9/8	1.1	
9/11-9/15	1.1-2	
9/18-9/22	1.3-4	
9/25-9/29	1.5-6	
10/2-10/6	1.6	
10/9-10/13	2.1-2	midterm 1 on 10/13
10/16-10/20	2.2-3	
10/23-10/27	4.1-2	
10/30-11/3	4.3	project proposals due 10/30
11/6-11/10	5.1, 4.4	
11/13-11/17	5.2, 5.3	
11/20-11/22		midterm 2 on 11/20
11/27-12/1	5.3, 5.4	
12/4-12/8	5.4	projects due 12/04
12/11-12/15	5.4	final review on 12/15
12/22		final

MAT 312/AMS 351: Applied Algebra

·Home
·Course Info
·Schedule
·Homework
·Exams
·Projects

Home Assignments

WEEK OF	PROBLEMS	DUE
9/8	1.1: 1(i-iii), 3, 4	9/15
9/11-9/16	1.1: 5, 6, 7 1.2: 1, 5, 8, 9, 12	9/22
9/18-9/22	1.3: 2, 3, 5, 6, 8 1.4: 2 (n=6 only), 3(ii,v), 5, 6, 9(ii,iii)	9/29
9/25-9/29	1.5: 1(i,ii,vii), 2(ii), 3, 4(ii) 1.6: 1(ii), 2(i,iii), 3, 7	10/6
10/2-10/6	1.6: 5, 6(ii,iii), 8, 12	10/13
10/9-10/13	2.1: 1, 3, 4, 7 2.2: 2, 5	10/20
10/16-10/20	2.2: 1, 4, 6, 7 2.3: 1, 3, 8, 9	10/27
10/23-10/27	4.1: 1(1st two partitions), 2(π_1), 4(ii), 6 4.2: 6 4.2: 1(i, ii), 2, 4, 10, 13	11/3
10/30-11/3	4.3: 1, 4 4.3: 2, 5, 7, 8(i,ii)	11/10
11/6-11/10	5.1: 1, 2, 4, 8 5.1: 3, 7 4.4: 3(i,v,viii), 5, 11	11/17
11/13-11/17	5.2: 1, 3, 4, 5 5.3: 1, 2, 3, 7(i)	11/27(Monday)
	NOTHING	11/29
11/27-12/1	5.3: 4, 5, 8, 9, 10 4.4: 9, 10 5.4: 1	12/8
12/4-12/8	5.4: 2, 3 5.4: 5, 6, 7	12/15

MAT 312/AMS 351: Applied Algebra

·Home
·Course Info
·Schedule
·Homework
·Exams
·Projects

Exam Information

FINAL: December 22, 11am-1pm.

Reviews: December 13 and 15, in-class.
The final covers Chapters 1, 2, 4, 5. You should know all definitions and theorems that were discussed in the lectures.
Practice problems are available here. Solutions.
Extra office hours: Wed, Dec. 20, 3-4pm

MIDTERM 2 was on November 20

This midterm covered sections 2.1-3, 4.1-4, 5.1. You should know all definitions and theorems that were discussed in the lectures.
Practice problems are available here. (11/15: typos corrected.)
Solutions are now posted.

MIDTERM 1 was on October 13

This mideterm covered all material from Chapter 1. You are should know all definitions and theorems that were discussed in the lectures.
Practice problems are available here. Solutions are now posted.
You should also go over all the homeworks from Chapter 1.

MAT 312/AMS 351: Applied Algebra

·Home
·Course Info
·Schedule
·Homework
·Exams
·Projects

Projects

Important dates:

October 30: project proposals due. You **must discuss** your choice of project with the instructor before this day.
Decemebr 4: projects due

No extensions will be granted

You may work on a project by yourself or in a small group.

Suggested Projects

1. A fast (polynomial-time) algorithm for factorising numbers into primes is unknown. However, recently Agrawal, Kayal, and Saxena discovered a way to determine if the number is prime in polynomial time. Read either the original paper or its summary elsewhere, write up a short description of the algorithm, and implement it.
2. A positive number n is *perfect* if it equals the sum of all of its divisors less than n. E.g., 6=1+2+3 or 28=1+2+4+7+14. A *Mersenne prime* is a prime number of the form $M(k)=2^k-1$. If M(k) is prime, then k is necessarily prime (see exercise 1.3.6).
   - Prove that if M(k) is a prime number, then $n=2^{k-1}M(k)$ is perfect. (Hint: compute the sum of all divisors of n.)
   - Try to prove the converse of the previous statement for even perfect numbers.
   - Write a program that finds even perfect numbers (use the connection with Mersenne primes).
3. In Exercise 1.3.8 you were asked to prove that there are infinitely many primes of the form 4k+3. For this project you will have to find a proof that there are infinitely many primes of the form 4k+1. Also, write a program that compares the number of primes of the form 4k+1 and the number of primes of the form 4k+3 for a range of values of k. Can you make any conjectures about the relationship between these numbers?
4. In certain situations, the RSA code is vulnerable. For example, if the exponent is small and the message is short, the message can be deciphered quickly. Discover how this can be done and write a program implementing this code-breaking. Alternatively, you may discuss the mathematics of other real-life vulnerabilities of the RSA code. More information can be found on the RSA Labs website.
5. There are public key cryptography algorithms other than RSA. One of them is the ElGamal algorithm. Give a brief description of ElGamal, explain the mathematics behind it, and implement it.
6. We define a group as a set with a particular operation. However, a group can be also defined as a collection of strings of letters (and the group operation is just putting two words together). This approach to groups is

