PREFACE

This is a study guide offered by SOS for the Fall 2014 Math 135 Final Examination. This guide aims to cover the majority of testable concepts that may or may not be present of the final examination, as well as provide tips & strategies on understanding course material and avoiding common mistakes. This guide excludes many of the concepts covered on the midterm examination, as the Fall 2014 Math 135 Midterm Study Guide is readily available.

This guide will cover 6 primary topics:

THE GREATEST COMMON DIVISOR, GCD

Recall that gcd(a,b) is the greatest common divisor of a and b. In particular, the gcd has three properties that follow from its definition.

1) The gcd(a,b) is a **positive integer.**

2) The gcd(a,b) is a **common divisor**, hence gcd(a,b) | a and gcd(a,b) | b.

3) The gcd(a,b) = ax+by for some integers x,y. (By the Extended Euclidean Algorithm, EEA)

Proofs involving GCD are simply an extension of divisibility proofs covered earlier in the course. By utilizing the above 3 properties, GCD theorems, and divisibility theorems, we can tackle any GCD proof.

Question 1

Suggestions for Approaching this proof:

A good way to start any proof involving GCDs is to let a variable such as d represent the gcd. While this isn't done in the solution below, making this substitution makes it easier to think about the gcd as an integer. If you are unable to see a solution immediately, using EEA to express the gcd as d = ax+by should be your next step. Doing this will allow you to manipulate the gcd algebraically.

Let n be a positive integer, and $a, b \in \mathbb{Z}$. Prove that $n \mid (\gcd(a,n) \cdot \gcd(b,n))$ if and only if $n \mid (ab)$. **[6 marks]**

Soln. By the *Extended Euclidean Algorithm (EEA)*, there exist integers x, y, u, v such that

$$\gcd(a,n) = ax + ny$$
$$\text{and } \gcd(b,n) = bu + nv.$$

Assume $n \mid (ab)$. Then

$$\begin{aligned}(\gcd(a,n) \cdot \gcd(b,n)) &= (ax+ny)\cdot(bu+nv)\\ &= (ab)(\quad xv + ybu + ybv).\end{aligned}$$

By *Divisibility of Integer Combinations (DIC)*, we get that $n \mid (\gcd(a,n) \cdot \gcd(b,n))$.

On the other hand, assume $n \mid (\gcd(a,n) \cdot \gcd(b,n))$. Since $\gcd(a,n) \mid a$ and $\gcd(b,n) \mid b$, therefore $(\gcd(a,n) \cdot \gcd(b,n)) \mid (ab)$. Then by *Transitivity of Divisibility (TD)*, we get that $n \mid (ab)$.

REMARKS ON QUESTION 1:

1. Notice how this is an "if and only if" statement. We must prove it in both directions.
2. We utilized two of the above 3 properties of gcd in this proof. In particular, EEA and that the gcd is a common divisor.

Question 2

Suggestions for Approaching this proof:

Once again, begin by letting d and e represent the two GCDs. Is there a divisibility theorem you can apply here?

Let $a, b, x, y \in \mathbb{N}$. Prove that if $\gcd(a, b) \mid \gcd(x, y)$ and $\gcd(x, y) \mid \gcd(a, b)$ then

$$\gcd(a, b) = \gcd(x, y).$$

[4 marks]

Soln. Assume $\gcd(a, b) \mid \gcd(x, y)$ and $\gcd(x, y) \mid \gcd(a, b)$.

Since $\gcd(a, b) \mid \gcd(x, y)$, using *Bounds by Divisibility (BBD)*, we get

$$|\gcd(a, b)| \leq |\gcd(x, y)|.$$

Similarly, $\gcd(x, y) \mid \gcd(a, b)$ gives us

$$|\gcd(x, y)| \leq |\gcd(a, b)|.$$

As $a, b, x, y \in \mathbb{N}$, then by definition, $\gcd(a, b) \in \mathbb{N}$ and $\gcd(x, y) \in \mathbb{N}$. So $|\gcd(a, b)| = \gcd(a, b)$ and $|\gcd(x, y)| = \gcd(x, y)$.

