MAT 312/ AMS 351 Applied Algebra, Fall 2014

- **Instructor:** Nikita Selinger, office 4-115 Math Tower.
- **Email:** nikita(at)math(dot)sunysb(dot)edu.
- **Office hours:** TuWe 4.00-5.30pm, or by appointment.
- **Class meetings:** TuTh, 11:30am-12:50pm, Math P131.

- **TA:** Ming-Tao Chuan, office 3-116 Math Tower.
- **Email:** ming-tao.chuan AT stonybrook.edu.
- **Office hours:** Tu 2.00-4.00pm (MLC), Tu 5.00-6.00 (office).
- **Recitations:** R01 - Tu 1:00pm - 1:53pm, R02 - We 11:00am - 11:53am.

Final Exam is on Wednesday 12/10 5.30-8.00pm. The final will cover Chapters 1, 4.1-4.3, 5, 6.1-6.4 of the textbook. See the webpage of the previous semesters course for more info and practice problems. See also the following files with sample solutions: 1 , 2 , 3 , 4 , 5.

Week 15: (Dec 2,4) Section 6.4

Week 14: (Nov 25) Section 6.3

Week 13: (Nov 18, 20) Section 6.2

Homework 10 due Dec 2 or 3. Solve the following exercises: Section 6.2 NN 1,2,3.

Week 12: (Nov 13) Section 6.1

Midterm II is on Tuesday 11/11. The midterm will cover Chapters 4.1-4.3, 5 of the textbook. See the webpage of the previous semesters course for more info and practice problems. See also the following files with sample solutions: 1 , 2 , 3 , 4 , 5.

Week 11: (Nov 4, 6) Sections 5.3, 5.4

Homework 9, due Nov 4 or 5. Solve the following exercises: Section 5.2 NN 2,3,5. Section 5.3 NN 1, 3, 9.

Week 10: (Oct 28,30) Sections 5.2, 5.3

Homework 8, due Oct 28 or 29. Solve the following exercises: Section 5.1 NN 2, 3, 5, 7, 8.

Week 9: (Oct 21,23) Sections 5.1, 5.2

Homework 7, due Oct 21 or 22. Solve the following exercises: Section 4.3 NN 1, 2, 3, 4, 5.

Week 8: (Oct 14,16) Sections 4.3, 5.1

Homework 6, due Oct 14 or 15. Solve the following exercises: Section 4.2 NN 1, 3, 4, 8, 10, 11.

Week 7: (Oct 7,9) Section 4.2

Homework 5, due Oct 7 or 8. Solve the following exercises: Section 4.1 NN 3, 4, 5.

Week 6: (Sep 30, Oct 2) Section 4.1

Homework 4, due Sep 30 or Nov 1. Solve the following exercises: Section 1.6 NN 5,6,7. Write a complete proof of Euler's Theorem.

Week 5: (Sep 23) Section 1.6

Midterm I is on Thursday 9/25. The midterm will cover Chapter 1 of the textbook. See the webpage of the previous semesters course for more info and practice problems and the midterm with solutions of the course offered this summer (you can ignore Question 5, we are not covering that topic).

Homework 3, due Sep 23 or 24. Solve the following exercises: Section 1.4 NN 2,5,6,7. Section 1.5 NN 3,5.

Week 4: (Sep 16,18) Sections 1.4, 1.5

Homework 2, due Sep 16 or 17. Solve the following exercises: Section 1.3 NN 2,5,6,7,8,9. Write a rigorous proof of Corollary 1.3.5.

Week 3: (Sep 9,11) Sections 1.3, 1.4

Homework 1, due Sep 9 or 10. Solve the following exercises: Section 1.1 NN 4, 6, 7 and Section 1.2 NN 3, 6, 10, 12.

Week 2: (Sep 4) Section 1.2

Week 1: (Aug 26,28) Section 1.1

Syllabus: We will cover chapters 1,4,5,6 from the textbook.

Homework is a compulsory part of the course. Homework assignments are due each week at the beginning of the recitation. Under no circumstances will late homework be accepted.

Grading system: The final grade is the weighted average according the following weights: homework 10%, Midterm1 25%, Midterm2 25%, Final 40%.

Textbook: *NUMBERS,GROUPS&CODES,* Author: HUMPHREYS, Publisher: CAMB, Edition: 2ND 04

Disability support services (DSS) statement: If you have a physical, psychological, medical, or learning disability that may impact your course work, please contact Disability Support Services (631) 6326748 or http://studentaffairs.stonybrook.edu/dss/. They will determine with you what accommodations are necessary and appropriate. All information and documentation is confidential. Students who require assistance during emergency evacuation are encouraged to discuss their needs with their professors and Disability

Support Services. For procedures and information go to the following website: http://www.stonybrook.edu/ehs/fire/disabilities/asp.

Academic integrity statement: Each student must pursue his or her academic goals honestly and be personally accountable for all submitted work. Representing another person's work as your own is always wrong. Faculty are required to report any suspected instance 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 at http://www.stonybrook.edu/uaa/academicjudiciary/.

Critical incident management: Stony Brook University expects students to respect the rights, privileges, and property of other people. Faculty are required to report to the Office of Judicial Affairs any disruptive behavior that interrupts their ability to teach, compromises the safety of the learning environment, and/or inhibits students' ability to learn.

MAT 312 - AMS 351

PRACTICE QUESTIONS for FINAL EXAM

SUMMER II, 2014

Q. 1. *Prove that the square of any odd integer always leaves a remainder of 1 when divided by 8.*

Proof. Let $n = 2k + 1$ for some $k \in \mathbb{Z}$. Then

$$n^2 = (2k+1)^2 = 4k^2 + 4k + 1 = 4k(k+1) + 1.$$

Either k or $k+1$ is an even integer. So, 8 divides $4k(k+1)$. Hence, $n^2 \equiv 1 \bmod 8$. □

Q. 2. *Let n be an integer greater than 1. Determine the value of*

$$\gcd(n! + 1, (n+1)! + 1).$$

Proof. Assume that $\gcd(n! + 1, (n+1)! + 1) = d$. Then $n! + 1 = da$ for some $a \in \mathbb{Z}$. Equivalently, $n! = da - 1$. We have

$$(n+1)! + 1 = (n+1)n! + 1 = (n+1)(da - 1) + 1 = da(n+1) - n.$$

So, $(n+1)! + 1 \equiv 1 \bmod d$. This is a contradiction unless $d = 1$. Therefore, $n! + 1$ and $(n+1)! + 1$ must be relatively prime.

Alternatively, you may use Euclidean Algorithm to conclude that $d = 1$. □

Q. 3. *Show that* 328 *divides* $25^{80} - 3^{800}$.

Proof. We will use Euler's Theorem to reduce the integers modulo 328. We have $\phi(328) = \phi(8)\phi(41) = 4 \cdot 40 = 160$. Also,

$$25^{80} - 3^{800} = (5^2)^{80} - (3^{160})^5 = 5^{160} - (3^{160})^5.$$

Since, $(5, 328) = 1$ and $(3, 328) = 1$, we find $5 \equiv 1 \bmod 328$ and $3 \equiv 1 \bmod 328$. Therefore, $5^{160} - (3^{160})^5 \equiv 1 - 1 \equiv 0 \bmod 328$. In other words, 328 divides $25^{80} - 3^{800}$. □

Q. 4. *Let p be a prime and let $1 \leq k \leq p-1$ be an integer. Prove that*

$$\binom{p-1}{k} \equiv (-1)^k \bmod p.$$

Proof. By definition

$$\binom{p-1}{k} = \frac{p!}{k!(p-1-k)!} = \frac{(p-1)(p-2)\cdots(p-k)}{k!}.$$

Notice that $p - i \equiv -i \bmod p$ for all $i \in \{0, 1, \ldots, p\}$. Therefore,

$$\binom{p-1}{k} = \frac{(p-1)(p-2)\cdots(p-k)}{k!} \equiv \frac{(-1)(-2)\cdots(-k)}{1 \cdot 2 \cdots k} \bmod p \equiv (-1)^k \bmod p.$$

□

Q. 5. *Let $G = \{a, b, c, d, f, g\}$ be a group with an operation $*$ given by the table*

$*$	a	b	c	d	f	g
a	d					
b	g	d			c	
c						
d				d		
f				f	g	d
g		c	a			f

a) *Fill in the remainder of the group table (the identity element does not necessarily head the first column or the first row).*
b) *Write down the product table for the group $S(3)$.*
c) *Show that G and $S(3)$ are isomorphic (describe a group isomorphism between the two groups).*
d) *What is the smallest group of G that contains g?*

Proof. a) First, we determine the identity element of $(G, *)$. We look for an element $e \in G$ satisfying $e * e = e$. According to the table, $d * d = d$. So d must be the identity element. Secondly, $d * x = x = x * d$ for all $x \in G$. Using this, we fill in the rows and columns represented by d to get

$*$	a	b	c	d	f	g
a	d			a		
b	g	d		b	c	
c				c		
d	a	b	c	d	f	g
f				f	g	d
g		c	a	g		f

Every element of G has to appear exactly once in each row and column of the table. Following this rule we can place b and d in the last row: in the first column, $a * a = d$ so $g * a$ cannot be equal to d. We must have $g * f = d$, and hence $g * a = b$:

$*$	a	b	c	d	f	g
a	d			a		
b	g	d		b	c	
c				c		
d	a	b	c	d	f	g
f				f	g	d
g	b	c	a	g	d	f

Now, let us consider the first column. We need to place c and f. Since, $c * d = c$, we cannot have $c * a = c$. So, $c * a$ must be f and $f * a = c$.

$*$	a	b	c	d	f	g
a	d			a		
b	g	d		b	c	
c	f			c		
d	a	b	c	d	f	g
f	c			f	g	d
g	b	c	a	g	d	f

In the fifth row, we have $f * b = a$ since we cannot have $f * c = a$ (as $g * c = a$); and $f * c = b$. Now the table has the form

$*$	a	b	c	d	f	g
a	d			a		
b	g	d		b	c	
c	f			c		
d	a	b	c	d	f	g
f	c	a	b	f	g	d
g	b	c	a	g	d	f

By a similar consideration for the remaining entries, we get

$*$	a	b	c	d	f	g
a	d	f	g	a	b	c
b	g	d	f	b	c	a
c	f	g	d	c	a	b
d	a	b	c	d	f	g
f	c	a	b	f	g	d
g	b	c	a	g	d	f

b) For the multiplication table for $S(3)$ see Example 2 on page 157 of the textbook.

c) Let us define a map $\varphi\colon G \to S(3)$. If φ is a group homomorphism then φ must map the identity d of G to the identity permutation id of $S(3)$. So, we set $\varphi(d) = \mathrm{id}$.

