# MTH5130 2021-2022 Semester A Exam

Dr Shu Sasaki

7th February 2022

**Q1** (a) Find an integer $1 \leq z \leq 143$ satisfying $z \equiv 3^{143} \bmod 143$. Show your working. (Hint: $143 = 2^7 + 2^3 + 2^2 + 2^1 + 1$ and $3^{16} \equiv 3 \bmod 143$) **[6]**

(b) Use (a) to show that 143 is not a prime number. State clearly any result you are using from lectures. **[3]**

(c) 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 $p$. **[9]**

**A1**. (a) [Similar to examples seen in lectures] Since

$$3^{2^2} = 81,\ 3^{2^3} = (81)^2 \equiv (-17),\ 3^{2^4} \equiv (-17)^2 \equiv 3,\ 3^{2^5} \equiv 3^2 = 9, 3^{2^6} \equiv 9^2 = 81,\ 3^{2^7} \equiv (-17)$$

it follows that

$$3^{143} = 3^{2^7+2^3+2^2+2+1} \equiv (-17) \cdot (-17) \cdot 81 \cdot 9 \cdot 3 \equiv 3 \cdot 81 \cdot 9 \cdot 3 \equiv (81)^2 \equiv (-17) \equiv 126.$$

Hence $z = 126$ is what we are looking for.

**[+2 for spotting $z = 126$; +4 for explaining how]**

(b) [Similar to examples seen in lectures] If 143 was a prime number, then it would have followed form the Fermat's Little Theorem that $3^{143} \equiv 3 \bmod 143$. 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]**

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

**[+3 for establishing that $z$ has multiplicative inverse (remarking that $z$ is coprime to $p$ is not enough, while deducing from $z^{p-1} \equiv 1 \bmod p$ qualifies for +3), and +3 for arguing why the argument leads to contradiction (the order of $z$ is $p - 1$)]**

**Q2** Let $p > 3$ be a prime number. State clearly any results you are using from lectures and prove the following:

(a)

$$\left(\frac{p}{3}\right) = \begin{cases} +1 & \text{if } p \equiv 1 \bmod 3, \\ -1 & \text{if } p \equiv 2 \bmod 3. \end{cases} \quad \textbf{[3]}$$

(b)

$$\left(\frac{3}{p}\right) = \begin{cases} +\left(\frac{p}{3}\right) & \text{if } p \equiv 1 \bmod 4, \\ -\left(\frac{p}{3}\right) & \text{if } p \equiv 3 \bmod 4. \end{cases} \quad \textbf{[3]}$$

(c)

$$\left(\frac{3}{p}\right) = \begin{cases} +1 & \text{if } p \equiv 1 \text{ or } 11 \bmod 12, \\ -1 & \text{if } p \equiv 5 \text{ or } 7 \bmod 12. \end{cases} \quad \textbf{[9]}$$

**A2** (a) [Seen in lectures] The only prime $p$ divisible by 3 is $p = 3$ and this is excluded. Modulo 3, we have

| $z$ | 1 | 2 |
|---|---|---|
| $z^2$ | 1 | 1, |

i.e. 1 is a square mod 3 while 2 is not. The statement paraphrases this.

**[Since I did not prove the Rules, I'd have to allow students to prove** $\left(\frac{p}{3}\right) = -1$ **if** $p \equiv 2$ **mod** $p$**, by arguing that** $\left(\frac{p}{3}\right) \overset{\text{R0}}{\equiv} \left(\frac{2}{3}\right) \overset{\text{R3}}{\equiv} (-1)^{(3^2-1)/8} = -1$ **]**

(b) [Seen in lectures] This follows from quadratic reciprocity (Rule 4):

$$\left(\frac{3}{p}\right) = (-1)^{\frac{p-1}{2}\frac{3-1}{2}} \left(\frac{p}{3}\right) = (-1)^{\frac{p-1}{2}} \left(\frac{p}{3}\right)$$

where $\dfrac{p-1}{2}$ is even (resp. odd) if and only if $p \equiv 1$ (resp. $p \equiv 3$) mod 4.