Consequently, $\gcd(a, b) \leq \gcd(x, y)$ and $\gcd(x, y) \leq \gcd(a, b)$, so

$$\gcd(a, b) = \gcd(x, y).$$

REMARKS ON QUESTION 2:

1. This is a relatively simple proof that involves the use of BBD. Representing the gcd as "d" and "e" should allow you to make the connection between this statement and BBD.

Linear Diophantine Equations and LCT

Recall that a LDE is of the form ax+by = c.

1) By LDET1, ax+by = c has a solution only if gcd(a,b) | c.

2) By LDET2, if LDET1 holds true, then the equation has **infinite** solutions.

3) These solutions are given by the set {x + (b/d)*n, y - (a/d)*n} for all n.
Note that d is gcd (a,b).

The LCT is simply an extension of the LDE theorems. In particular, LCT applies when solving a linear congruence. The only difference is that LCT has **finite** solutions, equal to the value of the gcd. Both these theorems will be explicitly written in your supplementary theorems sheet on the exam, but it is still good to know the difference between the two.

Question 1

Determine, with justification, the complete solution to the linear Diophantine Equation

$$2016x + 266y = 70.$$

[6 marks]

Soln. Using the *Extended Euclidean Algorithm (EEA)* table.

x	y	r	q	Division Algorithm
1	0	2016	0	$2016 = 0(266) + 2016$
0	1	266	0	$266 = 0(2016) + 266$
1	-7	154	7	$2016 = 7(266) + 154$
-1	8	1	112	$266 = 1(154) + 112$
2	-15	42	1	$154 = 1(112) + 42$
-5	38	28	2	$112 = 2(42) + 28$
7	-53	14	1	$42 = 1(28) + 14$
-19	144	0	2	$28 = 2(14)$

Table 1: Extended Euclidean Algorithm

Therefore, we get

$$2016(7) + 266(-53) = 14,$$

and hence

$$2016(35) + 266(-265) = 70.$$

Therefore, $x_0 = 35$ and $y_0 = -265$ is one particular solution. The complete solution is given by

Therefore, $x_0 = 35$ and $y_0 = -265$ is one particular solution. The complete solution is given by

$$x = 35 + \frac{266}{14}n = 35 + 19n$$
$$y = -265 - \frac{2016}{14}n = -265 - 144n.$$

for all $n \in \mathbb{Z}$.

REMARKS ON QUESTION 1:

1. You must be comfortable working through an EEA table in order to solve this question! The rest simply follows from the LDET theorems.

Question 2

Determine the complete solution to the equation $[203][x] = [35]$ in $\mathbb{Z}_{420}$ as congruence classes in $\mathbb{Z}_{420}$. Make sure to justify each of your steps. **[6 marks]**

Soln. The given equation $[203][x] = [35]$ in $\mathbb{Z}_{420}$ is equivalent to the linear congruence

$$203x \equiv 35 \pmod{420}$$

and is therefore the same as the linear diophantine equation $203x + 420y = 35$.

Using *Extended Euclidean Algorithm (EEA)* table,

x	y	r	q	Division Algorithm
1	0	203		
0	1	420		
1	0	203	0	$203 = 0(420) + 203$
-2	1	14	2	$420 = 2(203) + 14$
29	-14	7	14	$203 = 14(14) + 7$
		0		$14 = 2(7) + 0$

