MTH5130 Mock Exam Paper

9th January 2024

Q1

1. Find all integers satisfying $10x \equiv 511$ mod 841. Show your working. **[4]**
2. Find the last two digits of 2^{2021}. Show your working. **[8]**
3. Find all integers of order 6 mod 13. Moreover, find all primitive roots mod 13. **[8]** Show your working in both cases.

A1

(1) [Similar to examples seen in lectures] By Euclid's algorithm, $\gcd(10, 841) = 1$ and $(-84)\cdot 10 + 1 \cdot 841 = 1$ (simply spotting a solution to $10r + 841s = 1$ is fine). Multiplying -84 on the both sides of the congruence equation, we get

$$x \equiv 511 \cdot (-84) \equiv -33 \equiv 808$$

mod 841. Any integer congruent to 808 mod 841 defines a solution and this is unique mod 841.

[$x = 808$ gets only +2. Trial and error to find $x \equiv 808$ mod 841 gets only +3 as it does not really show that *the* solution to the equation is 808 mod 841]

(2) [Similar to examples seen in example sheets] We need to find $0 \leq z \leq 99$ satisfying $2^{2021} \equiv z$ mod 100. This is equivalent to finding $0 \leq z \leq 99$ satisfying $2^{2021} \equiv z$ mod 25 and $2^{2021} \equiv z$ mod 4. By Theorem 15,

$$2^{\phi(25)} = 2^{20} \equiv 1$$

mod 25 since $\phi(25) = \phi(5^2) = 5(5-1) = 20$. It follows that

$$2^{2021} = 2^{20\cdot 101+1} = (2^{20})^{101} 2 \equiv 2$$

mod 25.

On the other hand,

$$2^{2021} \equiv 0$$

mod 4.

Combining these, the integer z we are looking for is a solution to the system of congruence equations

$$\begin{aligned} x &\equiv 2 \mod 25 \\ x &\equiv 0 \mod 4 \end{aligned}$$

Since $\gcd(25, 4) = 1$, one can make appeal to the CRT. Euclid's algorithm shows that $1\cdot 25 + (-6)\cdot 4 = 1$, hence

$$x = 25 \cdot 1 \cdot 0 + 4 \cdot (-6) \cdot 2 = -48 \equiv 52$$

mod 100 defines a (unique) solution mod 100. Therefore, $z = 52$ is the last two digits.

[+2 for translating the problem into mod 4 and mod 25; +1 for computing 2^{2021} mod 4; +2 for computing 2^{2021} mod 25; +3 for the CRT]

(3) [Similar to examples seen in lectures]

z	1	2	3	4	5	6	7	8	9	10	11	12
order modulo 13	1	12	3	6	4	12	12	4	3	6	12	2

Hence the integers congruent to 4 or 10 all have order 6 mod 13 and the integers congruent to $2, 6, 7, 11$ are primitive roots mod 13.

[For order 3, +2 for correctly answering the question ('mod 13'); +2 for explaining how (for example, asserting that $4^6 \equiv 1$ is not enough; either showing by hand that $4^2, 4^3, 4^4, 4^5$ are all NOT congruent to 1 or make reference to a statement from the lecture that the order has to be a divisor of 12 and pointing out that $4^2, 4^3$ are not congruent to 1 mod 13). Similar for order 12]

Q2

1. Deduce that 143 is not a prime number from the congruence $3^{143} \equiv 126$ mod 143. State clearly any result you are using from lectures. **[3]**
2. Let p be a prime number and let z be a primitive root mod p. Prove that

$$1, z, z^2, \ldots, z^{p-2}$$

   are all distinct mod p. [Hint: z is invertible mod p, i.e. for any integers a and b, if $za \equiv zb$ mod p, then $a \equiv b$ mod p, and z has order $p - 1$] **[9]**
3. Assume that 741 and 9283 are prime numbers. Using the properties of Legendre symbol, compute the Legendre symbol $\left(\frac{741}{9283}\right)$. Justify your answer. **[6]**

A2

(1) [Similar to examples seen in lectures] If 143 was a prime number, then it would have followed form the Fermat's Little Theorem that $3^{143} \equiv 3$ mod 143. However, 3 is evidently not congruent to 126 mod 143. Hence 143 is NOT a prime number.