called "Combinatorial groups theory." Learn as much of it as you can and write a report. In particular, you will have to explain why the two definitions of a group are equivalent.

7. A group G is *simple* if its only normal subgroups are the trivial subgroup and G itself. Simple finite groups are the "building blocks" out of which other finite groups may be constructed. The classification of simple groups is nearing completion: some proofs need to be ironed out, but it is believed that all such groups are known. Learn what these groups are and write a short (4 or 5 typed pages) report.
8. Discuss Vigenere and Hill ciphers (encryption, decryption). Write a program that can perform encryption, decryption using such methods. Discuss vulnerability via statistics of blocks in the encrypted test. Write a program that does cryptanalysis for such cyphers based on statistics of blocks (for small sizes of blocks).
9. Write a short (4 or 5 typed pages) paper on the mathematical contributions of a number theorist or an algebraist. Note: This is not a biography — you will have to describe mathematical results, their proofs, etc.
10. Write a short (4 or 5 typed pages) historical report on material discussed in the course. You will need to describe mathematical results, outline proofs, etc.

Applied Algebra, MAT312/AMS351
Practice Problems for the Final

(1) Find the greatest common divisor of $12n+1$ and $30n+2$.

(2) Prove that the product of three consequtive natural numbers is always divisible by 6.

(3) Solve the following linear congruences
   (a) $26x \equiv 8 \mod 44$;
   (b) $24x \equiv 9 \mod 40$.

(4) Solve the following system of linear congruences:

$$\begin{cases} x \equiv 4 \mod 25 \\ 3x \equiv 6 \mod 39 \end{cases}$$

(5) Show that the equation $5x^7 - x^4 = 23$ has no integer solutions.

(6) Recall that the Fibonacci sequence is defined as $F_1 = 1, F_2 = 1$, and then for every $n > 2$, $F_n = F_{n-1} + F_{n-2}$. Prove that for every n, $F_2 + F_4 + \cdots + F_{2n} = F_{2n+1} - 1$.

(7) Find the last two digits of the number 3333^{4444}.

(8) Let G be a group and $C = \{a \in G : ax = xa \text{ for all } x \in G\}$. Prove that C is a subgroup of G.

(9) Let R be a relation on $\mathbb{Q}^\times$ (nonzero rational numbers) defined by:

aRb if and only if ab is a square of a rational number.

Prove that R is an equivalence relation.

(10) Let $\pi = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 & 7 \\ 3 & 5 & 1 & 6 & 7 & 4 & 2 \end{pmatrix}$.
   (a) Compute $(145)\pi$.
   (b) Determine the order of π.
   (c) Determine the sign of π.

(11) (a) What is the order of the group $S(4)$?
   (b) What are the possible orders of elements in the group of order 24?
   (c) What are the possible orders of permutations in the group $S(4)$?

(12) Let a, b, c be elements of some group G. Solve the equation $(ax)(bc) = e$ in G. Justify every step.

(13) (a) Let H be the subgroup of G_{15} generated by $[4]_{15}$. List all elements of H.
   (b) List all cosets of H in G_{15}.

(14) Let $R = \{a + b\sqrt{2} : a, b \in \mathbb{Q}\}$. Show that R is a ring. Is R a field?

(15) Let $f : B^3 \to B^5$ be a coding function given by $f(abc) = a\bar{a}b\bar{b}c$, where $\bar{a} = 1$ if $a = 0$ and $\bar{a} = 0$ if $a = 1$. What is the minimal distance between two nonzero codewords in B^5? How many errors can this code detect? How many errors can this code correct?

(16) Write down the two-column decoding table for the code given by the generator matrix

$$\begin{pmatrix} 1 & 0 & 0 & 1 & 1 & 0 \\ 0 & 1 & 0 & 1 & 0 & 1 \\ 0 & 0 & 1 & 0 & 1 & 1 \end{pmatrix}.$$

Use this table to correct the message

010101 101010 001101 100101.

Applied Algebra, MAT312/AMS351
Practice Problems for the Final: Solutions

(1) Find the greatest common divisor of $12n + 1$ and $30n + 2$.

Solution: Using the Euclidean algorithm, we find that

$$\gcd(30n + 2, 12n + 1) = \gcd(12n + 1, 6n) = \gcd(6n, 1) = 1.$$

(2) Prove that the product of three consecutive natural numbers is always divisible by 6.