In $S(3)$, the elements of order 2 are $(1\ 2), (1\ 3), (2\ 3)$. On the other hand, in G, we have $a * a = d$, $b * b = d$ and $c * c = d$. Therefore, φ should identify $\{a, b, c\}$ with $\{(1\ 2), (1\ 3), (2\ 3)\}$ and $\{f, g\}$ with $\{(1\ 2\ 3), (1\ 3\ 2)\}$. – mapping an element of order 2 to an element of order 3 (or vice versa) in $S(3)$ by φ would cause problems (see the solution for Q.8.). So, let $\varphi(f) = (1\ 2\ 3)$ and $\varphi(g) = (1\ 3\ 2)$ (this is optional, we could also choose $\varphi(f) = (1\ 3\ 2)$ and $\varphi(g) = (1\ 2\ 3)$).

We will assign the values of φ at a, b, c using the properties of group homomorphism. The key point is that φ 'respects' group operations on both G and $S(3)$. For example, $\varphi(a * b) = \varphi(a)\varphi(b)$, etc. We need to choose $\varphi(a), \varphi(b), \varphi(c)$ among $(1\ 2), (1\ 3), (2\ 3)$ so that the following hold

$$(2\ 3)(1\ 2) = (1\ 2)(1\ 3) = (1\ 3)(2\ 3) = (1\ 3\ 2) = \varphi(g),$$

$$(2\ 3)(1\ 3) = (1\ 3)(1\ 2) = (1\ 2)(2\ 3) = (1\ 2\ 3) = \varphi(f).$$

So, let $\varphi(a) = (1\ 2)$. Since $a * b = f$, we have

$$\varphi(a * b) = \varphi(a)\varphi(b) = (1\ 2)\varphi(b) = \varphi(f) = (1\ 2\ 3).$$

Then we must have $\varphi(b) = (2\ 3)$. This leaves $\varphi(c) = (1\ 3)$. You can check that now $\varphi(x * y) = \varphi(x)\varphi(y)$ for all $x, y \in G$ and φ is bijective. This ends the proof.

Alternatively, a bijection can be observed (after assigning $\varphi(d) = \mathrm{id}$) by comparing the two tables. If there is a bijection between two groups then their operation tables should 'coincide', possibly after a reordering of the rows and columns.

d) Let H denote the smallest subgroup of G containing g. Since H is a subgroup it must also contain the identity element, which is d. So, $d \in H$. We have $g * g = f$, so $f \in H$ (H is closed under $*$). As $f * f = g$ and $f * g = g * f = d \in H$, we conclude that $H = \{d, f, g\}$. □

Q. 6. *Let $f\colon G \to H$ be a group isomorphism. Prove that G is commutative if and only if H is commutative.*

Proof. Assume that G is commutative. Then $g_1 g_2 = g_2 g_1$ for all $g_1, g_2 \in G$. Let $h_1, h_2 \in H$. Since f is an isomorphism, it is one-to-one and surjective. So, there exist unique elements $g_1, g_2 \in G$ such that $f(g_1) = h_1$ and $f(g_2) = h_2$. By the definition of a group homomorphism and $g_1 g_2 = g_2 g_1$, we get

$$h_1 h_2 = f(g_1)f(g_2) = f(g_1 g_2) = f(g_2 g_1) = f(g_2)f(g_1) = h_2 h_1.$$

So, H is also commutative.

Now assume that H is commutative. Let $g_1, g_2 \in G$. Then $f(g_1 g_2) = f(g_1)f(g_2)$. Since $f(g_1), f(g_2) \in H$, $f(g_1)f(g_2) = f(g_2)f(g_1)$. So,

$$f(g_1 g_2) = f(g_1)f(g_2) = f(g_2)f(g_1) = f(g_2 g_1)$$

which implies that $g_1 g_2 = g_2 g_1$ and G is commutative. □

Q. 7. *Let H and K be subgroups of a group G. Prove that $H \cup K$ is a subgroup of G if and only if either $H \subseteq K$ or $K \subseteq H$.*

Proof. Let us assume that $H \cup K$ is a subgroup of G and show that either $H \subseteq K$ or $K \subseteq H$. The statement "$H \subseteq K$ or $K \subseteq H$" is equivalent to "$H \setminus K = \emptyset$ or $K \setminus H = \emptyset$". So, assume that $H \setminus K \neq \emptyset$ and $K \setminus H \neq \emptyset$. Let $x \in H \setminus K$ and $y \in K \setminus H$. Then, $x, y \in H \cup K$. Since H, K and $H \cup K$ are all subgroups, we have $x^{-1} \in H$, $y^{-1} \in K$ and $xy \in H \cup K$. Now, $xy \in H \cup K$ implies that $xy \in H$ or $xy \in K$.

If $xy \in H$ then $x^{-1}xy = y \in H$. This is a contradiction.

If $xy \in K$ then $xyy^{-1} = x \in K$. This is also a contradiction. So, $H \setminus K = \emptyset$ or $K \setminus H = \emptyset$.

On the other hand, if $H \subseteq K$ or $K \subseteq H$ then $H \cup K = H$ or $H \cup K = K$. In either case $H \cup K$ is a subgroup. □

Q. 8. *Prove that there exists no isomorphism between the groups G_7 and $S(3)$.*

Proof. Notice that, since $G_7 = \langle [3]_7 \rangle$, G_7 is a cyclic group of order 6 ($[3]_7$ has multiplicative order 6). On the other hand, $S(3)$ is not cyclic (there is no permutation of order 6 in $S(3)$). Let us assume that there exists an isomorphism $f \colon G_7 \to S(3)$ and find a contradiction.

Since f is a group homomorphism, f maps the identity of G_7 to the identity of $S(3)$: $f([1]_7) = \mathrm{id}$. Assume that $f([3]) = \pi$ for some $\pi \in S(3)$. The order of π is then either 1, 2 or 3. The order of π cannot be 1 because the only permutation of order 1 is the identity permutation and f is assumed to be one-to-one. If the order of π is 2 then

$$\mathrm{id} = \pi^2 = f([3]_7)f([3]_7) = f([3]_7[3]_7) = f([3]_7^2).$$

As $f([1]_7) = \mathrm{id}$, we must have $[3]_7^2 = [1]_7$ (f is one-to-one). This is a contradiction.

Similarly, assuming the order of π is 3 also yields a contradiction. Therefore there can be no isomorphism between G_7 and $S(3)$. □

Q. 9. *Let G be a group and $x \in G$ such that $x^2 \neq e$ but $x^6 = e$. Prove that $x^4 \neq e$ and $x^5 \neq e$. What can you say about the order of x in G?*

Proof. The assumption $x^6 = e$ implies that $x^4x^2 = e$ and then $x^4 = x^{-2}$. Since $x^2 \neq e$, $x^{-2} \neq e$. So, $x^4 \neq e$.

Multiplying both sides of $x^6 = e$ by x^{-1} gives $x^5 = x^{-1}$. Now, $x^{-1} \neq e$ since otherwise, $x^{-1} = e$ would imply $x^{-2} = e$. So, $x^5 \neq e$.

It follows that the order of x in G is either 3 or 6. □

Q. 10. *Let X be a finite set. Is $P(X)$, the set consisting of all subsets of X, a group with the set operation $\cup$? Why (not)?*

Proof. The operation $\cup$ on $P(X)$ is associative and closed. The identity element is $\emptyset \in P(X)$. However, there is no set $B \in P(X)$ for any $A \in P(X)$ satisfying $A \cup B = \emptyset$. Therefore, $(P(X), \cup)$ is not a group. $\square$

MAT 312 - AMS 351 FINAL EXAM

SUMMER II, 29 August 2014

NAME : ID :

ANSWER ALL QUESTIONS.

SHOW YOUR CALCULATIONS

DO NOT TEAR-OFF ANY PAGE

NO CALCULATORS NO CELLS NO NOTES ETC.

1		20pts
2		20pts
3		15pts
4		25pts
5		20pts
Total		100pts

Question 1.

a. Find the largest prime divisor of $42! + 43! + 44!$. **(7 pts)**

b. Show that 495 divides $21^{240} - 36^{120}$. **(8 pts)**

c. Find the greatest common divisor of 1365 and 4264 using Euclidean Algorithm. **(5 pts)**

Question 2. Consider the permutations

$$\pi = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 \\ 3 & 4 & 1 & 5 & 2 \end{pmatrix}$$
$$\sigma = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 \\ 5 & 3 & 4 & 2 & 1 \end{pmatrix}$$

a) Calculate the order, sign of the permutations π, σ and $\pi\sigma$ (show the formula that you use in each case). **(10 pts)**

b) Find an element τ in $S(5)$ satisfying

$$\tau\pi\tau^{-1} = \sigma.$$

[Hint: You may assume that τ is given by $\begin{pmatrix} 1 & 2 & 3 & 4 & 5 \\ a & b & c & d & e \end{pmatrix}$ and solve a, b, c, d, e.] **(10 pts)**

Question 3. Let p and q be two distinct primes. Consider the group $(\mathbb{Z}_p, +)$ and the map

$$\begin{aligned} \varphi\colon \mathbb{Z}_p &\to \mathbb{Z}_p \\ x &\mapsto qx \bmod p. \end{aligned}$$

Show that φ is an injective group homomorphism. **(15 pts)**

Question 4.