From the table we get $\gcd(204, 420) = 7$. Moreover, $203(29) + 420(-14) = 7$, so

$$203(29 \times 5) + 420(-14 \times 5) = 35.$$

Hence $[x_0] = [29 \times 5] = [145]$ is one solution to the given equation in $\mathbb{Z}_{420}$. According to the *Linear Congruence Theorem, version 2 (LCT 2)*, there are 7 solutions in $\mathbb{Z}_{420}$, given by

$$
\begin{aligned}
[x] &= [x_0] = [145] \\
\text{or } [x] &= \left[x_0 + (1)\frac{420}{7}\right] = [205] \\
\text{or } [x] &= \left[x_0 + (2)\frac{420}{7}\right] = [265] \\
\text{or } [x] &= \left[x_0 + (3)\frac{420}{7}\right] = [325] \\
\text{or } [x] &= \left[x_0 + (4)\frac{420}{7}\right] = [385] \\
\text{or } [x] &= \left[x_0 + (5)\frac{420}{7}\right] = [445] = [25] \\
\text{or } [x] &= \left[x_0 + (6)\frac{420}{7}\right] = [505] = [85].
\end{aligned}
$$

REMARKS ON QUESTION 2:

1. Once again we use an EEA table and apply the LCT theorems in order to solve the problem. This question tests your knowledge of linear diophantine equations and LCT.

Simultaneous Congruences

Determine, with justification, the value of the remainder when 2^{314} is divided by 91.

(Hint: $91 = 13 \times 7$.) **[6 marks]**

Soln. According to *Congruence Iff Same Remainder (CISR)*, we want to find an integer $0 \leq x < 91$ such that $x \equiv 2^{314} \pmod{91}$.

Since $91 = 13 \times 7$, and $\gcd(13, 7) = 1$, therefore this is equivalent to solving the simultaneous congruences

$$\begin{aligned} x &\equiv 2^{314} \pmod{13} \\ \text{and } x &\equiv 2^{314} \pmod{7}. \end{aligned}$$

Let us simplify each of the above congruence relations. Since 13 is a prime and $13 \nmid 2$, therefore by *Fermat's little Theorem (FlT)*, we have $2^{12} \equiv 1 \pmod{13}$. Consequently,

$$2^{314} \equiv 2^{12(26)+2} \equiv \left(2^{12}\right)^{26} \left(2^2\right) \equiv (1)^{26} \left(2^2\right) \equiv 4 \pmod{13}.$$

Similarly, as 7 is a prime and $7 \nmid 2$, then by *(FlT)*, we have $2^6 \equiv 1 \pmod{7}$. Thus,

$$2^{314} \equiv 2^{6(52)+2} \equiv \left(2^6\right)^{52} \left(2^2\right) \equiv 4 \pmod{7}.$$

As a result, the simultaneous congruences become

$$\begin{aligned} x &\equiv 4 \pmod{13} \\ \text{and } x &\equiv 4 \pmod{7}. \end{aligned}$$

Therefore $x_0 = 4$ satisfies both congruences, and thus by the *Chinese Remainder Theorem (CRT)*, the solutions to the simultaneous congruences satisfy

$$x \equiv 4 \pmod{91}.$$

Hence the remainder of 2^{314} divided by 91 is 4.

Question 1

Remarks on Question 1

1. Whenever you see a large power such as 2^314, it is a clear indication that FIT must be used. Also the hint that 91 = 13 x 7, which are two prime numbers is good indication that we should be splitting this congruence up and using CRT to solve it.

Question 2

Suppose you are given that the private key of an RSA scheme is $(d, n) = (7, 35)$. Decrypt the cipher-text $C = 19$. **[6 marks]**

Soln. We simply need to find an integer $0 \leq R \leq 34$ such that $R \equiv 19^7 \pmod{35}$.

Since $35 = 5 \times 7$, we may solve the simultaneous congruences

$$\begin{aligned} R &\equiv 19^7 \pmod{5} \\ \text{and } R &\equiv 19^7 \pmod{7}. \end{aligned}$$

Since 5 is a prime and $5 \nmid 19$, therefore using *Fermat's little Theorem (FlT)*, we have $19^4 \equiv 1 \pmod{5}$. Then

$$R \equiv 19^7 \equiv 4^7 \equiv \left(4^4\right)\left(4^3\right) \equiv 4 \pmod{5}.$$