Solution: If the first of the three integers is even, then the product is even. If it is odd, then the second of the three integers is even; thus the product is even in any case. A similar argument using the possible congruence classes of the first integer modulo 3 shows that the product is divisible by 3. Since 2 and 3 are relatively prime, the result follows by unique factorization of primes.

(3) Solve the following linear congruences
(a) $26x \equiv 8 \mod 44$;
(b) $24x \equiv 9 \mod 40$.

Solution: (a) Since the greatest common divisor of 26 and 44 is 2, which divides 8, this congruence–which is equivalent to $13x \equiv 4 \mod 22$–has a solution, namely $x = [13]_{22}^{-1}[4]_{22}$. Computing $[13]_{22}^{-1}$ by either running the Euclidean algortihm backwards or by the matrix method, we find $[13]_{22}^{-1} = [-5]_{22}$. Thus $x = [2]_{22}$.

(b) Since the greatest common divisor of 40 and 24 (i.e. 8) does not divide 9, this congruence has no solution.

(4) Solve the following system of linear congruences:

$$\begin{cases} x \equiv 4 \mod 25 \\ 3x \equiv 6 \mod 39 \end{cases}$$

Solution: This is equivalent to the system

$$\begin{cases} x \equiv 4 \mod 25 \\ x \equiv 2 \mod 13 \end{cases}$$

which, by the Chinese Remainder Theorem, has a solution. Since $25 \cdot (-1) + 13 \cdot (2) = 1$, the solution is $x \equiv (4 \cdot 13 \cdot 2) + (2 \cdot 25 \cdot (-1)) = 54 \mod 325$.

(5) Show that the equation $5x^7 - x^4 = 23$ has no integer solutions.

Solution: If we reduce this equation mod 2, it becomes $x^7 + x^4 \equiv 1 \mod 2$, which has no solution (direct check for all cogruence classes mod 2).

(6) Recall that the Fibonacci sequence is defined as $F_1 = 1, F_2 = 1$, and then for every $n > 2$, $F_n = F_{n-1}+F_{n-2}$. Prove that for every n, $F_2+F_4+\cdots+F_{2n} = F_{2n+1} - 1$.

Solution: We proceed by induction on n. When $n = 1$, the assertion amounts to $F_2 = F_3 - 1$; since $F_1 = 1$, this is immediate from the definition of the Fibonacci sequence. Now assume that it is true for k. We then have

$$\begin{aligned} F_2 + F_4 + \cdots + F_{2(k+1)} =& (F_2 + F_4 + \cdots + F_{2k}) + F_{2k+2} \\ =& (F_{2k+1} - 1) + F_{2k+2} \\ =& F_{2k+3} - 1 = F_{2(k+1)+1} - 1. \end{aligned}$$

(7) Find the last two digits of the number 3333^{4444}.

Solution: Since 3333 is relatively prime to 100, we may use Euler's Theorem. We have that $\phi(100) = 40$ and $3333 \equiv 33 \mod 100$, so $3333^{4444} \equiv 33^4 = 3^4 \cdot 11^4 = 81 \cdot 121 \cdot 121 \equiv 81 \cdot 21 \cdot 21 \equiv 1701 \cdot 21 \equiv 1 \cdot 21 = 21 \mod 100$.

(8) Let G be a group and $C = \{a \in G : ax = xa \text{ for all } x \in G\}$. Prove that C is a subgroup of G.

Solution: It suffices to show that for all $a, b \in C, ab \in C$ and $a^{-1} \in C$. Let $a, b \in C$ and x be any element of G. Then $(ab)x = a(bx) = (bx)a = (xb)a = x(ba) = x(ab)$. Also, since a commutes with every element of G, it commutes with x^{-1} in particular, i.e. $ax^{-1} = x^{-1}a$. Taking inverses of both sides gives $xa^{-1} = a^{-1}x$.

(9) Let R be a relation on $\mathbb{Q}^\times$ (nonzero rational numbers) defined by:

aRb if and only if ab is a square of a rational number.

Prove that R is an equivalence relation.

Solution: (Reflexivity) For all $a \in \mathbb{Q}^\times$, $aa = a^2$. (Symmetry) Observe that multiplication of rationals is commutative. (Transitivity) Let $a, b, c, q, r \in \mathbb{Q}^\times$ be such that $ab = q^2$ and $bc = r^2$. Then $(qrb^{-1})^2 = (ab)(bc)(b^{-2}) = ac$.

(10) Let $\pi = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 & 7 \\ 3 & 5 & 1 & 6 & 7 & 4 & 2 \end{pmatrix}$.

(a) Compute $(145)\pi$.
(b) Determine the order of π.
(c) Determine the sign of π.

Solution: First note that π may be written in cycle notation as $(13)(46)(257)$.

(a) $(145)\pi = (145)(13)(46)(257) = (1346572)$.

(b) $o(\pi) = \text{lcm}(o((13)), o((46)), o((257))) = 6$ (this works since the cycles in question are disjoint).