[+2 for reference to Fermat's Little Theorem]

(2) [Seen in lectures] If $z^r \equiv z^s$ for $0 \leq r \leq s \leq p - 2$, then $z^{s-r} \equiv 1$ mod p (since z is a primitive root mod p, z has multiplicative inverse mod p). However, $s - r \leq p - 2$ and the order of z by definition is $p - 1$. It therefore follows that $s = r$.

(3)

$$
\begin{aligned}
& \left(\frac{741}{9283}\right) \\
\overset{R4}{=}\ & \left(\frac{9283}{741}\right) \\
\overset{R0}{=}\ & \left(\frac{391}{741}\right) \\
\overset{R4}{=}\ & \left(\frac{741}{391}\right) \\
\overset{R0}{=}\ & \left(\frac{350}{391}\right) \\
\overset{R1}{=}\ & \left(\frac{2}{391}\right)\left(\frac{175}{391}\right) \\
\overset{R3}{=}\ & \left(\frac{175}{391}\right) \\
\overset{R4}{=}\ & -\left(\frac{391}{175}\right) \\
\overset{R0}{=}\ & -\left(\frac{41}{175}\right) \\
\overset{R4}{=}\ & -\left(\frac{175}{41}\right) \\
\overset{R0}{=}\ & -\left(\frac{11}{41}\right) \\
\overset{R4}{=}\ & -\left(\frac{41}{11}\right) \\
\overset{R0}{=}\ & -\left(\frac{8}{11}\right) \\
\overset{R1}{=}\ & -\left(\frac{2}{11}\right)^2\left(\frac{2}{11}\right) \\
=\ & -\left(\frac{2}{11}\right) \\
\overset{R2}{=}\ & (-1)(-1) = 1
\end{aligned}
$$

[+0 for answering that $\left(\frac{741}{9283}\right) = -1$**; +1 for simply answering that** $\left(\frac{741}{9283}\right) = +1$**;** -1 **for any single 'lucky mistake']**

Q3

Which of the following congruences are soluble? If soluble, find a positive integer solution less than 47; if insoluble, explain why.

(i) $x^2 \equiv 41 \bmod 47$. **[4]**

(ii) $3x^2 \equiv 32 \bmod 47$. **[8]**

A3

(a-i) [Similar to examples seen in lectures] Since

$$\left(\frac{41}{47}\right) \overset{R4}{=} (-1)^{\frac{47-1}{2}\frac{41-1}{2}}\left(\frac{47}{41}\right) = \left(\frac{47}{41}\right) \overset{R0}{=} \left(\frac{6}{41}\right) \overset{R1}{=} \left(\frac{2}{41}\right)\left(\frac{3}{41}\right) \overset{R3,\mathrm{Cor}26}{=} 1\cdot(-1) = -1,$$

this is insoluble.

[+1 for simply pointing out that it is insoluble; +3 for reference to the Legendre symbol (i.e. calculating it); get only +1 for merely pointing out 41 is a quadratic non-residue mod 47]

(a-ii) [Partly unseen] Since $\gcd(3,47) = 1$, we run the Euclid's algorithm, if necessary, to find $16 \cdot 3 + (-1) \cdot 47 = 1$. It therefore follows that

$$16 \cdot 3x^2 \equiv 16 \cdot 32$$

mod 47, i.e.