a. What is the order of the group $(\mathbb{Z}_n \times \mathbb{Z}_m, +)$? [The group operation is given by $(a, b) + (c, d) = (a + c, b + d)$ for all $(a, b), (c, d) \in \mathbb{Z}_n \times \mathbb{Z}_m$.] **(6 pts)**

b. Define the subset L of $\mathbb{Z}_n \times \mathbb{Z}_m$ by

$$L = \{(x, y) \in \mathbb{Z}_n \times \mathbb{Z}_m \mid x - y = 0\}.$$

Show that L is a subgroup of $\mathbb{Z}_n \times \mathbb{Z}_m$. **(10 pts)**

c. Assume that $n \leq m$. Determine the number of distinct cosets of L in $\mathbb{Z}_n \times \mathbb{Z}_m$. **(9 pts)**

Question 5.

a. Let f be a linear code function generated by the matrix

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

Using the corresponding parity check matrix, determine whether the following are codewords or not.

$$11101000,\ 01110111,\ 10001001.$$

(10 pts)

b. Find an example of a linear code $f\colon \mathbb{B}^4 \to \mathbb{B}^8$ with minimum distance 4 or prove that such code does not exist. **(10 pts)**

SCRATCH PAPER

MAT 312 - AMS 351 FINAL EXAM

SUMMER II, 14 August 2014

Question 1.

a. Find all four solutions to the equation $x^2 - 1 \equiv 0 \bmod 35$. **(5 pts)**

b. Solve the equation $[243]_n \cdot [x]_n \equiv [1]_n$ for $n = 1130$. **(7 pts)**

c. Find the last three digits of the integer

$$2003^{2002^{2001}}.$$

(8 pts)

Proof. **a.** Clearly, $1^2 = (-1)^2 \equiv \bmod 35$. Since, $1 \equiv 36 \bmod 35$, we see that 6 and -6 are also solutions to $x^2 \equiv 1 \bmod 35$. Therefore, the solutions are $[1]_{35}, [6]_{35}$, $[-6]_{35}, [-1]_{35}$, or equivalently, $[1]_{35}, [6]_{35}, [29]_{35}, [34]_{35}$.

b. We need to calculate the multiplicative inverse of 243 modulo 1130. By the Euclidean algorithm,

$$\begin{aligned} 1130 &= 4 \cdot 243 + 158 \\ 243 &= 1 \cdot 158 + 85 \\ 158 &= 1 \cdot 85 + 73 \\ 85 &= 1 \cdot 73 + 12 \\ 73 &= 6 \cdot 12 + 1 \\ 12 &= 1 \cdot 12. \end{aligned}$$

(This also confirms that $(1130, 243) = 1$ and the multiplicative inverse of 243 modulo 1130 does exist. Now we find a form $a \cdot 243 + b \cdot 1130 = 1$ for some $a, b \in \mathbb{Z}$. By the

algorithm above,

$$\begin{aligned}
1 &= 73 - 6 \cdot 12 \\
&= 73 + 6(73 - 85) \\
&= 7 \cdot 73 - 6 \cdot 85 \\
&= 7(158 - 85) - 6 \cdot 85 \\
&= 7 \cdot 158 - 13 \cdot 85 \\
&= 7 \cdot 158 - 13(243 - 158) \\
&= 20 \cdot 158 - 13 \cdot 243 \\
&= 20(1130 - 4 \cdot 243) - 13 \cdot 243 \\
&= 20 \cdot 1130 - 93 \cdot 243.
\end{aligned}$$

So, the inverse is $[-93]_{1130}$, or equivalently, $[1037]_{1130}$. Multiplying the both sides of $[243]_n \cdot [x]_n \equiv [1]_n$ by $[1037]_{1130}$ gives $[x]_{1130} = [1037]_{1130}$.

c. We are asked to calculate

$$2003^{2002^{2001}} \bmod 1000.$$

We have $\phi(1000) = \phi(2^3 5^3) = 4 \cdot 100 = 400$. So, by Euler's Theorem, for any $a \in \mathbb{Z}$ with $(a, 1000) = 1$, we have $a^{400} \equiv 1 \bmod 1000$. Using that we calculate

$$\begin{aligned}
2003^{2002^{2001}} &\equiv 3^{2002^{2001}} \\
&\equiv \left((3^{400})^5 3^2\right)^{2001} \\
&\equiv \left(1^5 3^2\right)^{2001} \\
&\equiv 9^{2001} \\
&\equiv (9^{400})^5 9 \equiv 9 \bmod 1000.
\end{aligned}$$

□

Question 2. Consider the permutations

$$\pi = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 & 7 & 8 & 9 & 10 & 11 & 12 \\ 9 & 5 & 10 & 11 & 7 & 1 & 12 & 4 & 3 & 2 & 8 & 6 \end{pmatrix}$$

$$\sigma = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 & 7 & 8 & 9 & 10 & 11 & 12 \\ 1 & 4 & 10 & 8 & 2 & 7 & 9 & 12 & 11 & 3 & 5 & 6 \end{pmatrix}$$

a) Write π and σ as a product of disjoint cycles. **(6 pts)**

b) Calculate the order, sign of the permutations π, σ and $\pi\sigma$ (show the formula that you use in each case). **(14 pts)**

Proof. *a*) $\pi = (1\ 9\ 3\ 10\ 2\ 5\ 7\ 12\ 6)(4\ 11\ 8)$, $\sigma = (2\ 4\ 8\ 12\ 6\ 7\ 9\ 11\ 5)(3\ 10)$.

b) $\pi\sigma = (1\ 9\ 8\ 6\ 12)(2\ 11\ 7\ 3)$.

$$\begin{aligned} \operatorname{ord}(\pi) &= \operatorname{lcm}(9,3) = 9, \\ \operatorname{ord}(\sigma) &= \operatorname{lcm}(9,2) = 18, \\ \operatorname{ord}(\pi\sigma) &= \operatorname{lcm}(5,4) = 20, \\ \operatorname{sgn}(\pi) &= (-1)^{9-1}(-1)^{3-1} = 1, \\ \operatorname{sgn}(\sigma) &= (-1)^{9-1}(-1) = -1, \\ \operatorname{sgn}(\pi\sigma) &= (-1)^{5-1}(-1)^{4-1} = -1. \end{aligned}$$

□

Question 3.

a. Find the smallest subgroup of $S(5)$ which contains both of the permutations $\pi = (1\ 4\ 5)$ and $\sigma = (1\ 4)$. **(10 pts)**

b. What is the order of the subgroup? **(4 pts)**

c. Determine the number of distinct cosets of the (same) subgroup in $S(5)$ without listing them. **(6 pts)**

Proof. **a.** Let us denote the smallest subgroup containing π and σ by H. Since H is a subgroup, it must contain the identity permutation id and the inverse of each member, and it must be closed under the composition. So $\pi^{-1}, \sigma^{-1}, \mathrm{id} \in H$. Also, all positive powers of π and σ must belong to H. Since, the length of π is 3, we have $\pi^3 = \mathrm{id}$. Similarly, $\sigma^2 = \mathrm{id}$. We have

$$\begin{aligned} \pi^2 &= \pi^{-1} = (1\ 5\ 4), \\ \sigma^{-1} &= \sigma = (1\ 4), \\ \pi\sigma &= (1\ 5), \\ \sigma\pi &= (4\ 5). \end{aligned}$$

Moreover,

$$(\pi\sigma)\pi = \sigma,\ \pi\sigma\pi^2 = \sigma\pi,\ \pi^2\sigma\pi = \pi\sigma,\ \pi^2\sigma = \sigma\pi,\ \sigma\pi^2 = \pi\sigma,\ \sigma\pi\sigma = \pi^{-1},\ \pi\sigma\pi = \sigma.$$

So, $H = \{\mathrm{id}, (1\ 4\ 5), (1\ 4), (1\ 5\ 4), (1\ 5), (4\ 5)\}$ and it is closed under composition.

b. The order of a group is equal to the number of its elements. Therefore, the order of H is 6.

c. The order of $S(5)$ is equal to $5! = 120$. By Lagrange's Theorem,

$$\text{the number of cosets of } H = \frac{\mathrm{ord}(S(5))}{\mathrm{ord}(H)} = \frac{120}{6} = 20.$$

□

Question 4. Let $f\colon G \to H$ be a group homomorphism. Define the set

$$K = \{g \in G \mid f(g) = e_H\}$$

where e_H is the identity element in H.

a) Prove that K is subgroup of G. **(10 pts)**
b) Prove that f is injective if and only if $K = \{e_G\}$. **(10 pts)**

Proof. *a*) Let $g_1, g_2 \in K$. Then, by the definition of K, g_1 and g_2 are mapped to the identity of H by f. We have

$$f(g_1g_2) = f(g_1)f(g_2) = e_He_H = e_H$$

So, $g_1g_2 \in K$. Also, $f(g_1) = e_H$ implies that $(f(g_1))^{-1} = e_H$ (here, $(f(g_1))^{-1}$ is the inverse of $f(g_1)$ with respect to the group operation over H). By the properties of group homomorphisms, $(f(g_1))^{-1} = f(g_1^{-1})$. Therefore, $g_1^{-1} \in K$. Hence, K is a subgroup of G.

Note. We can also show that $g^{-1} \in K$ for any $g \in K$ as follows. Since $g \in K$, we have

$$e_H = f(e_G) = f(g \cdot g^{-1}) = f(g)f(g^{-1}) = e_Hf(g^{-1}) = f(g^{-1}).$$

Therefore, $g^{-1} \in K$.

b) Assume that $K = \{e_G\}$. Let $g_1, g_2 \in G$ such that $f(g_1) = f(g_2)$. Then, $f(g_1)(f(g_2))^{-1} = e_H$. Since f is group homomorphism

$$f(g_1)(f(g_2))^{-1} = f(g_1)f(g_2^{-1}) = f(g_1g_2^{-1}) = e_H$$

which implies that $g_1g_2^{-1} \in K$. Since $K = \{e_G\}$, we must have $g_1g_2^{-1} = e_G$, equivalently, $g_1 = g_2$. Hence, $f\colon G \to H$ is injective.