(c) $\text{sign}(\pi) = \text{sign}((13)) \cdot \text{sign}((46)) \cdot \text{sign}((257)) = 1$. (Alternative solution: count inverstions in π.)

(11) (a) What is the order of the group $S(4)$?
(b) What are the possible orders of elements in a group of order 24?
(c) What are the possible orders of permutations in the group $S(4)$?

Solution: (a) The order of $S(4)$ is $4! = 24$. (b) By Lagrange's Theorem, the only possible orders of an element in a group of order 24 are 1,2,3,4,6,8,12, and 24. (c) An element of $S(4)$ which is not the identity can be written as either a 2-cycle, a 3-cycle, a 4-cycle, or a product of two disjoint 2-cycles. Thus the possible orders of an element of $S(4)$ are 1,2,3, and 4.

(12) Let a, b, c be elements of some group G. Solve the equation $(ax)(bc) = e$ in G. Justify every step.

Solution: $(ax)(bc) = e \Rightarrow ax = (bc)^{-1}$ (existence of inverses) $\Rightarrow ax = c^{-1}b^{-1}$ (by the formula for the inverse of the product) $\Rightarrow x = a^{-1}c^{-1}b^{-1}$ (can drop parentheses by associativity) .

(13) (a) Let H be the subgroup of G_{15} generated by $[4]_{15}$. List all elements of H.
(b) List all cosets of H in G_{15}.

Solution: (a) Since $([4]_{15})^2 = [1]_{15}$, $H = \{[1]_{15}, [4]_{15}\}$.
(b) The cosets are

$$\begin{aligned} H &= \{[1]_{15}, [4]_{15}\} \\ [2]_{15} \cdot H &= \{[2]_{15}, [8]_{15}\} \\ [7]_{15} \cdot H &= \{[7]_{15}, [13]_{15}\} \\ [11]_{15} \cdot H &= \{[11]_{15}, [14]_{15}\} \end{aligned}$$

(14) Let $R = \{a + b\sqrt{2} : a, b \in \mathbb{Q}\}$. Show that R, equipped with ordinary addition and multiplication of real numbers, is a ring . Is R a field?

Solution: To show that R is an additive abelian group, we show that it is a subgroup of the (abelian!) additive group of real numbers. It suffices to check that the difference of any two elements of R is in R. Indeed, given $a + b\sqrt{2}, c + d\sqrt{2} \in R$, $(a + b\sqrt{2}) - (c + d\sqrt{2}) = (a - c) + (b - d)\sqrt{2}$; since $a - c, b - d \in \mathbb{Q}$ we are done.

Then we only need to show that R is closed under multiplication, since associativity of multiplication and distributivity properties are "inherited" from the reals. Indeed, given $a+b\sqrt{2}, c+d\sqrt{2} \in R$, $(a+b\sqrt{2}) \cdot (c+d\sqrt{2}) = (ac + 2bd) + (ad + bc)\sqrt{2}$. Thus R is a ring as claimed.

Furthermore the multiplication in R is commutative and R contains a unit element $(1 = 1 + 0\sqrt{2})$.

Finally, we show that R is a field, i.e. that $R^\times$ is an abelian group. The only group axiom that needs checking is the existence of inverses. If $a+b\sqrt{2}$ is an element of $R^\times$, that is, $a, b \in \mathbb{Q}$ are not both zero, "rationalizing the denominator" tells us that $(a + b\sqrt{2}) \cdot (\frac{a}{a^2-2b^2} + \frac{-b}{a^2-2b^2}\sqrt{2}) = 1$. (Note that this is valid because $\sqrt{2}$ is irrational.)

(15) Let $f : B^3 \to B^5$ be a coding function given by $f(abc) = a\bar{a}b\bar{b}c$, where $\bar{a} = 1$ if $a = 0$ and $\bar{a} = 0$ if $a = 1$. What is the minimal distance between two distinct codewords in B^5? How many errors can this code detect? How many errors can this code correct?

Solution: Note that f, while not a linear code, is given by first applying the generating matrix

$$A = \begin{pmatrix} 1 & 1 & 0 & 0 & 0 \\ 0 & 0 & 1 & 1 & 0 \\ 0 & 0 & 0 & 0 & 1 \end{pmatrix}$$

and then adding 01010 to the result. For all $v, w \in B^3$, $(vA + 01010) - (wA + 01010) = vA - wA$, so it suffices to work with the linear code given by A instead. The minimum weight of a nonzero codeword of this linear code is 1 (look at the third row of A), so the minimum distance between distinct codewords of f is also 1. It follows that the code can neither correct nor detect any errors.

(16) Write down the two-column decoding table for the code given by the generator matrix

$$B = \begin{pmatrix} 1 & 0 & 0 & 1 & 1 & 0 \\ 0 & 1 & 0 & 1 & 0 & 1 \\ 0 & 0 & 1 & 0 & 1 & 1 \end{pmatrix}.$$

Use this table to correct the message

010101 101010 001101 100101.

