Math 312/AMS 351 - Spring 2015

Week of:	Monday	Wednesday	Friday	Homework (Due the following Wednesday unless stated).
1/26	snow day	snow day	1.1	
2/2	snow day	1.1-1.2	1.3	p.15; 1,3,4,5,6. p. 23; 1,3,8.
2/9	1.3-1.4	1.4	1.4	p.35; 4,6,8,9. p.48; 2,4,5,6,7.
2/16	1.5	1.5-1.6	1.6	p.59; 1,2,4. p.75; 2,5.
2/23	1.6	2.1	2.2	p.75; 6,7. p. 86; 2,3,7,9. **+ RSA problem**
3/2	2.3	2.3	4.1	p.102; 2,5,8,11. p. 115; 1,2,5. + your 4 favorite **review problems**.
3/9	review	Midterm 1	4.1	none
3/16	----------	spring	break	----------
3/23	4.2	4.2	4.3	p.158; 1,2,3,4,5. p;168; 1,2,9,11.
3/30	4.3	5.1	5.1-5.2	p.183; 1,2,3,4,7. p.211; 4,5,9,10.
4/6	5.2	5.3	5.3	p. 218; 1,2,3,5. p 230; 1,5,7,8,9.
4/13	5.4	5.4	5.4	p.252; 2,4,5,7 + your 3 favorite **review problems**. Due 4/24.
4/20	review	Midterm 2	6.1-6.2	none
4/27	6.2	6.3-6.4	6.4-6.5	p. 272; 1(iii), 2(iv,v), 3. p 278; 1,2,5,6. p.284; 1,2,3. Due 5/6
5/4	6.5	return exam 2 and review	review	Extra **Code Problem:** will replace lowest HW grade. Due at the final or before.
5/11				Final Exam: Thursday May 14, 11:15-1:45.

Course Information

Instructor: Dr. Ben Ward
Email: benjamin.ward at stonybrook...

Office: Simons Center 403
Office Hours: M 2:30-4:00, W 1:00-2:30, or by appt.

Lecture: MWF 11:00-11:53 in MATH P131

Recitation: W 8:30-9:23 in Earth & Space 079
Recitation Instructor: Tsung-Yin Lin

Textbook: Numbers, Groups & Codes by Humphreys & Prest, 2nd ed.

Final Exam: Thursday May 14, 11:15-1:45.

More course information is available on the syllabus **located here.**

Stony Brook University | The State University of New York

Math 312/AMS 351 - Spring 2015

Instructor: Dr. Ben Ward
- Email: benjamin.ward@stonybrook.edu
- Office: Simons Center 403
- Office Hours: M 2:15-3:45, W 1:00-2:30, or by appt.

Course Website: https://sites.google.com/a/stonybrook.edu/math-312-spring-2015/
Note that a schedule of the lecture topics and the homework due is available on the site.

Textbook. Numbers, Groups & Codes by Humphreys & Prest, 2^{nd} ed.

Grading. Grades will be based on homework, two midterm exams and one final exam. The percentage breakdown:

- **Homework -** 25%
  The homework will be listed on the course website and collected at the beginning of class each Wednesday. Late homeworks will not be accepted.
- **Midterm 1 -** 20%
  In class on Wednesday March 11.
- **Midterm 2 -** 20%
  Date TBD.
- **Final Exam -** 35%
  The final exam will take place Thursday May 14 at 11:15-1:45.

Recitation. Recitation takes place Wednesdays from 8:30-9:23 in Earth & Space 079. The recitation instructor is Tsung-Yin Lin and his email is tslin@math.sunysb.edu.

Students with Disabilities: If you have a physical, psychological, medical, or learning disability that may impact your ability to carry out assigned course work, please contact Disability Support Services at (631) 632-6748 DSS. DSS office: Room 133 in the Humanities Building. DSS will review your concerns and determine, with you, what accommodations are necessary and appropriate. All information and documentation is confidential. Arrangements should be made early in the semester so that your needs can be accommodated. Students who require assistance during emergency evacuation are encouraged to discuss their needs with their professors and DSS. For procedures and information go to the DSS website: *http://studentaffairs.stonybrook.edu/dss/*

Academic Integrity: Each student must pursue his or her academic goals honestly and be personally accountable for all submitted work. Representing another persons' work as your own is always wrong. Faculty are required to report any suspected instances of academic dishonesty to the Academic Judiciary. For more comprehensive information on academic integrity, including categories of academic dishonesty, please refer to the academic judiciary website:
http://www.stonybrook.edu/commcms/academic_integrity/index.html

Critical Incident Management: Stony Brook University expects students to respect the rights, privleges, and property of other people. Faculty are required to report to the Office of University Community Standards any disruptive behavior that interrupts their ability to teach, compromises the safety of the learning environment, or inhibits the students' ability to learn. Further information about most academic matters can be found in the Undergraduate Bulletin, the Undergraduate Class Handbook and the Faculty-Employee Handbook.

Your mission is to decrypt the following top secret message.

$$\{2151\},\{8530\},\{7042\},\{1564\},\{8301\},\{9654\},\{1680\},\{1876\},\{2340\},\{6127\},\{8513\},$$
$$\{1924\},\{5933\},\{2208\},\{1677\},\{2190\},\{0303\},\{2403\}$$

The base[1] of the code is 11021 and the exponent is 4325. The alphabet is listed below. Good luck.

