MATH 135 Final Examination
Algebra for Honours Mathematics Fall 2018

1. Determine the value of $\gcd(135^{2018}, 10!)$. (You may state your answer in factored form.) **[2 marks]**

   Solution: Answer: $3^4 5^2 = 2025$.

   Since $135^{2018} = (3^3 5)^{2018} = 3^{6054} 5^{2018}$ and $10! = 2^8 3^4 5^2 7$ then by GCD PF

   $$\gcd(135^{2018}, 10!) = 3^4 5^2 = 2025.$$

2. Determine the remainder when 31^{66} is divided by 17. **[2 marks]**

   Solution: Answer: 9

   $$\begin{aligned} 31^{66} &\equiv 14^{66} \pmod{17} \\ &\equiv (14^{16})^4 14^2 \pmod{17} \\ &\equiv (1)^4 14^2 \pmod{17} \qquad \text{(by F}\ell\text{ T)} \\ &\equiv 14^2 \pmod{17} \\ &\equiv (-3)^2 \pmod{17} \\ &\equiv 9 \pmod{17}. \end{aligned}$$

   Hence the remainder when divided by 17 is 9.

3. Alice's RSA public key is $(7, 407)$. Note that $407 = 11 \times 37$. What is Alice's private key, (d, n)? **[3 marks]**

   Solution: Answer: $(103, 407)$.

   To find Alice's private key we must solve

   $$7d \equiv 1 \pmod{360}$$

   which is equivalent to solving the LDE $7d + 360y = 1$. Using EEA we get:

y	d	r	q
1	0	360	0
0	1	7	0
1	-51	3	51
-2	103	1	2
7	-360	0	3

   We get $d = 103$. So Alice's private key is $(103, 407)$.

4. Determine the complete solution to the following system of equations in $\mathbb{Z}_6$. **[3 marks]**

$$[4][x] + [3][y] = [2]$$
$$[2][x] + [4][y] = [2]$$

Solution: Answer: $([x], [y]) \in \{([2], [4]), ([5], [4])\}$

We multiply the second equation by [2] and subtract it from the first equation to obtain $[y] = [4]$. Substituting into the first equation we obtain the equation $[4][x] = [2]$. This is equivalent to solving the linear Diophantine equation $4x + 6k = 2$ which is equivalent to solving $2x + 3k = 1$. By inspection, a solution is $x = 2$ and $k = -1$. The general solution for x is $x = 2 + 3n$ for $n \in \mathbb{Z}$. Therefore $x \equiv 2 \pmod 3$. This is equivalent to $x \equiv 2, 5 \pmod 6$. Thus $[x] = [2], [5]$. Therefore, $([x], [y]) \in \{([2], [4]), ([5], [4])\}$

5. Write $f(x) = x^4 - 3x^3 + 4x^2 - 2x$ as a product of irreducible polynomials in $\mathbb{C}[x]$. **[3 marks]**

Solution: Answer: $f(x) = x(x-1)(x-1-i)(x-1+i)$

We note that $f(x) = x(x^3 - 3x^2 + 4x - 2)$. By RRT the candidates for rational roots are $\pm 1, \pm 2$. We note that $f(1) = 0$ and thus $x - 1$ is a factor. Using long division (or synthetic division) we get that $f(x) = x(x-1)(x^2 - 2x + 2)$. Using the quadratic formula we obtain that $x = 1 + i, 1 - i$. Thus $f(x) = x(x-1)(x-1-i)(x-1+i)$.

6. For how many integers a satisfying $1 \leq a \leq 21$ does the linear equation

$$ax + 14y = 2$$

have at least one integer solution (x, y)? **[3 marks]**

Solution: Answer: 18

There will be at least one solution if $\gcd(a, 14) \mid 2$. The positive divisors of 14 are $1, 2, 7, 14$. Therefore $\gcd(a, 14)$ could possibly be 1, 2, 7, or 14. Only in the cases of 7 and 14 will we have that $\gcd(a, 14) \nmid 2$. For $1 \leq a \leq 21$, if $\gcd(a, 14) = 7$, then $a = 7, 21$. For $1 \leq a \leq 21$, if $\gcd(a, 14) = 14$, then $a = 14$. Therefore, there will be at least one integer solution provided $a \neq 7, 14, 21$. Therefore, there are $21 - 3 = 18$ values of a that will result in at least one integer solution.