Solution: First, we compute the parity-check matrix associated to B. This is

$$H = \begin{pmatrix} 1 & 1 & 0 \\ 1 & 0 & 1 \\ 0 & 1 & 1 \\ 1 & 0 & 0 \\ 0 & 1 & 0 \\ 0 & 0 & 1 \end{pmatrix}$$

We choose the zero vector, all 6 unit vectors (corresponding to rows of H), and 100001 (corresponding to $111 = 110 + 001$) to be coset leaders. The table is then

syndrome	**coset leader**
000	000000
001	000001
010	000010
100	000100
011	001000
101	010000
110	100000
111	100001

The syndrome of 010101 is 000, so it is a codeword. The syndromes of 101010, 001101, and 100101 are 111, 110, and 011, respectively. Adding the appropriate coset leaders gives the "corrected" message

010101 001011 101101 101101.

Applied Algebra, MAT312/AMS351
Practice Problems for Midterm II

(1) Let $R = \{(a, b) \mid a \equiv b \mod 5\}$ be a subset of $\mathbb{Z} \times \mathbb{Z}$. Prove or disprove that aRb is an equivalence relation on $\mathbb{Z}$.

(2) Let $\pi = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 & 7 \\ 4 & 6 & 2 & 7 & 3 & 1 & 5 \end{pmatrix}$ and $\sigma = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 & 7 \\ 3 & 6 & 5 & 1 & 4 & 2 & 7 \end{pmatrix}$. Compute $\pi\sigma$, π^{-1}. Determine orders and signs of π and σ.

(3) Prove that for any permutation π, the permutation $\pi^{-1}(12)\pi$ is a transposition.

(4) Leat a, b be elements of a group G. Solve equations $a^{-1}x = b$ and $xa^{-1}b = e$.

(5) Let G be a group such that for any two elements a, b in G, $(ab)^2 = a^2b^2$. Prove that G is abelian.

(6) Let G be a group. Define the relation of *conjugacy* on G: aRb if and only if there exists $g \in G$ such that $b = g^{-1}ag$. Prove that this is an equivalence relation.

(7) Compute orders of the following elements of the group $(\mathbb{C}^\times, \cdot)$: $3i$, $\frac{\sqrt{2}}{2} + \frac{\sqrt{2}}{2}i$.

(8) For a matrix A denote its transpose by A^t. A is orthogonal if $A^{-1} = A^t$ (A^t means the transpose of A). Prove that the set of invertible orthogonal $n \times n$ matrices is a subgroup of $GL(n, \mathbb{R})$. (*Hints:* First recall – or deduce – that $(AB)^t = B^tA^t$ and $(A^{-1})^t = (A^t)^{-1}$.)

(9) Let R be a commutative ring such that $1 + 1 = 0$. Prove that for any $x, y \in R$, $(x + y)^2 = x^2 + y^2$.

(10) Prove that the subset $\{a + bj | a, b \in \mathbb{R}\}$ of $\mathbb{H}$ is a field.

Applied Algebra, MAT312/AMS351
Practice Problems for Midterm II: Solutions

1. Let $R = \{(a,b) \mid a \equiv b \mod 5\}$ be a subset of $\mathbb{Z} \times \mathbb{Z}$. Prove or disprove that aRb is an equivalence relation on $\mathbb{Z}$.

Solution: R is reflexive: $a \equiv a \mod 5$ because $5|(a-a)$. R is symmetric: if $a \equiv b \mod 5$, i.e. $5|(a-b)$, then $5|(b-a)$, i.e. $b \equiv a \mod 5$. R is transitive: if $a \equiv b \mod 5$ and $b \equiv c \mod 5$, i.e. 5 divides $a-b$ and $b-c$, then $5|(a-c)$, i.e. $a \equiv c \mod 5$. Therefore, R is an equivalence relation.

2. Let $\pi = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 & 7 \\ 4 & 6 & 2 & 7 & 3 & 1 & 5 \end{pmatrix}$ and $\sigma = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 & 7 \\ 3 & 6 & 5 & 1 & 4 & 2 & 7 \end{pmatrix}$. Compute $\pi\sigma$, π^{-1}. Determine orders and signs of π and σ.