Now, assume that f is injective. Let $k \in K$. Then $f(k) = e_H$. We also have $f(e_G) = e_H$ since f is a group homomorphism. However, by the assumption, f is injective, and $f(k) = f(e_G)$ implies that $k = e_G$. Therefore $K = \{e_G\}$. □

Question 5. Calculate the two column decoding table (which is formed by syndromes and coset leaders) for the code generated by the matrix

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

A message is encoded using the letter equivalents

$$000 = \text{ M},\ 010 = \text{ B},\ 001 = \text{ T},\ 100 = \text{ A},$$

$$110 = \text{ S},\ 101 = \text{ H},\ 011 = \text{ E},\ 111 = \text{ C}$$

and received as

$$0010000,\ 1101011,\ 0011001,\ 1010110.$$

Correct and decode the received message. **(20 pts)**

Proof. The parity check matrix is given by

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

The rows from the 2nd to the 8th are formed by the rows of M in the two column decoding table. We fill the rows by adding the missing syndromes (which spans the whole $\mathbb{B}^4$. We get

0000	0000000
1011	1000000
0111	0100000
1001	0010000
1000	0001000
0100	0000100
0010	0000010
0001	0000001
1010	
1100	
0101	
0110	
0011	
1101	
1110	
1111	

Next, we calculate the coset leaders. Notice that each syndrome can be written as the sum of two or more syndromes. For example, $1010 = 1000+0010$. (Note that this is not a unique presentation.) Then we can choose the coset leader corresponding to 1010 to be the sum of coset leaders corresponding to 1000 and 0010. Repeating that for the rest of the syndromes we can fill the table as follows.

0000	0000000
1011	1000000
0111	0100000
1001	0010000
1000	0001000
0100	0000100
0010	0000010
0001	0000001
1010	0001010
1100	0001100
0101	0000101
0110	0000110
0011	0000011
1101	0010100
1110	0001110
1111	0001111.

In order the correct the received message, we calculate the syndromes

$$\begin{aligned} 0010000 \cdot M &= 1001, \\ 1101011 \cdot M &= 0111, \\ 0011001 \cdot M &= 0000, \\ 1010110 \cdot M &= 0100. \end{aligned}$$

We add the corresponding coset leaders to the words to get

$$\begin{aligned} 0010000 + 0010000 &= 0000000, \\ 1101011 + 0100000 &= 1001011, \\ 0011001 + 0000000 &= 0011001, \\ 1010110 + 0000100 &= 1010010. \end{aligned}$$

Therefore the original message is 000, 100, 001, 101, which reads "MATH".

□

Question 6.

a. Let $f\colon \mathbb{B}^4 \to \mathbb{B}^5$ be a function defined by $f(w) = wM$ where M is the matrix

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

Show whether f is a code function or not. **(5 pts)**

b. Let $W = \{000000, 101110, 001010, 110111, 100100, 011001, 111101, 010011\}$ be the set of codewords for some linear code function. Find a generator matrix for the code. Determine the minimum distance, and the number of errors that can be detected and corrected by the code. **(8 pts)**

c. Let $d(x, y)$ be the distance between two words $x, y \in \mathbb{B}^n$. Prove that for any $x, y, z \in \mathbb{B}^n$,

- $d(x, y) \geq 0$, with equality if and only if $x = y$,
- $d(x, y) = d(y, x)$,
- $d(x, y) \leq d(x, z) + d(z, y)$. **(7 pts)**

Proof. **a.** It is not a code word since it is not injective. For example, both 0001 and 1100 are mapped to 01110.

b. We can take

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

The minimal distance is 2. So, the code function can detect 1 error but correct none.

c. Note that $d(x, y) = \mathrm{wt}(x + y)$ and it counts the number of digits that differ between x and y.

- $d(x, y) \geq 0$, with equality if and only if $x = y$. This is clear since, by definition, the weight cannot be negative, and all the 1s in x can be cancelled only by adding x to x.
- $d(x, y) = d(y, x)$. This follows from $\mathrm{wt}(x + y) = \mathrm{wt}(y + x)$.
- $d(x, y) \leq d(x, z) + d(z, y)$. First notice that $\mathrm{wt}(x + y) \leq \mathrm{wt}(x) + \mathrm{wt}(y)$ (by adding x to y we cannot produce a word with more 1s). Secondly, $\mathrm{wt}(x) + \mathrm{wt}(y) = \mathrm{wt}(x + z) + \mathrm{wt}(y + z)$ for any word z (if x and y agree on the ith digit then adding another word z to x and y does not change the sum of the new values on the ith digit). This completes the proof.

□

Homework Week 2

29 July 2014

Deadline: 7 August 2014, 13:00.

Let π and σ be permutations in $S(9)$ given by

$$\begin{aligned}\pi &= \begin{pmatrix}1&2&3&4&5&6&7&8&9\\2&3&7&1&6&5&4&9&8\end{pmatrix},\\ \sigma &= \begin{pmatrix}1&2&3&4&5&6&7&8&9\\9&5&6&8&7&1&2&4&3\end{pmatrix}.\end{aligned}$$

1. *Write π and σ as a product of disjoint cycles.* **(2 pts)**

$$\begin{aligned}\pi &= \begin{pmatrix}1&2&3&4&5&6&7&8&9\\2&3&7&1&6&5&4&9&8\end{pmatrix} = (1\ 2\ 3\ 7\ 4)(5\ 6)(8\ 9),\\ \sigma &= \begin{pmatrix}1&2&3&4&5&6&7&8&9\\9&5&6&8&7&1&2&4&3\end{pmatrix} = (1\ 9\ 3\ 6)(2\ 5\ 7)(4\ 8).\end{aligned}$$

2. *Check whether $\pi\sigma$ is equal to $\sigma\pi$ or not. Find* $\mathrm{ord}(\pi\sigma)$ *and* $\mathrm{sgn}(\pi\sigma)$. **(2 pts)**

We have

$$\begin{aligned}\pi\sigma &= (1\ 8)(2\ 6)(3\ 5\ 4\ 9\ 7),\\ \sigma\pi &= (1\ 5)(2\ 6\ 7\ 8\ 3)(4\ 9).\end{aligned}$$

So $\sigma\pi \neq \pi\sigma$. Now it follows from those factorisations that

$$\begin{aligned}\mathrm{ord}(\pi\sigma) &= \mathrm{lcm}(2,2,5) = 10,\\ \mathrm{sgn}(\pi\sigma) &= \mathrm{sgn}(1\ 8)\cdot\mathrm{sgn}(2\ 6)\cdot\mathrm{sgn}(3\ 5\ 4\ 9\ 7) = (-1)(-1)(-1)^4 = 1.\end{aligned}$$

3. *Find* $\mathrm{ord}(\pi)$, $\mathrm{ord}(\sigma)$, $\mathrm{sgn}(\pi)$ *and* $\mathrm{sgn}(\sigma)$. **(2 pts)**

Use the factorisations in Question 1 to get

$$\begin{aligned}\mathrm{ord}(\pi) &= \mathrm{lcm}(2,2,5) = 10,\\ \mathrm{sgn}(\pi) &= \mathrm{sgn}(1\ 2\ 3\ 7\ 4)\cdot\mathrm{sgn}(5\ 6)\cdot\mathrm{sgn}(8\ 9) = (-1)^4(-1)(-1) = 1.\\ \mathrm{ord}(\sigma) &= \mathrm{lcm}(2,3,4) = 12,\\ \mathrm{sgn}(\sigma) &= \mathrm{sgn}(1\ 9\ 3\ 6)\cdot\mathrm{sgn}(2\ 5\ 7)\cdot\mathrm{sgn}(4\ 8) = (-1)^3(-1)^2(-1) = 1.\end{aligned}$$

4. *Exercise 4.2.4. Show that if π and σ are any permutations such that $(\pi\sigma)^2 = \pi^2\sigma^2$ then $\pi\sigma = \sigma\pi$.* **(2 pts)**

By the assumption,

$$(\pi\sigma)^2 = \pi\sigma\pi\sigma = \pi^2\sigma^2.$$

Multiply both sides on the left by π^{-1} to get

$$\sigma\pi\sigma = \pi\sigma^2.$$

Now on the right by σ^{-1} to get

$$\pi\sigma = \sigma\pi.$$

5. *Compute the order and sign of the non-disjoint cycles* $(1\ 3\ 5)(4\ 6)(1\ 2\ 4)(3\ 5\ 7)$ *and* $(1\ 4\ 7\ 3)(3\ 2\ 5)(1\ 6\ 4)(2\ 3\ 6\ 7)$. *[Hint: Write each of them as a product of disjoint cycles.]* **(2 pts)**

We have

$$\begin{aligned} \pi_1 &= (1\ 3\ 5)(4\ 6)(1\ 2\ 4)(3\ 5\ 7) = (1\ 2\ 6\ 4\ 3)(5\ 7) \\ \pi_2 &= (1\ 4\ 7\ 3)(3\ 2\ 5)(1\ 6\ 4)(2\ 3\ 6\ 7) = (1\ 6\ 3\ 7\ 5). \end{aligned}$$

So,

$$\begin{aligned} \mathrm{ord}(\pi_1) &= \mathrm{lcm}(2,5) = 10, \\ \mathrm{sgn}(\pi_1) &= \mathrm{sgn}(1\ 2\ 6\ 4\ 3)\cdot\mathrm{sgn}(5\ 7) = (-1)^4(-1) = -1, \\ \mathrm{ord}(\pi_2) &= 5, \\ \mathrm{sgn}(\pi_2) &= \mathrm{sgn}(1\ 6\ 3\ 7\ 5) = (-1)^4 = 1. \end{aligned}$$

6. *Exercise 4.3.4. Let G be a group and let c be a fixed element of G. Define a new operation "$*$" on G by*

$$a * b = ac^{-1}b.$$

Prove that G is a group under $*$. **(2 pts)**

We need to show that $(G, *)$ satisfies the group axioms. Notice that the new operation $*$ is given in terms of the initial operation on G which makes it into a group. So, a^{-1} exists for any $a \in G$.

(1) Clearly, $ac^{-1}b \in G$ since G is closed under the the initial operation (multiplication). So, $a * b \in G$.

(2) Let $a, b, d \in G$. Then

$$\begin{aligned} (a * b) * d &= (ac^{-1}b) * d = (ac^{-1}b)c^{-1}d \\ a * (b * d) &= a * (bc^{-1}d) = ac^{-1}(bc^{-1}d). \end{aligned}$$

Since $a(bc) = (ab)c$ for any $a, b, c \in G$, the calculation above shows that $(a*b)*d = a*(b*d)$. So, $*$ is associative.