$$x^2 \equiv 512 \equiv 42$$

mod 47. Since

$$\begin{aligned} & \left(\frac{42}{47}\right) \\ \overset{R1}{=} \quad & \left(\frac{2}{47}\right)\left(\frac{3}{47}\right)\left(\frac{7}{47}\right) \\ \overset{R3,\text{Cor}26}{=} \quad & 1 \cdot (-1) \left(\frac{7}{47}\right) \\ \overset{R4}{=} \quad & (-1)(-1)^{\frac{47-1}{2}\frac{7-1}{2}} \left(\frac{47}{7}\right) \\ \overset{R0}{=} \quad & -\left(\frac{5}{7}\right) \\ \overset{R4}{=} \quad & (-1)(-1)^{\frac{5-1}{2}\frac{7-1}{2}} \left(\frac{7}{5}\right) \\ \overset{R0}{=} \quad & \left(\frac{2}{5}\right) \\ \overset{R3}{=} \quad & (-1)(-1) \\ = \quad & 1 \end{aligned},$$

this latter congruence equation is soluble. To find a solution, either you do trial and error (I'll allow it), or make appeal to Proposition 28 which shows that

$$42^{\frac{47+1}{4}} = 42^{12}$$

defines a solution mod 47. It remains to simply 42^{12} mod 47. Since $12 = 2^3 + 2^2$ and

$$42^2 \equiv (-5)^2 = 25, 42^{2^2} \equiv 25^2 = 625 \equiv 14,\ 42^{2^3} \equiv 14^2 = 196 \equiv 8$$

mod 47

$$42^{12} = 2^{2^3+2^2} \equiv 8 \cdot 14 = 112 \equiv 18$$

mod 47. So $x = 18$ does the job.

[+4 for simplifying the equation; +2 for reference to Proposition 28; +2 for simplifying 42^{12} mod 47]

Q4

1. Compute the continued fraction expression for $\sqrt{23}$. Show your working. **[4]**

2. Compute the convergents $\frac{s_1}{t_1}, \frac{s_2}{t_2}, \frac{s_3}{t_3}$ to $\sqrt{23}$. Show your working. **[4]**

3. ($\geq$ Week 9) By working out the second smallest positive solution to the equation $x^2 - 23y^2 = 1$, compute the convergent $\frac{s_7}{t_7}$. **[10]**

A4 (1) [Similar to examples seen in lectures] By the algorithm:

$$\begin{array}{ccc}
\alpha = \lfloor\sqrt{23}\rfloor = 4 & \Rightarrow & \rho_1 = \dfrac{1}{\sqrt{23}-4} = \dfrac{\sqrt{23}+4}{7} \\
& \swarrow & \\
\alpha_1 = \lfloor\dfrac{\sqrt{23}+4}{7}\rfloor = 1 & \Rightarrow & \rho_2 = \dfrac{1}{\frac{\sqrt{23}+4}{7} - 1} = \dfrac{\sqrt{23}+3}{2} \\
& \swarrow & \\
\alpha_2 = \lfloor\dfrac{\sqrt{23}+3}{2}\rfloor = 3 & \Rightarrow & \rho_3 = \dfrac{1}{\frac{\sqrt{23}+3}{2} - 3} = \dfrac{\sqrt{23}+3}{7} \\
& \swarrow & \\
\alpha_3 = \lfloor\dfrac{\sqrt{23}+3}{7}\rfloor = 1 & \Rightarrow & \rho_4 = \dfrac{1}{\frac{\sqrt{23}+3}{7} - 1} = \sqrt{23}+4 \\
& \swarrow & \\
\alpha_4 = \lfloor\sqrt{23}+4\rfloor = 8 & \Rightarrow & \rho_5 = \dfrac{1}{(\sqrt{23}+4)-8} = \dfrac{1}{\sqrt{23}-4} = \rho_1 \\
& \swarrow & \\
\alpha_5 = \alpha_1 & \cdots &
\end{array}$$

we find $\sqrt{23} = [\alpha; \overline{\alpha_1, \alpha_2, \alpha_3, \alpha_4}] = [4; \overline{1, 3, 1, 8}]$.