Solution: $\pi\sigma =$
$$\begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 & 7 \\ 4 & 6 & 2 & 7 & 3 & 1 & 5 \end{pmatrix}\begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 & 7 \\ 3 & 6 & 5 & 1 & 4 & 2 & 7 \end{pmatrix} = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 & 7 \\ 2 & 1 & 3 & 4 & 7 & 6 & 5 \end{pmatrix}.$$

$$\pi^{-1} = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 & 7 \\ 4 & 6 & 2 & 7 & 3 & 1 & 5 \end{pmatrix}^{-1} = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 & 7 \\ 6 & 3 & 5 & 1 & 7 & 2 & 4 \end{pmatrix}.$$

$$\pi = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 & 7 \\ 4 & 6 & 2 & 7 & 3 & 1 & 5 \end{pmatrix} = (1475326), \text{ order}=7.$$

$$\sigma = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 & 7 \\ 3 & 6 & 5 & 1 & 4 & 2 & 7 \end{pmatrix} = (1354)(26), \text{ order}=\text{lcm}(4,2) = 4.$$

Inversions in π: $(4,1)$, $(6,1)$, $(2,1)$, $(7,1)$, $(3,1)$, $(4,2)$, $(6,2)$, $(4,3)$, $(6,3)$, $(7,3)$, $(6,5)$, $(7,5)$. 12 inversions, thus $\text{sign}(\pi) = (-1)^{12} = 1$.

Inversions in σ: $(3,1)$, $(6,1)$, $(5,1)$, $(3,2)$, $(6,2)$, $(5,2)$, $(4,2)$, $(6,4)$, $(5,4)$, $(6,5)$. 10 inversions, thus $\text{sign}(\sigma) = (-1)^{10} = 1$.

3. Prove that for any permutation π, the permutation $\pi^{-1}(12)\pi$ is a transposition.

Solution: Let k, l be such that $\pi(k) = 1$, $\pi(l) = 2$. Then $\pi^{-1}(1) = k, \pi^{-1}(2) = l$, so that $\pi^{-1}(12)\pi(k) = l$ and $\pi^{-1}(12)\pi(l) = k$, i.e. $\pi^{-1}(12)\pi$ permutes k and l. Now let m be any number distinct from k and l. Since $m \neq k, l$, $\pi(m) \neq 1, 2$ and the transposition (12) leaves $\pi(m)$ in place. Therefore, $\pi^{-1}(12)\pi(m) = \pi^{-1}(\pi(m)) = m$. Hence, $\pi^{-1}(12)\pi$ leaves $m \neq k, l$ in place. We conclude that $\pi^{-1}(12)\pi = (kl)$, a transposition.

4. Leat a, b be elements of a group G. Solve equations $a^{-1}x = b$ and $xa^{-1}b = e$.

Solution: $a^{-1}x = b$: multiply by a on the left: $aa^{-1}x = ab$. Thus $x = ab$.

$xa^{-1}b = e$: multiply by $b^{-1}a$ on the right: $xa^{-1}bb^{-1}a = eb^{-1}a$. Thus $x = eb^{-1}a = b^{-1}a$.

5. Let G be a group such that for any two elements a, b in G, $(ab)^2 = a^2b^2$. Prove that G is abelian.

Solution: $(ab)^2 = a^2b^2$ means $abab = aabb$. Multiply by a^{-1} on the left and b^{-1} on the right: $a^{-1}ababb^{-1} = a^{-1}aabbb^{-1}$. Cancelling $a^{-1}a$ etc gives $ba = ab$ for all a, b. This means that G is abelian.

6. Let G be a group. Define the relation of *conjugacy* on G: aRb if and only if there exists $g \in G$ such that $b = g^{-1}ag$. Prove that this is an equivalence relation.

Solution: R is reflexive: aRa because $e^{-1}ae = a$. R is symmetric: if aRb, i.e. if $b = g^{-1}ag$ for some g, then $a = gbg^{-1} = (g^{-1})^{-1}bg^{-1}$ and bRa. R is transitive: if aRb, i.e. $b = g^{-1}ag$, and bRc, i.e. $c = h^{-1}bh$, then $c = h^{-1}g^{-1}agh = (gh)^{-1}a(gh)$

and aRc. (Notice that the definition of relation requires that $b = g^{-1}ag$ for some g, i.e. for different pairs of a and b, g may be different.)

7. Compute orders of the following elements of the group $(\mathbb{C}^{\times}, \cdot)$: $3i$, $\frac{\sqrt{2}}{2} + \frac{\sqrt{2}}{2}i$.

Solution: $(3i)^n = 3^n i^n$. Since $|3^n i^n| = 3^n$ (or, equivalently, since $3^n i^n$ equals either of $3^n, -3^n, 3^n i, -3^n i$), $(3i)^n \neq 1$ for any n. Hence $3i$ has infinite order.

Taking subsequent powers of $\frac{\sqrt{2}}{2} + \frac{\sqrt{2}}{2}i$ shows that $\left(\frac{\sqrt{2}}{2} + \frac{\sqrt{2}}{2}i\right)^8 = 1$. Alternatively, you can just compute $\left(\frac{\sqrt{2}}{2} + \frac{\sqrt{2}}{2}i\right)^8 = i$ and take it from there.

8. For a matrix A denote its transpose by A^t. A is orthogonal if $A^{-1} = A^t$ (A^t means the transpose of A). Prove that the set of invertible orthogonal $n \times n$ matrices is a subgroup of $GL(n, \mathbb{R})$. (*Hints:* First recall – or deduce – that $(AB)^t = B^t A^t$ and $(A^{-1})^t = (A^t)^{-1}$.)