A	1	34	67
B	2	35	68
C	3	36	69
D	4	37	70
E	5	38	71
F	6	39	72
G	7	40	73
H	8	41	74
I	9	42	75
J	10	43	76
K	11	44	77
L	12	45	78
M	13	46	79
N	14	47	80
O	15	48	81
P	16	49	82
Q	17	50	83
R	18	51	84
S	19	52	85
T	20	53	86
U	21	54	87
V	22	55	88
W	23	56	89
X	24	57	90
Y	25	58	91
Z	26	59	92
space	27	60	93
.	28	61	94
,	29	62	95
?	30	63	96
!	31	64	97
&	32	65	98
;	33	66	99

Use the above space to outline your work and record the result. However, you should use a computer to do any big calculations.[2]

[1] You will notice that my blocks are larger than my prime factors, but as the book points out, this is only a problem if the blocks are not relatively prime to the base. Each of my blocks are, so this does not create a problem. See 9 p.75 for more discussion of this.

[2] As I explained in class possibilities include mathematica or excel or open office. Note however that using open office, I had to reduce after each exponentiation get the correct answer.

Math 312 - AMS 351 **Midterm Exam 1 - Practice** **Spring 2015**

Name: _____

1. Let k be a positive integer. Prove that $(n-1)|(n^k-1)$ for all integers $n \geq 2$.
2. Find all integers less than 300 such that (simultaneously)

$$x \equiv 1 \pmod 3$$
$$x \equiv 1 \pmod 5$$
$$x \equiv 1 \pmod 7$$

3. Find $d = gcd(156, 72)$. Then find integers x and y such that $156x + 72y = d$.
4. Prove that if $p, p+2$, and $p+4$ are all prime then $p = 3$. (Hint: by contradiction; use modular arithmetic).
5. Find all $[x] \in \mathbb{Z}_{15}$ such that $[6] \cdot [x] = [9]$.
6. List the invertible elements in $\mathbb{Z}_{24}$. Show using Euler's ϕ function that your list has the expected number of classes.
7. Calculate the orders of all elements in $\mathbb{Z}_{11}$.
8. Given an RSA public key code with base 55 and exponent 7, what power x will the coded blocks need to be raised to in order to decode a message?
9. Define a function $\rho\colon \mathbb{Z}_{\geq 2} \to P(\mathbb{Z})$ from those integers greater than or equal to 2 to the power set of the integers, as follows. If $a = p_1^{n_1} \cdot \cdots \cdot p_r^{n_r}$ is the prime factorization of a, grouping common primes (so that $p_i \neq p_j$ for $i \neq j$), then $\rho(a) = \{p_1, \ldots, p_r\}$. Is ρ injective? Is ρ surjective? Explain.
10. Define a relation on positive integers by saying $a \Phi b$ if $\phi(a) = \phi(b)$. Prove that Φ is an equivalence relation. Find $a > b \geq 1000000$ such that $a \Phi b$.
11. In a room with 1000000 light switches, all off to begin with, I first go and flip every second one. That I go back to the beginning and flip every third one, then every forth etc.[1] Which light switches will be off at the end of this process. (Hint: prime factorization).

[1] So at the end of the process the first one is off the second is on the third is on the forth is off...

Name: _____

1. Make a table listing the elements of S_4 along with their signs, orders and inverses.[1]

2. Prove that G_{20} (the group of invertible congruence classes modulo 20) is not a cyclic group. Prove that G_{20} is isomorphic to a product of cyclic groups.[2]

3. Let $x \in G$ be a fixed element. Define a function $\phi\colon G \to G$ by $\phi(g) = xgx^{-1}$. Prove that ϕ is an isomorphism.

4. Give an example of a group G and a nontrivial subgroup H such that $[G : H] = 2015$.

5. Prove that rotation of a regular triangle can be achieved as a product of two different reflections.

6. Let $H \subset S_4$ be the subgroup of permutations of $\{1, 2, 3, 4\}$ which leave 1 fixed. So for example $(23) \in H$ but $(143) \notin H$. List the distinct cosets of H. What familiar group of small order is H isomorphic to?

7. Let σ be a 100-cycle and let π be a 350-cycle. Suppose further that π and σ are disjoint. What is the order and sign of $\pi\sigma$?

8. If G is a group and H and K are subgroups prove that $H \cap K$ is a subgroup of G.

9. Describe the group $D_5 \cap A_5$. Describe the group $D_6 \cap A_6$. What can you say about $D_n \cap A_n$?

Note that there are no review problems covering section 5.4, since the current homework covers this material.

[1] I am not asking you to make the multiplication table for S_4, which would be much more tedious.
[2] Easy way: use the classification of groups of small order. Fun way: write down an isomorphism.

I stumbled upon a message so important I had to use the following convoluted procedure to encode it:

1. First I translated the message using the table below.
2. Next I encoded the binary using the cyclic code of length 6 generated by $1 + x + x^2$.
3. Then I added a parity check digit.
4. Then I converted the result to base 10.
5. Finally I encoded these numbers using an RSA public key code with base 1073 exponent 605.

The result was $\{1008\}, \{517\}$.
Good Luck. Feel free to use a computer if necessary, but outline your work in the space provided:

J	0000
F	0001
R	0010
D	0100
L	1000
B	0011
A	0101
N	1001
I	0110
S	1010
C	1100
M	0111
E	1011
H	1101
T	1110
O	1111