(c) [Partly seen in lectures] Combining (a) and (b),

$$\left(\frac{3}{p}\right) = \begin{cases} +\left(\frac{p}{3}\right) & \text{if } p \equiv 1 \bmod 4, \text{ which yields} \begin{cases} +1 & \text{if } p \equiv 1 \bmod 3, \\ -1 & \text{if } p \equiv 2 \bmod 3, \end{cases} \\ -\left(\frac{p}{3}\right) & \text{if } p \equiv 3 \bmod 4, \text{ which yields} \begin{cases} -1 & \text{if } p \equiv 1 \bmod 3, \\ +1 & \text{if } p \equiv 2 \bmod 3, \end{cases} \end{cases}$$

hence

$$\left(\frac{3}{p}\right) = \begin{cases} +1 & \text{if (1) } p \equiv 1 \bmod 4 \;\&\; p \equiv 1 \bmod 3 \text{ or (2) } p \equiv 3 \bmod 4 \;\&\; p \equiv 2 \bmod 3, \\ -1 & \text{if (3) } p \equiv 1 \bmod 4 \;\&\; p \equiv 2 \bmod 3 \text{ or (4) } p \equiv 3 \bmod 4 \;\&\; p \equiv 1 \bmod 3. \end{cases}$$

It then follows from the CRT that (1) is equivalent to $p \equiv 1$ mod 12, (2) is equivalent to $p \equiv 11$ mod 12, (3) is equivalent to $p \equiv 5$ mod 12 and (4) is equivalent to $p \equiv 7$ mod 12.

To show (1) for example, we look for solutions (in prime numbers) to the following system of congruence equations:

$$\begin{aligned} x &\equiv 1 \mod 4 \\ x &\equiv 1 \mod 3 \end{aligned}$$

As $\gcd(4,3) = 1$, we use Euclidean algorithm to find $r$ and $s$ such that $4r+3s = \gcd(4,3) = 1$; in this case it is simple to spot $(r,s) = (1,-1)$ works and the proof of the CRT (Theorem 9) then shows that

$$4 \cdot 1 \cdot 1 + 3 \cdot (-1) \cdot 1 = 1$$

defines a unique solution mod $4 \cdot 3 = 12$. Similar for (2), (3) and (4).

**[+3 for reducing the problem into (1)-(4); +6 for the CRT or any valid argument for the punchline (+1 out of +6 for reference to CRT, +2 in total for proving the case I demonstrated); though it is not how I intended, I'd allow the full +9 for the case-by-case analysis: if $p \equiv 1$ mod $12$, then... etc.]**

**Q3** (a) 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]**

(b) Using Hensel's lemma, find all integers $1 \leq z \leq 125$ satisfying $z^2 + z \equiv -3 \bmod 125$. **[9]**

**A3** (a-i) [Similar to examples seen in lectures] Since

$$\left(\frac{41}{47}\right) \stackrel{R4}{=} (-1)^{\frac{47-1}{2}\frac{41-1}{2}} \left(\frac{47}{41}\right) = \left(\frac{47}{41}\right) \stackrel{R0}{=} \left(\frac{6}{41}\right) \stackrel{R1}{=} \left(\frac{2}{41}\right)\left(\frac{3}{41}\right) \stackrel{R3,\mathrm{Cor26}}{=} 1 \cdot (-1) = -1,$$

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 $47$; -1 for no reference to Rules]**

(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

$$
\begin{aligned}
& \left(\frac{42}{47}\right) \\
\overset{R1}{=} \quad & \left(\frac{2}{47}\right)\left(\frac{3}{47}\right)\left(\frac{7}{47}\right) \\
\overset{R3,\mathrm{Cor26}}{=} \quad & 1 \cdot (-1)\left(\frac{7}{47}\right) \\
\overset{R4}{=} \quad & (-1)(-1)^{\frac{47-1}{2}\frac{7-1}{2}}\left(\frac{47}{7}\right) \\
\overset{R0}{=} \quad & -\left(\frac{5}{7}\right) \\
\overset{R4}{=} \quad & (-1)(-1)^{\frac{5-1}{2}\frac{7-1}{2}}\left(\frac{7}{5}\right) \\
\overset{R0}{=} \quad & \left(\frac{2}{5}\right) \\
\overset{R3}{=} \quad & (-1)(-1) \\
= \quad & 1
\end{aligned},
$$

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]**

(b) [Similar to examples seen in lectures] Let $P(x) = x^2 + x + 3$. The $P'(x) = 2x + 1$.

$\boxed{\text{Step 1}}$ Find all solutions to $P(x) \equiv 0$ mod 5. By trial and error, $z_1 \equiv 1$ or 3 mod 5 works.