Solution: We have to prove that (1) if A and B are invertible orthogonal matrices, then so is AB; (2) if A is an invertible orthogonal matrix, then so is A^{-1}.

(1) $(AB)^t = B^t A^t = B^{-1} A^{-1} = (AB)^{-1}$.

(2) $(A^{-1})^t = (A^t)^{-1} = (A^{-1})^{-1}$.

9. Let R be a commutative ring such that $1+1 = 0$. Prove that for any $x, y \in R$, $(x+y)^2 = x^2 + y^2$.

Solution: $(x+y)^2 = (x+y)(x+y) = x^2 + xy + yx + y^2$ (distributive law). Since R is commutative, $yx = xy$. Since $1+1 = 0$, $xy + xy = (1+1)xy = 0xy = 0$. Thus $(x+y)^2 = x^2 + 0 + y^2 = x^2 + y^2$.

10. Prove that the subset $\{a + bj | a, b \in \mathbb{R}\}$ of $\mathbb{H}$ is a field.

Solution: Since $\mathbb{H}$ is a unital ring, we only have to prove that every nonzero element of the form $a + bj$ is invertible and that $(a+bj)(c+dj) = (c+dj)(a+bj)$ (commutativity of multiplication).

Invertibility of $a + bj$: $(a+bj)(a-bj) = a^2 - b^2 j^2 = a^2 + b^2$. Therefore, $(a+bj)^{-1} = \dfrac{a - bj}{a^2 + b^2}$.

Commutativity of multiplication: $(a+bj)(c+dj) = ac + bcj + adj + bdj^2 = ca + cbj + daj + dbj^2 = (c+dj)(a+bj)$.

Applied Algebra, MAT312/AMS351
Practice Problems for Midterm 1

1. Find the greatest common divisor of $12n + 1$ and $30n + 2$.

2. Prove that for every natural number n, the number $3^{2n+2} + 8n - 9$ is divisible by 16.

3. Recall that the Fibonacci sequence is defined as $F_1 = 1, F_2 = 1$, and then for every $n > 2$, $F_n = F_{n-1} + F_{n-2}$. Prove that for every n, $F_1 + F_3 + \cdots + F_{2n-1} = F_{2n}$.

4. Find all $n > 2$ such that $n^3 - 3$ is divisible by $n - 1$.

5. When questioned by the police, the suspect claimed that he did not remember his home address but could definitely recall that the house number is less than 1000 and is divisible by 7, 11, and 13. Is the suspect telling the truth?
And what if he said that the number was divisible by 7, 11, and 14?

6. Let a, b, and c be positive integers such that $a^2 + b^2 = c^2$. Prove that at least one of them is divisible by 3.
(*Hint*: reduce mod 3.)

7. Solve the following linear congruences:
(a) $5x \equiv 7 \mod 31$;
(b) $2x \equiv 19 \mod 2006$;
(c) $19x + 3 \equiv 4 \mod 83$.

8. Find the minimal positive integer satisfying the following conditions:
(i) when divided by 7, its remainder is 4,
(ii) when divided by 12, its remainder is 5.

9. Compute $\phi(1001)$, $\phi(96)$.

10. Find the last two digits of 1221^{122}.

Applied Algebra, MAT312/AMS351
Practice Problems for Midterm 1: Solutions

1. Find the greatest common divisor of $12n+1$ and $30n+2$.

Solution: $30n+2 = 2(12n+1)+6n$; $12n+1 = 6n \cdot 2+1$. Thus $\gcd(12n+1, 30n+2) = 1$.

2. Prove that for every natural number n, the number $3^{2n+2}+8n-9$ is divisible by 16.

Solution: Induction on n.

Base: $n=0$, $3^{2n+2}+8n-9=0$.

Step: we assume that $3^{2k+2}+8k-9$ is divisible by 16. For $n=k+1$, the expression becomes $3^{2(k+1)+2}+8(k+1)-9 = 9(3^{2k+2}+8k-9)-64k+80$.

Since $3^{2k+2}+8k-9$, $64k$, and 80 are divisible by 16, so is $3^{2(k+1)+2}+8(k+1)-9$.

3. Recall that the Fibonacci sequence is defined as $F_1=1, F_2=1$, and then for every $n>2$, $F_n = F_{n-1}+F_{n-2}$. Prove that for every n, $F_1+F_3+\cdots+F_{2n-1} = F_{2n}$.

Solution: Induction on n.

Base: $n=1$. $F_1 = F_2$ (both equal 1.

Step: we assume that $F_1+F_3+\cdots+F_{2k-1} = F_{2k}$. Then $F_1+F_3+\cdots+F_{2(k+1)-1} = (F_1+F_3+\cdots+F_{2k-1})+F_{2(k+1)-1} = F_{2k}+F_{2k+1} = F_{2k+2} = F_{2(k+1}$.