(3) An element $b \in G$ is called the identity element (with respect to $*$) if, for any $a \in G$, $a * b = a$. We need to solve b from

$$a * b = ac^{-1}b = a.$$

First, multiply both sides of $ac^{-1}b = a$ on the left by a^{-1} to get

$$c^{-1}b = a^{-1}a = e$$

where e is the identity element with respect to the initial operation (i.e. multiplication). Now, multiplying both sides on the left by c gives $b = ce = c$. Hence, c is the identity element with respect to $*$.

(4) An element $b \in G$ is called the inverse of an element $a \in G$ (with respect to $*$) if $a * b = c$ (c is the identity element). We have

$$\begin{aligned} a * b = c &\Leftrightarrow ac^{-1}b = c \\ &\Leftrightarrow c^{-1}b = a^{-1}c \\ &\Leftrightarrow b = ca^{-1}c. \end{aligned}$$

Hence the inverse of $a \in G$ with respect to $*$ is $ca^{-1}c$.

Since $(G, *)$ satisfies all four axioms, it is a group.

7. *Determine whether the following are groups are not.* **(2 pts)**

• $\mathbb{R}$ with $*$ defined by $a * b = a + b + ab$ for all $a, b \in \mathbb{R}$.

This is not a group. Clearly, $a * b = a + b + ab \in \mathbb{R}$. So, $\mathbb{R}$ is closed under $*$. The operation is associative since, for any $a, b, c \in \mathbb{R}$, we have

$$a * (b * c) = a * (b + c + bc) = a + (b + c + bc) + a(b + c + bc) = a + b + c + ab + ac + bc + abc,$$

$$(a * b) * c = (a + b + ab) * c = (a + b + ab) + c + c(a + b + ab) = a + b + c + ab + ac + bc + abc,$$

and $a * (b * c) = (a * b) * c$. Furthermore, the identity element is $0 \in \mathbb{R}$. However, $-1 \in \mathbb{R}$ does not have an inverse. It may be observed as follows. By definition, b is the inverse of an element $a \in \mathbb{R}$ with respect to $*$ if $a * b = 0$. We can solve b from $a * b = a + b + ab = 0$ to be $-\frac{a}{1+a}$ if and only if $a \neq -1$. In other words, b is not well defined if $a = -1$.

• $\mathbb{Z} \times \mathbb{Z}$ with $*$ defined by $(a, b) * (c, d) = (ad + bc, bd)$ for all $a, b, c, d \in \mathbb{Z}$.

This is not a group. (1) For any $a, b, c, d \in \mathbb{Z}$, $ad + bc \in \mathbb{Z}$. Hence, $(a, b) * (c, d) = (ad + bc, bd) \in \mathbb{Z} \times \mathbb{Z}$.

(2) The operation $*$ is associative: Let $(a, b), (c, d), (g, h) \in \mathbb{Z} \times \mathbb{Z}$. Then

$$[(a, b) * (c, d)] * (g, h) = (ad + bc, bd) * (g, h) = ((ad + bc)h + bdg, bdh) = (adh + bch + bdg, bdh)$$

and

$$(a, b) * [(c, d) * (g, h)] = (a, b) * (ch + dg, dh) = ((adh + b(ch + dg), bdh) = (adh + bch + bdg, bdh).$$

(3) The identity element is $(0, 1)$: Assume that $(a, b) * (c, d) = (a, b)$ and solve $(a, b) * (c, d) = (ad + bc, bd) = (a, b)$ in terms of c and d. So, $ad + bc = a$ and $bd = b$. These equalities have solution only for $c = 0$ and $d = 1$.

However,

(4) The inverse element does not exist in $\mathbb{Z} \times \mathbb{Z}$. For any $(a, b) \in \mathbb{Z} \times \mathbb{Z}$, $(c, d) \in \mathbb{Z} \times \mathbb{Z}$ is called the inverse if $(a, b) * (c, d) = (0, 1)$, equivalently, $ad + bc = 0$ and $bd = 1$. But $d = \frac{1}{b} \notin \mathbb{Z}$ unless $b = 1$ or $b = -1$.

8. *Exercise 4.3.2. Let G be a group and let a, b be elements of G. Show that*

$$(ab)^{-1} = b^{-1}a^{-1}.$$

Give an example of a group G with elements a, b for which $(ab)^{-1} \neq a^{-1}b^{-1}$. [Warning: Do not give the same answer as the one given in the book.] **(2 pts)**

By definition, $(ab)^{-1}(ab) = e$. Multiply both sides on the right by b^{-1} to get $(ab)^{-1}a = b^{-1}$. Now, by a^{-1} to get $(ab)^{-1} = b^{-1}a^{-1}$.

As for an example, let $G = \mathrm{GL}(2, \mathbb{R})$ and choose

$$a = \begin{pmatrix} 1 & 2 \\ 0 & 1 \end{pmatrix}, \quad b = \begin{pmatrix} 1 & 0 \\ 3 & 1 \end{pmatrix}$$

Then,

$$a^{-1} = \begin{pmatrix} 1 & -2 \\ 0 & 1 \end{pmatrix}, \quad b^{-1} = \begin{pmatrix} 1 & 0 \\ -3 & 1 \end{pmatrix}.$$

We find

$$(ab)^{-1} = \begin{pmatrix} 1 & -2 \\ -3 & 7 \end{pmatrix}$$

but

$$a^{-1}b^{-1} = \begin{pmatrix} 7 & -2 \\ -3 & 1 \end{pmatrix}.$$

9. *Exercise 4.3.3. Let G be a group in which $a^2 = e$ for all $a \in G$. Show that G is Abelian.*

(2 pts)

By the assumption, $aa = e$ for all $a \in G$. So, $a^{-1} = a$. Also, for any $a, b \in G$, $ab \in G$ since G is a group. Therefore $(ab)^2 = e$. It follows that

$$(ab)(ab) = e \Leftrightarrow abab b^{-1} = eb^{-1} \Leftrightarrow aba = b^{-1} = b \Leftrightarrow abaa^{-1} = ba^{-1} \Leftrightarrow ab = ba.$$

10. *Is the subset $\{(1\ 2\ 4), (2\ 3)(1\ 4), (1\ 3)(2\ 4)\}$ a subgroup of $S(4)$? Why (not)?*

(2 pts)

One of the conditions we need to check is that for any $a, b \in \{(1\ 2\ 4), (2\ 3)(1\ 4), (1\ 3)(2\ 4)\}$, the product ab also belongs to $\{(1\ 2\ 4), (2\ 3)(1\ 4), (1\ 3)(2\ 4)\}$. However,

$$(1\ 2\ 4)(2\ 3)(1\ 4) = (2\ 3\ 4)$$

and $(2\ 3\ 4) \notin \{(1\ 2\ 4), (2\ 3)(1\ 4), (1\ 3)(2\ 4)\}$. Therefore it is not a subgroup. (Another direct observation is that the identity permutation id is not in the given subset.)

11. *Find the generators of the group $\mathbb{Z}_{18}$ under addition, and list all of its subgroups.*

(2 pts)

It is easy to see that $\mathbb{Z}_{18}$ is cyclic and generated by $[1]_{18}$. It can also be generated by $n \cdot [1]_{18}$ if and only if $(n, 18) = 1$. Therefore

$$\mathbb{Z}_{18} = \langle [1]_{18} \rangle = \langle [5]_{18} \rangle = \langle [7]_{18} \rangle = \langle [11]_{18} \rangle = \langle [13]_{18} \rangle = \langle [17]_{18} \rangle.$$

The subgroups are

$$\begin{aligned}
\langle [0]_{18} \rangle &= \{0\} \\
\langle [2]_{18} \rangle &= \{[0]_{18}, [2]_{18}, [4]_{18}, [6]_{18}, [8]_{18}, [10]_{18}, [12]_{18}, [14]_{18}, [16]_{18}\} \\
&= \langle [4]_{18} \rangle = \langle [8]_{18} \rangle = \langle [10]_{18} \rangle = \langle [14]_{18} \rangle = \langle [16]_{18} \rangle \\
\langle [3]_{18} \rangle &= \{[0]_{18}, [3]_{18}, [6]_{18}, [9]_{18}, [12]_{18}, [15]_{18}\} = \langle [15]_{18} \rangle \\
\langle [6]_{18} \rangle &= \{[0]_{18}, [6]_{18}, [12]_{18}\} = \langle [12]_{18} \rangle \\
\langle [9]_{18} \rangle &= \{[0]_{18}, [9]_{18}\}.
\end{aligned}$$

12. *Consider $(G_8, \cdot\,)$, the group of invertible congruence classes modulo 8. Write down the distinct left cosets of the subgroup $\{[1]_8, [5]_8\}$.* **(1 pts)**

We have $G_8 = \{[1]_8, [3]_8, [5]_8, [7]_8\}$. So,

$$\begin{aligned}
[1]_8\{[1]_8, [5]_8\} &= \{[1]_8, [5]_8\} = [5]_8\{[1]_8, [5]_8\}, \\
[3]_8\{[1]_8, [5]_8\} &= \{[3]_8, [7]_8\} = [7]_8\{[1]_8, [5]_8\}.
\end{aligned}$$

Therefore, the order of each coset is 2.

13. *What are the possible orders of elements of $(G_{15}, \cdot\,)$ and which of these integers are actually orders of elements of G_{15}?* **(2 pts)**

We have $\phi(15) = \phi(3)\phi(5) = 8$. Therefore, the possible orders are $1, 2, 4, 8$. Let us calculate the subgroups generated by each element in G_{15}.

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

Hence, there are elements of orders $1, 2$ and 4 but no element with order 8.

HOMEWORK WEEK 4

05 AUGUST 2014

Deadline: 12 August 2014, TUESDAY 13:00. (Notice the change of day.)