For each part below, in the box provided, indicate whether the given statement is true (T) or false (F). No justification is required. **[1 mark each]**

7. (a) For all statement variables P and Q, $\neg(P \implies Q)$ is logically equivalent to $\neg P \implies \neg Q$.

   FALSE

   (b) For all $x, y, z \in \mathbb{Z}$, if $5 \mid (xy + xz)$, then $5 \mid x$ or $5 \mid y$ or $5 \mid z$.

   FALSE

   (c) The number -32 has a complex fifth root which is purely imaginary.

   FALSE

   (d) The element [5] has a multiplicative inverse in $\mathbb{Z}_9$.

   TRUE

(e) For all sets A, B and C, $A - (B \cup C) = (A - B) \cup (A - C)$.

FALSE

(f) For all polynomials $f(x) \in \mathbb{R}[x]$, if $f(i) = 0$, then $f\left(\frac{1}{i}\right) = 0$.

TRUE

(g) If $f(z) = z^{12} - z + 65 + i$, then $1 + i$ is a complex root of $f(z)$.

TRUE

The remaining questions require proofs. Write clearly and justify your steps. Do NOT use the amount of available space as an indication of how long your answer "should be".

8. Prove that for all integers a, b, c and d, if $a \mid b$ and $ac \mid d$, then $a \mid (3b - 5d)$. **[3 marks]**

Solution: Assume that $a \mid b$ and $ac \mid d$. Since $a \mid ac$, then by TD, $a \mid d$. Then by DIC, $a \mid (3b - 5d)$.

9. Prove that for all $a, b \in \mathbb{Z}$, and all $c \in \mathbb{N}$, if $\gcd(a, b) = 1$ and $c \mid a$, then $\gcd(a, bc) = c$. **[4 marks]**

Solution: Assume that $\gcd(a, b) = 1$ and $c \mid a$. Clearly $c \mid bc$ and so c is a common divisor of a and bc. By BL, there exist integers s and t such that $as + bt = 1$. Multiplying through by c we obtain $acs + bct = c$. Since $cs, t \in \mathbb{Z}$, then by GCD CT, $\gcd(a, bc) = c$.

10. Prove that for all $z \in \mathbb{C}$, if $w = z^3 - 3z^2(\overline{z}) + 3z(\overline{z})^2 - (\overline{z})^3$, then w is purely imaginary. **[3 marks]**

Solution 1: Consider $\overline{w} = \overline{z^3 - 3z^2(\overline{z}) + 3z(\overline{z})^2 - (\overline{z})^3} = \overline{z}^3 - 3\overline{z}^2 z + 3\overline{z}z^2 - z^3 = -w$. Since $\overline{w} = -w$, then w is purely imaginary.

Solution 2: We note that $w = (z - \overline{z})^3$. Since $z - \overline{z} = 2\text{Im}(z)i$, then $w = (2\text{Im}(z)i)^3 = -8i\text{Im}(z)$. Since $-8\text{Im}(z) \in \mathbb{R}$, then w is purely imaginary.

Solution 3: Let $z = a + bi$ where $a, b \in \mathbb{R}$. Then $\overline{z} = a - bi$. Expanding, $z^2 = (a + bi)^2 = a^2 - b^2 + 2abi$ and $(\overline{z})^2 = (a - bi)^2 = a^2 - b^2 - 2abi$.