4. Find all $n>2$ such that n^3-3 is divisible by $n-1$.

Solution: $n^3-3 = (n-1)(n^2+n+1)-2$. If n^3-3 is divisible by $n-1$, $n-1$ divides 2, i.e. $n-1=1,2$. Given that $n>2$, we conclude that $n=3$.

5. When questioned by the police, the suspect claimed that he did not remember his home address but could definitely recall that the house number is less than 1000 and is divisible by 7, 11, and 13. Is the suspect telling the truth?

And what if he said that the number was divisible by 7, 11, and 14?

Solution: Since 7, 11, and 13 are relatively prime, a number divisible by them must be divisible by their product. (This follows from the Unique Factorisation Theorem.) But $7 \cdot 11 \cdot 13 = 1001$, so the house number is both less than 1000 and divisible by 1001.

However, if a number is divisible by 7, 11, and $14 = 2 \cdot 7$, it should only be divisible by $2 \cdot 7 \cdot 11 = 154$, i.e. may be less than 1000.

6. Let a, b, and c be positive integers such that $a^2+b^2=c^2$. Prove that
at least one of them is divisible by 3.

Solution: Reducing mod 3, we get $[a]_3^2+[b]_3^2=[c]_3^2$. If neither a, b nor c are divisible by 3, then they belong to either $[1]_3$ or $[-1]_3$. Hence $[a]_3^2=[b]_3^2=[c]_3^2=[1]_3$ and the equality does not hold.

7. Solve the following linear congruences:

(a) $5x \equiv 7 \mod 31$;

Solution: $\gcd(5,31)=1$, hence the solution is $[5]_{31}^{-1}[7]_{31}$. To compute $[5]_{31}^{-1}$, we first perform the Euclidean algorithm for the pair $(5,31)$: $31 = 5\cdot 6+1$. Therefore $31+5(-6)=1$, i.e. $[5]_{31}^{-1}=[-6]_{31}$. Finally, $[5]_{31}^{-1}[7]_{31} = [-6]_{31}[7]_{31} = [-42]_{31} = [20]_{31}$.

(b) $2x \equiv 19 \mod 2006$;
Solution: $\gcd(2, 2006) = 2$ does not divide 19. No solutions.

(c) $19x + 3 \equiv 4 \mod 83$.
Solution: If $19x + 3 \equiv 4$, then $19x \equiv 1$. Thus $x = [19]_{83}^{-1}$. Euclidean algorithm for 19 and 83: $83 = 19 \cdot 4 + 7$; $19 = 7 \cdot 2 + 5$; $7 = 5 \cdot 1 + 2$; $5 = 2 \cdot 2 + 1$. Then $2 \cdot 2 = 5 - 1$; $7 \cdot 2 = 5 \cdot 2 + 2 \cdot 2 = 5 \cdot 3 - 1$; $19 \cdot 3 = 7 \cdot 2 \cdot 3 + 5 \cdot 3 = 7 \cdot 6 + 7 \cdot 2 + 1 = 7 \cdot 8 + 1$; $83 \cdot 8 = 19 \cdot 4 \cdot 8 + 7 \cdot 8 = 19 \cdot 32 + 19 \cdot 3 - 1 = 19 \cdot 35 - 1$. Hence, $19 \cdot 35 \equiv 1 \mod 83$. (Alternatively, you could use the matrix method.) Answer: $[35]_{83}$.

8. Find the minimal positive integer satisfying the following conditions:
(i) when divided by 7, its remainder is 4,
(ii) when divided by 12, its remainder is 5.
Solution: We have to find x such that

$$\begin{cases} x \equiv 4 \mod 7 \\ x \equiv 5 \mod 12. \end{cases}$$

Since $7 \cdot (-5) + 12 \cdot 3 = 1$, by the Chinese Remainder Theorem, the solution is $[5 \cdot 7 \cdot (-5) + 4 \cdot 12 \cdot 3]_{7 \cdot 12} = [-31]_{84} = [53]_{84}$. Answer: 53.

9. Compute $\phi(1001)$, $\phi(96)$.
Solution: $1001 = 7 \cdot 11 \cdot 13$, thus $\phi(1001) = \phi(7)\phi(11)\phi(13) = 6 \cdot 10 \cdot 12 = 720$. $96 = 2^5 \cdot 3$, thus $\phi(96) = \phi(2^5)\phi(3) = (2^5 - 2^4) \cdot 2 = 32$.

10. Find the last two digits of 1221^{122}.
Solution: Last two digits of any number = remainder of division by 100. Therefore, we have to compute $[1221^{122}]_{100}$. Simplifying, $[1221^{122}]_{100} = [1221]_{100}^{122} = [21]_{100}^{122}$. By Euler's theorem $[a]_{100}^{\phi(100)} = [1]_{100}$. Since $\phi(100) = \phi(2^2 \cdot 5^2) = (2^2 - 2)(5^2 - 5) = 40$, $[21]_{100}^{122} = [21]_{100}^{2} = [441]_{100} = [41]_{100}$. Answer: 41.