Q. 1. *Show whether the groups G_{10} and G_7 are cyclic or not. If so, determine their generators.*

Proof. The subgroups generated by the elements of G_7 are

$$\begin{aligned}
\langle [1]_7 \rangle &= \{[1]_7\}, \\
\langle [2]_7 \rangle &= \{[1]_7, [2]_7, [4]_7, [6]_7\}, \\
\langle [3]_7 \rangle &= \{[1]_7, [2]_7, [3]_7, [4]_7, [5]_7, [6]_7\}, \\
\langle [4]_7 \rangle &= \{[1]_7, [4]_7\}, \\
\langle [5]_7 \rangle &= \{[1]_7, [2]_7, [3]_7, [4]_7, [5]_7, [6]_7\}, \\
\langle [6]_7 \rangle &= \{[1]_7, [6]_7\}.
\end{aligned}$$

Therefore $G_7 = \langle [1]_7 \rangle = \langle [5]_7 \rangle$ and G_7 is cyclic.

Over $G_{10} = \{[1]_{10}, [3]_{10}, [7]_{10}, [9]_{10}\}$, we have

$$\begin{aligned}
\langle [1]_{10} \rangle &= \{[1]_{10}\}, \\
\langle [3]_{10} \rangle &= \{[1]_{10}, [3]_{10}, [7]_{10}, [9]_{10}\}, \\
\langle [7]_{10} \rangle &= \{[1]_{10}, [3]_{10}, [7]_{10}, [9]_{10}\}, \\
\langle [9]_{10} \rangle &= \{[1]_{10}, [9]_{10}\}.
\end{aligned}$$

Therefore $G_{10} = \langle [1]_{10} \rangle = \langle [7]_{10} \rangle$ and G_{10} is cyclic. **(4 pts)** □

Q. 2. *Let $(G, *)$ and $(H, \circ)$ be two groups. Consider the cartesian product $G \times H$ with the operation $(g_1, h_1)(g_2, h_2) = (g_1 * g_2, h_1 \circ h_2)$ for all $(g_1, h_1), (g_2, h_2) \in G \times H$. Show that $G \times H$ is a group. Prove that $G \times H$ is Abelian (commutative) if and only if both G and H are Abelian.*

Proof. First, we show that $G \times H$ is a gorup. We go through the four group axioms.

(1) For all $(g_1, h_1), (g_2, h_2) \in G \times H$, we have $(g_1, h_1)(g_2, h_2) = (g_1 * g_2, h_1 \circ h_2)$ and $g_1 * g_2 \in G$, $h_1 \circ h_2 \in H$. So $(g_1, h_1)(g_2, h_2) \in G \times H$. This shows that $G \times H$ is closed under the group operation.

(2) For all $(g_1, h_1), (g_2, h_2), (g_3, h_3) \in G \times H$, we have

$$[(g_1, h_1)(g_2, h_2)](g_3, h_3) = (g_1 * g_2, h_1 \circ h_2)(g_3, h_3) = ((g_1 * g_2) * g_3, (h_1 \circ h_2) \circ h_3).$$

Notice that $(g_1 * g_2) * g_3 = g_1 * (g_2 * g_3)$ since G is a group. Similarly, $(h_1 \circ h_2) \circ h_3) = h_1 \circ (h_2 \circ h_3)$. So, continuing from the last equation

$$\begin{aligned}
((g_1 * g_2) * g_3, (h_1 \circ h_2) \circ h_3) &= (g_1 * (g_2 * g_3), h_1 \circ (h_2 \circ h_3)) \\
&= (g_1, h_1)(g_2 * g_3, h_2 \circ h_3) \\
&= (g_1, h_1)[(g_2, h_2)(g_3, h_3)].
\end{aligned}$$

Therefore, the group operation is associative.

(3) The identity element is (e_G, e_H) where e_G is the identity element in $(G, *)$ and e_H is the identity element in $(H, \circ)$.

(4) The inverse of $(g, h) \in G \times H$ is $(g', h') \in G \times H$ where g' is the inverse of g with respect to $*$ in G and h' is the inverse of h with respect to $\circ$ in H. Since all four axioms are satisfied, we conclude that $G \times H$ is a group.

Now let us show the second part of the question. Let $(g_1, h_1), (g_2, h_2) \in G \times H$. Then,

$$(g_1, h_1)(g_2, h_2) = (g_1 * g_2, h_1 \circ h_2)$$

and

$$(g_2, h_2)(g_1, h_1) = (g_2 * g_1, h_2 \circ h_1).$$

By definition, $G \times H$ is commutative if and only if $(g_1, h_1)(g_2, h_2) = (g_2, h_2)(g_1, h_1)$. The latter holds if and only if $(g_1 * g_2, h_1 \circ h_2) = (g_2 * g_1, h_2 \circ h_1)$, that is, if and only if $g_1 * g_2 = g_2 * g_1$ and $h_1 \circ h_2 = h_2 \circ h_1$, in other words, G and H both are commutative. **(4 pts)** □

Q. 3. *Show that $\mathbb{Z} \times \mathbb{Z}$ is not cyclic.*

Proof. The standard group operation on $\mathbb{Z} \times \mathbb{Z}$ is given by $(a, b)(c, d) = (a + c, b + d)$ for $(a, b), (c, d) \in \mathbb{Z} \times \mathbb{Z}$. We will say that $\mathbb{Z} \times \mathbb{Z}$ is cyclic if and only if it can be generated by a single element $(x, y) \in \mathbb{Z} \times \mathbb{Z}$. That is, if any $(a, b) \in \mathbb{Z} \times \mathbb{Z}$ can be written as $(a, b) = (nx, ny)$ for some $n \in \mathbb{Z}$. The equality $(a, b) = (nx, ny)$ has a solution for n if and only if $n = \frac{a}{x}$ and $n = \frac{b}{y}$. The common divisor of all integers is 1 (or -1). So, x, y must be 1 or -1. However, $(1, 1)$ can only generate the elements of the form $(a, a) \in \mathbb{Z} \times \mathbb{Z}$ and $(1, -1)$ can generate the elements of the form $(a, -a) \in \mathbb{Z} \times \mathbb{Z}$. Therefore, $\mathbb{Z} \times \mathbb{Z}$ is not cyclic. **(1 pt)** □

Q. 4. *Consider $\mathbb{R}^2 = \mathbb{R} \times \mathbb{R}$ as a group with the addition defined by $(a, b) + (c, d) = (a + b, c + d)$ for all $(a, b), (c, d) \in \mathbb{R}^2$. Show that the function $f \colon \mathbb{R}^2 \to \mathbb{R}^2$ given by $f(x, y) = (x, x)$ is a group homomorphism.*

Proof. The condition for f to be a group homomorphism is that

$$f((a, b) + (c, d)) = f(a, b) + f(c, d)$$

for all $(a, b), (c, d) \in \mathbb{R}^2$. By the assumption, $f((a, b) + (c, d)) = f(a + c, b + d) = (a + c, a + c)$. On the other hand,

$$f(a, b) + f(c, d) = (a, a) + (c, c) = (a + c, a + c)$$

Therefore, $f((a, b) + (c, d)) = f(a, b) + f(c, d)$ and f is a group homomorphism. **(1 pt)** □

Q. 5. *Exercise 5.3.3. Let G be any group and g be an element of G. Define the function $f \colon G \to G$ by $f(a) = g^{-1}ag$ for $a \in G$. Show that f is an isomorphism G to itself.*

Proof. First of all, f is a group homomorphism since for any $a, b \in G$, we have

$$f(ab) = g^{-1}abg = g^{-1}agg^{-1}bg = (g^{-1}ag)(g^{-1}bg) = f(a)f(b).$$

So, we need to show that f is bijective.

Let $a, b \in G$ and assume that $f(a) = f(b)$. Then

$$g^{-1}ag = g^{-1}bg \Leftrightarrow ag = bg \Leftrightarrow a = b.$$

Hence, f is one-to-one.

Now, let $b \in G$. Then $g^{-1}ag = b$ if and only if $ag = gb$, and the latter holds if and only if $a = gbg^{-1}$. Hence $b = f(a)$ for $a = gbg^{-1} \in G$, and f is surjective.

Therefore f is an isomorphism of G to itself. **(3 pts)** □

Q. 6. *Exercise 5.2.4. Let H be a subgroup of the group G and let a be an element of G. Fix an element b in aH (so $b = ah$ for some $h \in H$). Show that*

$$H = \{b^{-1}c \mid c \in aH\}.$$

Proof. Let us denote the set $\{b^{-1}c \mid c \in aH\}$ by K and show that $H = K$.

Let $\ell \in H$ then $b\ell = ah\ell$. By Multiplying both sides of $b\ell = ah\ell$ on the left by b^{-1} we get $\ell = b^{-1}ah\ell$. Since $h\ell \in H$, we have $ah\ell \in aH$. As a result, ℓ has the form $\ell = b^{-1}c$ for $c = ah\ell$. So, $\ell \in K$. Therefore, $H \subseteq K$.

Let $k \in K$. Then $k = b^{-1}c$ for some $c \in aH$, (or $c = ah_1$ for some $h_1 \in H$). So,

$$k = (ah)^{-1}c = (ah)^{-1}ah_1 = h^{-1}a^{-1}ah_1 = h^{-1}h_1.$$

Since $h, h_1 \in H$ and H is a subgroup, $hh_1 \in H$. So, $k \in H$. Hence, $K \subseteq H$.

Consequently, $H = K$. **(2 pts)** □

Q. 7. *Exercise 5.4.1. Show that the check digit at the end of an ISBN code can detect an error made by interchanging two adjacent digits.*

Proof. Let us assume that n is the correct integer calculated by $\sum_{i=2}^{10} i \cdot a_i$ and b is the check digit. Suppose that a_i and a_{i+1} are exchanged. Then,

$$\begin{aligned} n' &= 10 \cdot a_{10} + 9 \cdot a_9 + \cdots + (i+1) \cdot a_i + i \cdot a_{i+1} + \cdots + 2 \cdot a_2 \\ &= 10 \cdot a_{10} + 9 \cdot a_9 + \cdots + (i+1) \cdot a_{i+1} + i \cdot a_i + \cdots + 2 \cdot a_2 - a_{i+1} + a_i \\ &= n - a_{i+1} + a_i. \end{aligned}$$

The value of the check digit after the error is equal to

$$b' \equiv -n' \bmod 11 \equiv -n + a_{i+1} - a_i \equiv b + a_{i+1} - a_i.$$

Therefore, the code detects the error if and only if $b' \neq b$, that is, if and only if $a_{i+1} - a_i \neq 0$. Since exchanging a_{i+1} with a_i when $a_{i+1} = a_i$ is not error, we conclude that the code detects that type error.