Similarly, as 7 is a prime, then by the corollary to *(FlT)*, we have

$$R \equiv 19^7 \equiv 19 \equiv 5 \pmod{7}.$$

From $R \equiv 5 \pmod{7}$, we get $R = 5 + 7k$ for some integer k. Then $R \equiv 4 \pmod{5}$ gives us

$$\begin{aligned} & (5 + 7k) \equiv 4 \pmod{5} \\ \implies & 7k \equiv (-1) \pmod{5} \\ \implies & 2k \equiv 4 \pmod{5}. \end{aligned}$$

As $5 \nmid 2$, therefore $\gcd(5, 2) = 1$, and thus using *Congruence and Division (CD)* to divide both sides by 2, we get

$$k \equiv 2 \pmod{5}.$$

Consequently, we have $k = 2 + 5l$ for some integer l, and hence $R = 5 + 7(2 + 5l)$, that is, $R = 19 + 35l$. Thus, the decrypted message is $R = 19$.

Remarks on Question 2

1. Remember that RSA is simply an application of the Chinese remainder theorem. You will have the full RSA details available on your proposition sheet, so there is no need to memorize it.

Primes and Prime Factorization

Question 1

Statement 1. Let $a, b \in \mathbb{N}$ and p be a prime. If p divides both ab and $a + b$, then p is a common divisor of a and b.

Prove statement 1. **[4 marks]**

Soln. Assume $p \mid (ab)$ and $p \mid (a + b)$.

Since p is a prime, then by *Primes and Divisibility (PAD)*, $p \mid (ab)$ means $p \mid a$ or $p \mid b$.

Suppose, for the sake of contradiction, $p \nmid a$. Then $p \mid b$ and $p \mid (a + b)$. Using *Divisibility of Integer Combinations (DIC)*, we get that

$$p \mid ((a + b) - b),$$

so $p \mid a$ (contradiction).

The assumption $p \nmid b$ also gives us a similar contradiction. Therefore we must conclude that $p \mid a$ and $p \mid b$.

An integer n is said to be a *perfect square* if there exist some integer m such that $n = m^2$.

Let $a, b \in \mathbb{N}$. Prove that if $\gcd(a, b) = 1$ and (ab) is the perfect square, then both a and b are perfect squares. **[6 marks]**

Soln. Assume that (ab) is a perfect square. If $(ab) = 1$, the we have $a = 1$ and $b = 1$, so the proposition is satisfied.

Suppose $(ab) > 1$. If either a or b is equal to 1, then the other must be equal to (ab), and hence must be a perfect square.

Therefore, we need to verify the proposition when both $a \geq 2$ and $b \geq 2$. Assume that $\gcd(a, b) = 1$. Therefore, we may say that a and b cannot have any prime factors in common.

Since $a, b \geq 2$, we use the following prime factorizations of a and b. Let

$$a = p_1^{\alpha_1} p_2^{\alpha_2} \cdots p_k^{\alpha_k}$$
$$b = q_1^{\beta_1} q_2^{\beta_2} \cdots q_l^{\beta_l}$$

where $p_1, p_2, \ldots, p_k$ and $q_1, q_2, \ldots, q_l$ are distinct primes, such that $\alpha_i, \beta_j \in \mathbb{N}$ for each $1 \leq i \leq k$ and each $1 \leq j \leq l$.

Therefore,

$$(ab) = (p_1^{\alpha_1} p_2^{\alpha_2} \cdots p_k^{\alpha_k}) \left(q_1^{\beta_1} q_2^{\beta_2} \cdots q_l^{\beta_l} \right).$$

Since (ab) is a perfect square (and is greater than 1), therefore there exists some integer $m \geq 2$ such that $(ab) = m^2$. Suppose a prime factorization of m is given by

$$m = (u_1)^{\gamma_1} (u_2)^{\gamma^2} \cdots (u_s)^{\gamma_s},$$

Question 2

where $u_1, u_2, \ldots, u_s$ are distinct primes and $\gamma_i \in \mathbb{N}$ for each $1 \leq i \leq s$.