Multiplying, $z^2(\overline{z}) = (a^2 - b^2 + 2abi)(a - bi) = a^3 + ab^2 + (a^2b + b^3)i$ and $(\overline{z})^2 z = (a^2 - b^2 - 2abi)(a + bi) = a^3 + ab^2 + (-a^2b - b^3)i$. By the Binomial Thm, $z^3 = a^3 - 3ab^2 + i(3a^2b - b^3)$ while $(\overline{z})^3 = a^3 - 3ab^2 + i(b^3 - 3a^2b)$. Finally,

$$\begin{aligned} z^3 - 3z^2(\overline{z}) + 3z(\overline{z})^2 - (\overline{z})^3 &= a^3 - 3ab^2 + (3a^2b - b^3)i \\ &\quad -3(a^3 + ab^2) - 3(a^2b + b^3)i \\ &\quad +3(a^3 + ab^2) + 3(-a^2b - b^3)i \\ &\quad -(a^3 - 3ab^2) - (b^3 - 3a^2b)i \\ &= -8b^3 i \end{aligned}$$

which is purely imaginary.

Solution 4:

Let $z = r\text{cis}\theta$. Then $\overline{z} = r\text{cis}(-\theta)$. Thus $z^2(\overline{z}) = r^3\text{cis}\theta$ and $z(\overline{z})^2 = r^3\text{cis}(-\theta)$ while $z^3 = r^3\text{cis}3\theta$ and $(\overline{z})^3 = r^3\text{cis}(-3\theta)$. Thus

$$\begin{aligned} & z^3 - 3z^2(\overline{z}) + 3z(\overline{z})^2 - (\overline{z})^3 \\ = \; & r^3\text{cis}3\theta - 3r^3\text{cis}\theta + 3r^3\text{cis}(-\theta) - r^3\text{cis}(-3\theta) \\ = \; & r^3[(\cos 3\theta - 3\cos\theta + 3\cos(-\theta) - \cos(-3\theta)) \\ & +i(\sin 3\theta - 3\sin\theta + 3\sin(-\theta) - \sin(-3\theta)] \\ = \; & r^3[0 + i(2\sin 3\theta - 6\sin\theta)] \text{ since } \cos(\beta) = \cos(-\beta), \sin(-\beta) = -\sin(\beta) \end{aligned}$$

which is purely imaginary.

11. A sequence $a_1, a_2, a_3, \ldots$ is defined by $a_1 = 14$, $a_2 = 21$ and $a_m = 3a_{m-1} + a_{m-2}$ for all integers $m \geq 3$. Prove that $\gcd(a_n, a_{n+1}) = 7$ for all $n \in \mathbb{N}$. **[5 marks]**

Solution: *Base case:* When $n = 1$ we need to show that $\gcd(a_1, a_2) = 7$. Since $a_1 = 14$ and $a_2 = 21$, then $\gcd(a_1, a_2) = \gcd(14, 21) = 7$ as required.

Inductive Hypothesis: For an arbitrary natural number k, we assume that $\gcd(a_k, a_{k+1}) = 7$.

Inductive Conclusion: We need to show that $\gcd(a_{k+1}, a_{k+2}) = 7$.

Since $k \in \mathbb{N}$, then $k + 2 \geq 3$. Therefore, $a_{k+2} = 3a_{k+1} + a_k$. Thus $\gcd(a_{k+2}, a_{k+1}) = \gcd(a_{k+1}, a_k)$ by GCD WR. By the Inductive Hypothesis, we have that $\gcd(a_k, a_{k+1}) = 7$. Therefore, $\gcd(a_{k+2}, a_{k+1}) = 7$ as desired.

By POMI, $\gcd(a_n, a_{n+1}) = 7$ for all $n \in \mathbb{N}$.

12. Let $A = \{x \in \mathbb{Z} : x \equiv 4 \pmod 6 \wedge x \equiv 4 \pmod{10}\}$ and $B = \{y \in \mathbb{Z} : y \equiv 4 \pmod{60}\}$. For each of the following statements, clearly indicate whether it is true or false and then prove or disprove the statement. **[5 marks]**

(a) $A \subseteq B$.