(2 pts) □

Q. 8. *For each of the following generator matrices, find the minimum distance and determine the number of errors that it can detect and correct.*

$$M_1 = \begin{pmatrix} 1 & 0 & 0 & 1 & 1 & 0 & 1 & 0 \\ 0 & 1 & 0 & 0 & 1 & 1 & 0 & 1 \\ 0 & 0 & 1 & 0 & 0 & 1 & 1 & 1 \end{pmatrix},$$

$$M_2 = \begin{pmatrix} 1 & 0 & 0 & 0 & 1 & 0 & 0 & 1 \\ 0 & 1 & 0 & 0 & 0 & 1 & 0 & 1 \\ 0 & 0 & 1 & 0 & 1 & 1 & 1 & 1 \\ 0 & 0 & 0 & 1 & 0 & 1 & 1 & 0 \end{pmatrix},$$

$$M_3 = \begin{pmatrix} 1 & 0 & 0 & 0 & 1 & 1 & 1 \\ 0 & 1 & 0 & 0 & 1 & 1 & 0 \\ 0 & 0 & 1 & 0 & 1 & 0 & 1 \\ 0 & 0 & 0 & 1 & 1 & 1 & 0 \end{pmatrix}.$$

Proof. Consider M_1. Then 100 is mapped to $100 \cdot M_1 = 1001101 = w_1$, 010 to $010 \cdot M_1 = 01001101 = w_2$ and 001 to $001 \cdot M_1 = 00100111 = w_3$. The minimum weight among w_1, w_2, w_3 is 4. The rest of the codewords are of the form $\alpha w_1 + \beta w_2 + \gamma w_3$ for $\alpha, \beta, \gamma \in \{0, 1\}$. However, it is not possible to produce a codeword of weight 3 or less by that formula. Therefore the minimum distance between the codewords is 4. The code can detect 3 errors and correct 1 error.

By a similar discussion, we find that the minimum distance between the codewords produced by the code generated by M_2 is 3. So, it can detect 2 errors and correct 1.

Let us consider M_3. We have $1000 \cdot M_3 = 1000111$, $0100 \cdot M_3 = 0100110$, $0010 \cdot M_3 = 0010101$ and $0001 \cdot M_3 = 0001110$. The minimum weight among those codewords is 3. However, if we consider the rest of the codewords, we observe that the weight of

$$0100110 + 0001110 = 0101000$$

is 2. Therefore the minimum distance is 2 and the code can detect 1 error but correct none.
(3 pts) □

Q. 9. *Exercise 5.4.3. Let $f : \mathbb{B}^3 \to \mathbb{B}^9$ be a coding function given by*

$$f(abc) = abcab\bar{c}\bar{a}\bar{b}\bar{c}$$

for $abc \in \mathbb{B}^3$ where $\bar{x} = 1$ if $x = 0$ and $\bar{x} = 0$ if $x = 1$. List the eight codewords of f. Show that f does not give a group (linear) code.

Proof. The code maps

$$\begin{aligned} 000 &\mapsto 000000111 \\ 100 &\mapsto 100100011 \\ 010 &\mapsto 010010101 \\ 001 &\mapsto 001001110 \\ 110 &\mapsto 110110001 \\ 101 &\mapsto 101101010 \\ 011 &\mapsto 011011100 \\ 111 &\mapsto 111111000. \end{aligned}$$

However, f is not a linear code since the sum of the two codewords $010010101 + 110110001 = 100100100$ is not a codeword. **(2 pts)** □

Q. 10. *Write down the complete coset decoding table for the code generated by the matrix*

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

A message is encoded using the letter equivalents

$$00 = \text{ G},\ 10 = \text{ S},\ 01 = \text{ Z},\ 11 = \text{ Y},$$

and received as

$$101111,\ 111111,\ 011110,\ 111101,\ 010000,\ 101101.$$

Correct and decode the received message.

Proof. We see that by the code

$$\begin{aligned} 00 &\mapsto 000000 \\ 10 &\mapsto 101011 \\ 01 &\mapsto 010110 \\ 11 &\mapsto 111101. \end{aligned}$$

The coset decoding table can be formed as follows.

000000	101011	010110	111101
100000	101011	110110	011101
010000	111011	000110	101101
001000	100011	011110	110101
000100	101111	010010	111001
000010	101001	010100	111111
000001	101010	010111	111100
100001	001010	110111	011100
100010	001001	110100	011111
100100	001111	110010	011001
101000	000011	111110	010101
110000	011011	100110	001101
010001	111010	000111	101100
011000	110011	001110	100101
001100	100111	011010	110001
000101	101110	010011	111000

We observe that in the received message 111101 is a codeword. For the rest of the words, we locate them in the coset decoding table and note the column leader. So, the words

$$101111,\ 111111,\ 011110,\ 111101,\ 010000,\ 101101$$

are corrected into

$$101011,\ 111101,\ 010110,\ 111101,\ 000000,\ 111101.$$

The encoded message is formed by the first two digits of those: 10, 11, 01, 11, 00, 11 which translates into SYZYGY. **(3 pts)** □

MAT 312 SUMMER II, 2014 MIDTERM Solutions

Question 1.

a. Find all $n \in \mathbb{N}$, with $n \geq 2$, for which the following congruences hold.

$$\text{(i) } 13 \equiv 7 \bmod n, \quad \text{(ii) } -1 \equiv 6 \bmod n, \quad \text{(iii) } 0 \equiv -3 \bmod n.$$

b. Find all $n \in \mathbb{N}$ such that $\phi(n) = 12$.

c. Prove that if an odd prime number can be expressed as $p = x^2 + y^2$ with integers x and y then $p \equiv 1 \bmod 4$.

Solution.

a. (i). $13 \equiv 7 \bmod n \Rightarrow 13 = k \cdot n + 7$ for some $k \in \mathbb{Z}$. Equivalently, $6 = k \cdot n$, or $n|6$. The divisors of 6 are $1, 2, 3$ and 6. So, n can be $2, 3$ or 6.

(ii). $-1 \equiv 6 \bmod n \Rightarrow -1 = k \cdot n + 6$ for some $k \in \mathbb{Z}$. Equivalently, $-7 = k \cdot n$, or $n|7$. The divisors of 7 are 1 and 7. So, n is equal to 7.

(iii) $0 \equiv -3 \bmod n \Rightarrow 0 = k \cdot n - 3$ for some $k \in \mathbb{Z}$. Equivalently, $3 = k \cdot n$, or $n|3$. The divisors of 7 are 1 and 3. So, n is equal to 3.

b. Let us assume that $n = p_1^{\alpha_1} p_2^{\alpha_2} \cdots p_r^{\alpha_r}$ where $p_1,\ p_2, \ldots, p_r$ are distinct primes and $\alpha_i \in \mathbb{N}$ for all $i = 1, \ldots, r$. Then

$$\begin{aligned} \phi(n) &= \phi(p_1^{\alpha_1})\phi(p_2^{\alpha_2}) \cdots \phi(p_r^{\alpha_r}) \\ &= \left(p_1^{\alpha_1} - p_1^{\alpha_1 - 1}\right)\left(p_2^{\alpha_2} - p_1^{\alpha_2 - 1}\right) \cdots \left(p_r^{\alpha_r} - p_r^{\alpha_r - 1}\right) \\ &= p_1^{\alpha_1 - 1}(p_1 - 1) \cdot p_2^{\alpha_2 - 1}(p_2 - 1) \cdots p_r^{\alpha_r - 1}(p_r - 1). \end{aligned}$$

Note that $p_i^{\alpha_i - 1}(p_i - 1) \neq p_j^{\alpha_j - 1}(p_j - 1)$ since $p_i \neq p_j$ for $i \neq j$. So we just need to solve $p^{\alpha-1}(p-1) = a$ for p prime and α where a is a factor of 12. Since $12 = 1 \cdot 12$, $12 = 4 \cdot 3$ and $12 = 2 \cdot 6$ are the only possible factorisations, r is at most 2. We are considering any factorisations of 12 since the factors $(p_i - 1)$ are not prime for $p > 2$.

Consider $12 = 1 \cdot 12$. Clearly, $p^{\alpha-1}(p-1) = 1$ if and only if $p = 1$ and $\alpha = 1$, and $p^{\alpha-1}(p-1) = 12$ if and only if $p = 13$ and $\alpha = 1$. Notice that there is no prime satisfying $p^{\alpha-1} = 12$ for any $\alpha \in \mathbb{N}$. We have $n = 13$ or $n = 2 \cdot 13 = 26$.

Now consider $12 = 4 \cdot 3$. If $p^{\alpha-1}(p-1) = 3$ then $p - 1 = 3$, $p^{\alpha-1} = 1$ or $p - 1 = 1$, $p^{\alpha-1} = 3$. However, $p = 4$ is not a prime. In the latter case, $p = 2$ but there is no natural number α giving $2^{\alpha-1} = 3$. So $\phi(n)$ cannot be of the form $\phi(n) = 4 \cdot 3$.

Finally, consider $12 = 2 \cdot 6$. We need to solve $p^{\alpha-1}(p-1) = 2$ and $p^{\alpha-1}(p-1) = 6$. For $p^{\alpha-1}(p-1) = 2$ we have two solutions:

$$p = 2,\ \alpha = 2, \quad \text{or} \quad p = 3,\ \alpha = 1.$$

For $p^{\alpha-1}(p-1) = 6$ we also have two solutions:

$$p = 7,\ \alpha = 1, \quad \text{or} \quad p = 3,\ \alpha = 2$$

(consider $6 = 6 \cdot 1$ or $6 = 3 \cdot 2$.) Therefore, the possibilities for n are $n = 2^2 \cdot 7 = 28$, $n = 2^2 \cdot 3^2 = 36$ and $n = 3 \cdot 7 = 21$ (we choose $p_1,\ \alpha_1$ from the first group and $p_2,\ \alpha_2$ from the second group). Notice that $n = 3 \cdot 3^2 = 3^3$ is not an answer since $\phi(3^3) = 3^3 - 3^2 = 18$.

c. Since p is odd $p \equiv 1 \bmod 4$ or $p \equiv 3 \bmod 4$. For any $x \in \mathbb{Z}_4$, $x^2 \in \{[0]_4, [1]_4\}$. So, $x^2 + y^2 \equiv 1 \bmod 4$ for any $x \in [0]_4$ and $y \in [1]_4$. However, there is no possible choices for x and y that could give $x^2 + y^2 \equiv 3 \bmod 4$. Therefore, if $p = x^2 + y^2$ then it has to satisfy $p \equiv 1 \bmod 4$.