This means

$$\begin{aligned} m^2 &= \left((u_1)^{\gamma_1} (u_2)^{\gamma^2} \cdots (u_s)^{\gamma_s} \right)^2 \\ &= (u_1)^{2\gamma_1} (u_2)^{2\gamma^2} \cdots (u_s)^{2\gamma_s}. \end{aligned}$$

Now, since $ab = m^2$, then according to the *Unique Factorization Theorem (UFT)*, by comparing the prime factorization on both sides of the equation $ab = m^2$, we may conclude that $s = (k + l)$, and

$$p_1 = u_1,\ p_2 = u_2,\ \ldots,\ p_k = u_k,\ q_1 = u_{k+1},\ q_2 = u_{k+2},\ \ldots,\ q_l = u_{k+l}.$$

Moreover, each $\alpha_i = 2\gamma_i$ for $1 \leq i \leq k$ and each $\beta_j = 2\gamma_{k+j}$ for $1 \leq j \leq l$.

So overall, we get

$$a = \left(p_1^{2\gamma_1} p_2^{2\gamma_2} \cdots p_k^{2\gamma_k} \right) = (p_1^{\gamma_1} p_2^{\gamma_2} \cdots p_k^{\gamma_k})^2$$

and

$$b = \left(q_1^{2\gamma_{k+1}} q_2^{2\gamma_{k+2}} \cdots q_l^{2\gamma_{k+l}} \right) = \left(q_1^{\gamma_{k+1}} q_2^{\gamma_{k+2}} \cdots q_l^{\gamma_{k+l}} \right)^2.$$

Therefore a and b are perfect squares.

Complex Numbers

Question 1

Prove that **[3 marks]**

$$|1 - z\overline{w}|^2 - |z - w|^2 = \left(1 - |z|^2\right)\left(1 - |w|^2\right).$$

Soln. Using *properties of modulus (PM)*,

$$|1 - z\overline{w}|^2 - |z - w|^2 = (1 - z\overline{w}) \cdot \overline{(1 - z\overline{w})} - (z - w) \cdot \overline{(z - w)}.$$

Then, using *properties of conjugates (PCJ)*,

$$\begin{aligned}
&(1 - z\overline{w}) \cdot \overline{(1 - z\overline{w})} - (z - w) \cdot \overline{(z - w)} \\
=&(1 - z\overline{w}) \cdot \left(1 - \overline{z} \cdot \overline{\overline{w}}\right) - (z - w) \cdot (\overline{z} - \overline{w}) \\
=&(1 - z\overline{w}) \cdot (1 - \overline{z} \cdot w) - (z - w) \cdot (\overline{z} - \overline{w}) \\
=&(1 - \overline{z} \cdot w - z \cdot \overline{w} + (z \cdot \overline{w}) \cdot (\overline{z} \cdot w)) - (z \cdot \overline{z} - z \cdot \overline{w} - w \cdot \overline{z} + w \cdot \overline{w}) \\
=&1 + |z|^2 |w|^2 - |z|^2 - |w|^2 \\
=&\left(1 - |w|^2\right) - |z|^2 \left(1 - |w|^2\right) \\
=&\left(1 - |z|^2\right)\left(1 - |w|^2\right).
\end{aligned}$$

Thus

$$|1 - z\overline{w}|^2 - |z - w|^2 = \left(1 - |z|^2\right)\left(1 - |w|^2\right).$$

Solve $z = \frac{1+8i}{2-z}$. Demonstrate and justify your steps. **[8 marks]**

Soln. We get

$$\begin{aligned} z(2-z) &= 1+8i \\ \implies z^2 - 2z + (1+8i) &= 0 \end{aligned}$$