[+1 for simply answering the question; +3 for explaining calculations]

(2) [Similar to examples seen in lectures] The convergents are calculated as

$$\begin{aligned}
\frac{s_{-1}}{t_{-1}} &= \frac{1}{0}, \\
\frac{s_0}{t_0} &= \frac{\alpha}{1} = \frac{4}{1}, \\
\frac{s_1}{t_1} &= \frac{\alpha_1 s_0 + s_{-1}}{\alpha_1 t_0 + t_{-1}} = \frac{1\cdot 4+1}{1\cdot 1+0} = \frac{5}{1}, \\
\frac{s_2}{t_2} &= \frac{\alpha_2 s_1 + s_0}{\alpha_2 t_1 + t_0} = \frac{3\cdot 5+4}{3\cdot 1+1} = \frac{19}{4}, \\
\frac{s_3}{t_3} &= \frac{\alpha_3 s_2 + s_1}{\alpha_3 t_2 + t_1} = \frac{1\cdot 19+5}{1\cdot 4+1} = \frac{24}{5}.
\end{aligned}$$

[+1 each]

(3) [Similar to examples seen in lectures] Since the cycle is of length $l = 4$, the fundamental solution to $x^2 - 23y^2 = \pm 1$ is $(s_3, t_3) = (24, 5)$. By Theorem 48, for every $N = 1, 2, \ldots$, the pair (s_{4N-1}, t_{4N-1}) is a solution to $x^2 - 23y^2 = (-1)^{4N} = 1$, hence the second smallest solution to $x^2 - 23y^2 = \pm 1$ is defined to be (s_7, t_7). On the other hand, $s_7 + t_7\sqrt{23}$ can be computed by

$$(24 + 5\sqrt{23})^2 = 1151 + 240\sqrt{23},$$

hence $(s_7, t_7) = (1151, 240)$.

[+1 for spotting the fundamental solution; +3 for pointing out (s_3, t_3) is the fundamental solution; +3 for pointing out that the second smallest positive solution is (s_7, t_7); +3 for correctly calculating (s_7, t_7)]

Q5

1. Using that 137 is a prime number, find all solutions to
$$x^2 \equiv -1 \mod 137$$
satisfying $1 \leq x \leq 137$. Show your working. **[9]**

2. ($\geq$ Week 10) Using (1), write 137 as a sum of two squares. Show your working. State clearly any results you are using from lectures. **[9]**

A5 (1) Since $137 \equiv 1 \bmod 4$, we may use Proposition 29. To this end, we firstly find a such that $\left(\frac{a}{137}\right) = -1$. For example $a = 3$ does the job. It then follows from Proposition 29 that $3^{\frac{137-1}{4}} = 3^{34}$ is a solution mod 137. Since

$$3^{2^2} = 81,\ \ 3^{2^3} = 81^2 \equiv 122,\ \ 3^{2^4} \equiv 88,\ \ 3^{2^5} \equiv 72,$$

we see that
$$3^{34} = 3^{2^5+2} = 3^{2^5}3^2 \equiv 72 \cdot 9 = 648 \equiv 100$$
mod 137. Since 100 is a solution mod 137, so is $-100 \equiv 37$ mod 137.

[+2 for reference to Proposition 29 (in particular, +1 for asserting that $137 \equiv 1$ mod 4); +2 for finding a; +3 for simplifying 3^{34} mod 137 to get one solution; +2 for spotting the solutions]