Question 2. Using the Chinese Remainder Theorem, or otherwise, deduce whether the following systems of linear congruences have a solution. If they do, calculate the solutions.

(i) $6x \equiv 5 \bmod 11$ and $3x \equiv 4 \bmod 5$.

(ii) $x \equiv 2 \bmod 21$, $4x \equiv 2 \bmod 18$ and $2x \equiv 3 \bmod 7$.

Solution.

(i) First bring the congruences into the form $x \equiv a \bmod n$. So, multiply them by the inverse of 6 mod 11 and the inverse of 3 mod 5, respectively. We have $[6]_{11}^{-1} = 2$, $[3]_5^{-1} = 2$. Then

$$\begin{aligned} 6x &\equiv 5 \bmod 11 \\ 2 \cdot 6x &\equiv 2 \cdot 5 \bmod 11 \\ x &\equiv 10 \bmod 11 \end{aligned}$$

and

$$\begin{aligned} 3x &\equiv 4 \bmod 5 \\ 2 \cdot 3x &\equiv 2 \cdot 4 \bmod 5 \\ x &\equiv 8 \bmod 5 \\ x &\equiv 3 \bmod 5. \end{aligned}$$

Notice that $(11, 5) = 1$. By the theorem, there exists a unique solution to the system mod $5 \cdot 11 = 55$. Let us calculate the solution. If x is a solution to the first congruence then $x = 11k + 10$ for some $k \in \mathbb{Z}$. If x is also a solution to the second one, then

$$x = 11k + 10 \equiv 1 \cdot k + 0 \equiv k \equiv 3 \bmod 5.$$

So, $k = 5m + 3$ for some $m \in \mathbb{Z}$. This gives $x = 11(5m + 3) + 10 = 55m + 43$. Therefore $[43]_{55}$ is the unique solution.

(ii) We apply the theorem to $x \equiv 2 \bmod 21$ and $2x \equiv 3 \bmod 7$. Again, we need to bring the latter into the form $x \equiv a \bmod 7$ for some $a \in \mathbb{Z}$. So multiply the both sides by $[2]_7^{-1} = [4]_7$ to get

$$\begin{aligned} 2x &\equiv 3 \bmod 7 \\ 4 \cdot 2x &\equiv 4 \cdot 3 \bmod 7 \\ x &\equiv 12 \bmod 7 \\ x &\equiv 5 \bmod 7. \end{aligned}$$

Now, by the Chinese Remainder Theorem, "$x \equiv 2 \bmod 21$, $x \equiv 5 \bmod 7$" have a common solution if and only if $(21, 7) = 1$. Since this is not the case, there is no common solution satisfying the two congruences. Therefore, there cannot be a common solution to "$x \equiv 2 \bmod 21$, $4x \equiv 2 \bmod 18$, $2x \equiv 3 \bmod 7$".

Question 3. Let $a \in \mathbb{Z}^+$. Show that for any integer $n \geq 1$,

$$\begin{pmatrix} a & 1 \\ 0 & a \end{pmatrix}^n = \begin{pmatrix} a^n & na^{n-1} \\ 0 & a^n \end{pmatrix}.$$

Solution.
For $n = 1$, we have

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

Assume that the equality holds for $n = k$. For $n = k + 1$ we have

$$\begin{aligned} \begin{pmatrix} a & 1 \\ 0 & a \end{pmatrix}^{k+1} &= \begin{pmatrix} a & 1 \\ 0 & a \end{pmatrix}^k \cdot \begin{pmatrix} a & 1 \\ 0 & a \end{pmatrix} \\ &= \begin{pmatrix} a^k & na^{k-1} \\ 0 & a^k \end{pmatrix} \cdot \begin{pmatrix} a & 1 \\ 0 & a \end{pmatrix} \qquad \text{(by the assumption)} \\ &= \begin{pmatrix} a^{k+1} & (k+1)a^k \\ 0 & a^{k+1} \end{pmatrix}. \end{aligned}$$

Therefore the equality is true for all $n \geq 1$ by the induction principle. $\square$

Question 4. A public key code has base 69 and exponent 15. It uses the following letter-to-number equivalents.

$$\text{B} = 1,\ \text{G} = 2,\ \text{L} = 3,\ \text{A} = 4,\ \text{E} = 5,\ \text{S} = 6,\ \text{“ ”} = 7,\ \text{T} = 8,\ \text{R} = 0.$$

(Note that 7 corresponds to the "space" character.) A message has been converted to numbers and broken into 2-digits blocks. The coded message is 34/16/28/47. Decode the message.

Solution.

We have $n = 69 = 3 \cdot 23$. So, $\phi(69) = (3-1)(23-1) = 44$. Notice that $(44, 15) = 1$. We calculate the other integer x by the formula

$$1 = x \cdot 15 + s \cdot 44$$

where $s \in \mathbb{Z}$. We find $x = 3$ since

$$1 = 3 \cdot 15 - 44.$$

Let us decode 34/16/28/47. We find $\beta_1/\beta_2/\beta_3/\beta_4$ by

$$\begin{aligned}
\beta_1 &= 34^3 \bmod 69 \equiv 52 \cdot 34 \equiv 43 \bmod 69,\\
\beta_2 &= 16^3 \bmod 69 \equiv 49 \cdot 16 \equiv 25 \bmod 69,\\
\beta_3 &= 28^3 \bmod 69 \equiv 25 \cdot 28 \equiv 10 \bmod 69,\\
\beta_4 &= 47^3 \bmod 69 \equiv 1 \cdot 47 \equiv 47 \bmod 69.
\end{aligned}$$

Hence, the coded message is 43/25/10/47 which translates into "ALGEBRA ". □

Question 5. Let A, B and C be nonempty sets. Prove the following two equalities.

(i) $(A \setminus B) \cup (B \setminus A) = (A \cup B) \setminus (B \cap A)$,

(ii) $A \setminus (B \setminus C) = (A \setminus B) \cup (A \cap C)$,

Solution.

(i) We use the equality $A \setminus B = A \cap B^c$ and the properties of the set operations $\cap$, $\cup$ and " ^{c} " to get

$$\begin{aligned}
(A \setminus B) \cup (B \setminus A) &= (A \cap B^c) \cup (B \cap A^c) \\
&= [(A \cap B^c) \cup B] \cap [(A \cap B^c) \cup A^c] \\
&= [(A \cup B) \cap (B^c \cup B)] \cap [(A \cup A^c) \cap (A^c \cup B^c)] \\
&= (A \cup B) \cap (A^c \cup B^c) \\
&= (A \cup B) \cap (A \cap B)^c \\
&= (A \cup B) \setminus (B \cap A).
\end{aligned}$$

Alternatively, we can use the definitions.

$$\begin{aligned}
x \in (A \setminus B) \cup (B \setminus A) &\Rightarrow x \in A \setminus B \text{ or } x \in B \setminus A \\
&\Rightarrow \text{“}x \in A \text{ and } x \notin B\text{”} \text{ or “}x \in B \text{ and } x \notin A\text{”} \\
&\Rightarrow \text{“}x \in A \text{ or } x \in B\text{”} \text{ and “}x \notin A \text{ or } x \notin B\text{”} \text{ and} \\
&\quad \text{“}x \in A \text{ or } x \notin A\text{”} \text{ and “}x \in B \text{ or } x \notin B\text{”} \\
&\Rightarrow \text{“}x \in A \text{ or } x \in B\text{”} \text{ and “}x \notin A \text{ or } x \notin B\text{”} \\
&\Rightarrow \text{“}x \in A \cup B\text{”} \text{ and “}x \notin A \cap B\text{”} \\
&\Rightarrow x \in (A \cup B) \setminus (A \cap B).
\end{aligned}$$

Note that both "$x \in A$ or $x \notin A$" and "$x \in B$ or $x \notin B$" implies $x \in U$ and that does not effect the claim. Hence, $(A \setminus B) \cup (B \setminus A) \subseteq (A \cup B) \setminus (B \cap A)$.

Now assume that $x \in (A \cup B) \setminus (B \cap A)$. Then

$$\begin{aligned}
x \in (A \cup B) \setminus (B \cap A) &\Rightarrow x \in A \cup B \text{ and } x \notin A \cap B \\
&\Rightarrow \text{“}x \in A \text{ or } x \in B\text{”} \text{ and “}x \notin A \text{ or } x \notin B\text{”} \\
&\Rightarrow \text{“}x \in A \text{ and } x \notin A\text{”} \text{ or “}x \in A \text{ and } x \notin B\text{”} \text{ or} \\
&\quad \text{“}x \in B \text{ and } x \notin B\text{”} \text{ or “}x \in B \text{ and } x \notin A\text{”} \\
&\Rightarrow \text{“}x \in A \text{ and } x \notin B\text{”} \text{ or } \text{ or “}x \in B \text{ and } x \notin A\text{”} \\
&\Rightarrow x \in A \setminus B \text{ or } x \in B \setminus A.
\end{aligned}$$

Note that both "$x \in A$ and $x \notin A$" and "$x \in B$ and $x \notin B$" imply $x \in \emptyset$ and that does not effect the claim. Hence $(A \cup B) \setminus (B \cap A) \subseteq A \setminus B$ or $x \in B \setminus A$. Thus, $(A \setminus B) \cup (B \setminus A) = (A \cup B) \setminus (B \cap A)$.

(ii) Similarly,

$$\begin{aligned} A \setminus (B \setminus C) &= A \cap (B \setminus C)^c \\ &= A \cap (B \cap C^c)^c \\ &= A \cap (B^c \cup (C^c)^c) \\ &= A \cap (B^c \cup C) \\ &= (A \cap B^c) \cup (A \cap C) \\ &= (A \setminus B) \cup (A \cap C). \end{aligned}$$