Using the quadratic formula,

$$z = \frac{2 \pm \sqrt{4-4(1+8i)}}{2} = 1 \pm \sqrt{-8i} = 1 \pm 2\sqrt{-2i}.$$

Use the *Complex N^{th} Roots Theorem (CNRT)* to find the square roots of $(-2i)$. In its polar form,

$$-2i = 2\cos\left(\frac{3\pi}{2}\right) + i\sin\left(\frac{3\pi}{2}\right).$$

Thus, the square roots are given by

$$\begin{aligned} z_0 &= \sqrt{2}\cos\left(\frac{3\pi}{4}\right) + i\sin\left(\frac{3\pi}{4}\right) = \sqrt{2}\left(\frac{-1+i}{\sqrt{2}}\right) = -1+i \\ \text{and } z_1 &= \sqrt{2}\cos\left(\frac{7\pi}{4}\right) + i\sin\left(\frac{7\pi}{4}\right) = \sqrt{2}\left(\frac{1-i}{\sqrt{2}}\right) = 1-i. \end{aligned}$$

Therefore, our solutions are given by

$$z = 1 \pm 2(1-i),$$

so $z = 3-2i$ or $z = -1+2i$.

Question 2

Polynomials

Question 1

Let $f(x) = x^5 + 4x^3 + 8x^2 + 32$ be a polynomial. Given that $f(2i) = 0$, express $f(x)$ as a product of linear complex polynomials. Make sure to justify each of your steps.

[8 marks]

Soln. The given polynomial $f(x)$ has only real coefficients. Therefore, given $x = 2i$ is a root of $f(x)$, by the *Conjuagate Roots Theorem (CJRT)*, $x = -2i$ must also be a root of $f(x)$.

By the *Factor Theorem (FT)*, therefore we have two linear factors: $(x - 2i)$ and $(x + 2i)$. Multiplying these two factors gives us

$$(x - 2i)(x + 2i) = \left(x^2 - 2Re(2i)x + |2i|^2\right) = (x^2 + 4)$$

as a quadratic factor of $f(x)$.

Then by long division, we get

$$f(x) = \left(x^2 + 4\right) \cdot \left(x^3 + 8\right).$$

The roots of $(x^3 + 8)$ can be obtained using the *Complex N^{th} Roots Theorem (CNRT)*. First, in polar form,

$$-8 = 8\left[\cos(\pi) + i\sin(\pi)\right].$$

Then, the cubic roots of (-8) are given by

$$z_0 = \sqrt[3]{8}\left[\cos\left(\frac{\pi}{3}\right) + i\sin\left(\frac{\pi}{3}\right)\right] = 2\left(\frac{1}{2} + i\frac{\sqrt{3}}{2}\right) = 1 + i\sqrt{3},$$

$$z_1 = \sqrt[3]{8}\left[\cos\left(\frac{3\pi}{3}\right) + i\sin\left(\frac{3\pi}{3}\right)\right] = 2\left((-1) + i(0)\right) = -2,$$

$$z_2 = \sqrt[3]{8}\left[\cos\left(\frac{5\pi}{3}\right) + i\sin\left(\frac{5\pi}{3}\right)\right] = 2\left(\frac{1}{2} - i\frac{\sqrt{3}}{2}\right) = 1 - i\sqrt{3}.$$

Now we have all the roots of $f(x)$. So we may express

$$f(x) = (x+2)(x-2i)(x+2i)(x-(1+i\sqrt{3}))(x-(1-i\sqrt{3})).$$

Find all the complex roots of the polynomial $x^5 + 5x^4 + 13x^3 + 19x^2 + 10x$. **[7 marks]**

Soln. Let $f(x) = x^5 + 5x^4 + 13x^3 + 19x^2 + 10x$. Clearly, $x = 0$ is a root. Hence, we look for the roots of

$$g(x) = x^4 + 5x^3 + 13x^2 + 19x + 10.$$

By the *Rational Roots Theorem (RRT)*, the candidates for rational roots of $g(x)$ are

$$\pm 1,\ \pm 2,\ \pm 5.$$

Note that all the terms in $g(x)$ are being added, so $g(x)$ cannot have a positive root. So, we only need to check the negative candidates. We find:

x	-1	-2	-5
$g(x)$	0	0	240.

So, we get two rational roots, $x = -1$ and $x = -2$.