(2) We make appeal to Hermite's algorithm with $z = 37$ as its first step. Convergents to $\frac{37}{137}$ are calculated as follows: by the algorithm,

$$\begin{array}{ccc}
\alpha = \lfloor \frac{37}{137} \rfloor = 0 & \Rightarrow & \rho_1 = \frac{1}{\frac{37}{137} - 0} = \frac{137}{37} \\
 & \swarrow & \\
\alpha_1 = \lfloor \frac{137}{37} \rfloor = 3 & \Rightarrow & \rho_2 = \frac{1}{\frac{137}{37} - 3} = \frac{37}{26} \\
 & \swarrow & \\
\alpha_2 = \lfloor \frac{37}{26} \rfloor = 1 & \Rightarrow & \rho_3 = \frac{1}{\frac{37}{26} - 1} = \frac{26}{11} \\
 & \swarrow & \\
\alpha_3 = \lfloor \frac{26}{11} \rfloor = 2 & \Rightarrow & \rho_4 = \frac{1}{\frac{26}{11} - 2} = \frac{11}{4} \\
 & \swarrow & \\
\alpha_4 = \lfloor \frac{11}{4} \rfloor = 2 & \Rightarrow & \rho_5 = \frac{1}{\frac{11}{4} - 2} = \frac{4}{3} \\
 & \swarrow & \\
\alpha_5 = \lfloor \frac{4}{3} \rfloor = 1 & \Rightarrow & \rho_6 = \frac{1}{\frac{4}{3} - 1} = 3 \in \mathbb{N} \\
 & \swarrow & \\
\alpha_6 = \lfloor 3 \rfloor = 3, & &
\end{array}$$

we see that $\frac{37}{137} = [\alpha; \alpha_1, \alpha_2, \alpha_3, \alpha_4, \alpha_5, \alpha_6] = [0; 3, 1, 2, 2, 1, 3]$. It therefore follows that

$$\frac{s_1}{t_1} = [0; 3] = \frac{1}{3}, \ \frac{s_2}{t_2} = [0; 3, 1] = \frac{1}{4}, \ \frac{s_3}{t_3} = [0; 3, 1, 2] = \frac{3}{11}, \ \frac{s_4}{t_4} = [0; 3, 1, 2, 2] = \frac{7}{26}, \ldots$$

Since

$$t_3 < \sqrt{137} < t_4,$$

the pair $(x, y) = (t_3, 137 \cdot s_3 - 37t_3) = (11, 137 \cdot 3 - 37 \cdot 11) = (11, 4)$ satisfies $x^2 + y^2 = 137$.

[+2 for correctly working out convergents; +4 for observing via Hermite that $(x, y) = (t_3, 137 \cdot s_3 - 37t_3)$ **is a solution; +3 to spot the solution]**

textbfQ6 Describe the units in the ring of integers in $\mathbb{Q}(\sqrt{75})$.

A6 While $75 \equiv 3$ mod 4, we can not use Proposition 63 to describe the ring of integers nor Proposition 66 to describe its units. Since $\sqrt{75} = 5\sqrt{3}$, it follows by definition that $\mathbb{Q}(\sqrt{75}) = \mathbb{Q}(\sqrt{3})$. It now follows from Proposition 63 that its ring of integers is $\mathbb{Z}[\sqrt{3}]$ and from Proposition 66 that the units in $\mathbb{Z}[\sqrt{3}]$ are of the form $s + t\sqrt{3}$ such that $r^2 - 3t^2 = \pm 1$. We know how to solve Pell's equation $x^2 - 3y^2 = \pm 1$. The continued fraction of $\sqrt{3}$ is $[1; \overline{1, 2}]$ with $l = 2$, hence the fundamental solution is $(s, t) = (s_1, t_1) = (2, 1)$. Defining $v_n + w_n\sqrt{3} = (s + t\sqrt{3})^n = (2 + \sqrt{3})^n$, the pairs (v_n, w_n) define all the positive integer solutions to Pell's equation $x^2 - 3y^2 = \pm 1$, hence units. As the questions asks to describe all the units,

$$v_n + w_n\sqrt{3}, -v_n + w_n\sqrt{3}, v_n - w_n\sqrt{3}, -v_n - w_n\sqrt{3}$$

define the units. □