Solution: The statement is false.

Consider $x = 34$ as a counterexample. We note that $34 \equiv 4 \pmod 6$ and $34 \equiv 4 \pmod{10}$. Therefore, $x \in A$. However $34 \not\equiv 4 \pmod{60}$. Therefore $x \notin B$. Therefore $A \not\subseteq B$.

(b) $B \subseteq A$.

Solution: The statement is true.

Let $y \in B$. Therefore, $y \equiv 4 \pmod{60}$. Therefore, $y = 4 + 60k$ for some integer k. Thus, $y \equiv 4 + 60k \equiv 4 \pmod 6$ and $y \equiv 4 + 60k \equiv 4 \pmod{10}$. Therefore, $y \in A$. Therefore, $B \subseteq A$.

13. Prove that for all $a \in \mathbb{Z}$, if $a^8 \not\equiv 1 \pmod{64}$, then $a \not\equiv 1 \pmod 8$. **[4 marks]**

Solution1: We will prove the contrapositive: If $a \equiv 1 \pmod 8$, then $a^8 \equiv 1 \pmod{64}$.

Assume that $a \equiv 1 \pmod 8$. Therefore, $[a] = [1]$ in $\mathbb{Z}_8$. So $[a^4 + 1] = [a^2 + 1] = [a + 1] = [2]$. So $[(a^4 + 1)(a^2 + 1)(a + 1)] = [0]$. Therefore, $8 \mid (a^4 + 1)(a^2 + 1)(a + 1)$. Since we also have that $a - 1 \equiv 0 \pmod 8$, then $64 \mid (a^4 + 1)(a^2 + 1)(a + 1)(a - 1)$. But $(a^4 + 1)(a^2 + 1)(a + 1)(a - 1) = a^8 - 1$ and so $64 \mid (a^8 - 1)$. Therefore, $a^8 \equiv 1 \pmod{64}$.

Solution 2: We will prove the contrapositive: If $a \equiv 1 \pmod 8$, then $a^8 \equiv 1 \pmod{64}$.

If $a \equiv 1 \pmod 8$ then $a = 8k+1$ for some integer k.
By BT1, $a^8 = (8k+1)^8 = 1 + \binom{8}{1}(8k)^1 + \sum_{m=2}^{8}\binom{8}{m}(8k)^m = 1 + 64k + 64\sum_{m=2}^{8}\binom{8}{m}8^{m-2}k^m$. Since each term in the sum is an integer, thus $a^8 \equiv 1 \pmod{64}$.

14. Prove that there exists a complex number $z \in \mathbb{C}$ such that $|z| > 1$ and $z^{135} + (2+3i)z - 100 = 0$.
[3 marks]

Solution 1: By FTA, there exists a complex number z such that $z^{135} + (2+3i)z - 100 = 0$. By way of contradiction we assume that for every root z, $|z| \leq 1$. Since $z^{135} + (2+3i)z - 100 = 0$, then $|z^{135} + (2+3i)z| = |100| = 100$. However, by the Triangle Inequality and the Properties of Modulus,

$$|z^{135} + (2+3i)z| \leq |z^{135}| + |(2+3i)z| = |z|^{135} + |2+3i||z| \leq 1 + \sqrt{13}.$$

Therefore, we have deduced that $100 \leq 1 + \sqrt{13}$ and this is a contradiction.

Solution 2: Let $f(z) = z^{135} + (2+3i)z - 100$. By FTA $f(z)$ has at least one complex root. By CPN $f(z) = (z-c_1)(z-c_2)\cdots(z-c_{135})$ for $c_i \in \mathbb{C}$. Comparing constant terms we obtain that $\prod_{i=1}^{135} c_i = 100$. By way of contradiction we assume that $|c_i| \leq 1$ for $1 \leq i \leq 135$. But then $100 = \left|\prod_{i=1}^{135} c_i\right| = \prod_{i=1}^{135}|c_i| \leq 1$ which is a contradiction.