Now, we have the three factors of $f(x)$, namely x, $(x+1)$ and $(x+2)$, corresponding to the roots $x = 0$, $x = -1$ and $x = -2$ respectively. Multiplying these factors together gives us a cubic factor:

$$x(x+1)(x+2) = x^3 + 3x^2 + 2x.$$

Then, use long division to divide $f(x)$ by $x^3 + 3x^2 + 2x$.

$$\begin{array}{rl|rrrrrrrrrr}
 & & & & & & & x^2 & + & 2x & + & 5 \\
x^3 + 3x^2 + 2x & | & x^5 & + & 5x^4 & + & 13x^3 & + & 19x^2 & + & 10x & + & 0 \\
 & & x^5 & + & 3x^4 & + & 2x^3 & & & & & & \\
\hline
 & & & & 2x^4 & + & 11x^3 & + & 19x^2 & + & 10x & + & 0 \\
 & & & & 2x^4 & + & 6x^3 & + & 4x^2 & & & & \\
\hline
 & & & & & & 5x^3 & + & 15x^2 & & 10x & + & 0 \\
 & & & & & & 5x^3 & + & 15x^2 & & 10x & & \\
\hline
 & & & & & & & + & & & & & 0
\end{array}$$

Thus, we get a quadratic factor of $f(x)$, given by

$$x^2 + 2x + 5.$$

Use the quadratic formula to solve for the roots:

$$x = \frac{-2 \pm \sqrt{(2)^2 - 4(1)(5)}}{2} = \frac{-2 \pm \sqrt{-16}}{2} = -1 \pm 2i.$$

Finally, we now have all the complex roots of $f(x)$, given by

$$x = 0;\ x = -1;\ x = -2;\ x = 1 + 2i;\ x = 1 - 2i.$$

Additional Questions

Question 1 - Induction

Prove using induction that $6 \mid (2n^3 + 3n^2 + n)$ for all $n \in \mathbb{N}$. **[6 marks]**

Soln. Let $P(n)$: $\quad 6 \mid (2n^3 + 3n^2 + n)$.

Base Case: When $n = 1$, we have

$$2n^3 + 3n^2 + n = 2(1)^3 + 3(1)^2 + (1) = 6.$$

Therefore $P(1)$ is true.

Induction Hypothesis: Let $k \in \mathbb{N}$. Assume that $P(k)$ is true.

Induction Conclusion: When $n = k + 1$, we have

$$\begin{aligned} & 2(k+1)^3 + 3(k+1)^2 + (k+1) \\ =& 2\left(k^3 + 3k^2 + 3k + 1\right) + 3\left(k^2 + 2k + 1\right) + (k+1) \\ =& \left(2k^3 + 3k^2 + k\right) + (6)\left(k^2 + 2k + 1\right) \\ =& \left(2k^3 + 3k^2 + k\right) + 6(k+1)^2. \end{aligned}$$

As $(k+1)^2 \in \mathbb{Z}$, therefore $6 \mid [6(k+1)^2]$. Also, by the induction hypothesis, $6 \mid (2k^3 + 3k^2 + k)$. Therefore, by the *Divisibility of Integer Combinations (DIC)*, we get that

$$6 \mid \left[2(k+1)^3 + 3(k+1)^2 + (k+1)\right].$$

Thus $P(k+1)$ is true. Therefore, by the *Principle of Mathematical Induction (POMI)*, we get that $\forall\ n \in \mathbb{N},\ P(n)$ is true.

Question 2 - GCD-WR

Problem 2. Find $\gcd(8a+3, 5a+2)$, where a is an integer.

Solution: We showed in class that $\gcd(x, y) = \gcd(y, x - ny)$ for any integer n. Using this formula repeatedly, with $n = 1$ (the first three times) and then with $n = 2$, we obtain $\gcd(8a+3, 5a+2) =$

$$\gcd(5a+2, 3a+1) = \gcd(3a+1, 2a+1) = \gcd(2a+1, a) = \gcd(a, 1) = 1\,.$$

Note that the above calculation is valid for any integer value of a.