$\boxed{\text{Step 2}}$ Let $z_1 = 1$. Since $P'(z_1) = 2z_1 + 1 = 3$, the multiplicative inverse $Q'(z_1)$ of $P'(z_1)$ mod 5 is 2. To find $Q'(z_1)$, we need to solve the congruence equation $3x \equiv 1$ mod 5 by either using Euclid's algorithm to find a pair of integers $r, s$ such that $3r + 5s = 1$ (and reduce mod 5) or computing the mod 5 table

| $r$ | 0 | 1 | 2 | 3 | 4 |
|---|---|---|---|---|---|
| $3r$ | 0 | 3 | 1 | 4 | 2 |

It now follows from Hensel's lemma that

$$z_1 - P(z_1)Q'(z_1) = 1 - 5 \cdot 2 = -9 \equiv 16$$

defines a solution to $P(x) \equiv 0 \bmod 5^2$.

$\boxed{\text{Step 3}}$ Let $z_2 = 16$. Since $Q'(z_1) = Q'(z_2) = 2$, it follows from Hensel's lemma that

$$z_2 - P(z_2)Q'(z_2) = 16 - 275 \cdot 2 = -534 \equiv 91$$

defines a solution mod $5^3 = 125$.

To find the other solution, we repeat run the same algorithm:

$\boxed{\text{Step 2'}}$ Let $z_1 = 3$. Since $P'(z_1) = 2z_1 + 1 = 2 \cdot 3 + 1 = 7 \equiv 2 \bmod 5$, the multiplicative inverse $Q'(z_1)$ of $P'(z_1)$ mod 5 is 3. It then follows from Hensel's lemma that

$$z_1 - P(z_1)Q'(z_1) = 3 - 15 \cdot 3 = -42 \equiv 8$$

defines a solution to $P(x) \equiv 0 \bmod 5^2$.

$\boxed{\text{Step 3'}}$ Let $z_2 = 8$. Since $Q'(z_1) = Q'(z_2) = 2$, it follows from Hensel's lemma that

$$z_2 - P(z_2)Q'(z_2) = 8 - 75 \cdot 3 = -217 \equiv 33$$

defines a solution mod $5^3 = 125$.

Since $P(x)$ is quadratic, there are at most two solutions mod 125. They are $\{91, 33\}$.

**[+1 for spotting the solutions correctly; +2 for spotting the mod 5 solutions; +2 for Step 2 with $z_1 = 1$; +1 for Step 3 with $z_1 = 1$; +2 for Step 2 with $z_1 = 3$; +1 for Step 3 with $z_1 = 3$]**

**Q4** (a) Compute the continued fraction expression for $\sqrt{23}$. Show your working. **[4]**

(b) 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]**

(c) 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** (a) [Similar to examples seen in lectures] By the algorithm:

$$
\begin{array}{ccc}
a = \lfloor\sqrt{23}\rfloor = 4 & \longrightarrow & \rho_1 = \dfrac{1}{\sqrt{23}-4} = \dfrac{\sqrt{23}+4}{7} \\
 & \swarrow & \\
a_1 = \lfloor\dfrac{\sqrt{23}+4}{7}\rfloor = 1 & \longrightarrow & \rho_2 = \dfrac{1}{\frac{\sqrt{23}+4}{7}-1} = \dfrac{\sqrt{23}+3}{2} \\
 & \swarrow & \\
a_2 = \lfloor\dfrac{\sqrt{23}+3}{2}\rfloor = 3 & \longrightarrow & \rho_3 = \dfrac{1}{\frac{\sqrt{23}+3}{2}-3} = \dfrac{\sqrt{23}+3}{7} \\
 & \swarrow & \\
a_3 = \lfloor\dfrac{\sqrt{23}+3}{7}\rfloor = 1 & \longrightarrow & \rho_4 = \dfrac{1}{\frac{\sqrt{23}+3}{7}-1} = \sqrt{23}+4 \\
 & \swarrow & \\
a_4 = \lfloor\sqrt{23}+4\rfloor = 8 & \longrightarrow & \rho_5 = \dfrac{1}{(\sqrt{23}+4)-8} = \dfrac{1}{\sqrt{23}-4} = \rho_1 \\
 & \swarrow & \\
a_5 = a_1 & \dots &
\end{array}
$$

we find $\sqrt{23} = [a; \overline{a_1, a_2, a_3, a_4}] = [4; \overline{1, 3, 1, 8}]$.

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

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

$$
\begin{aligned}
\frac{s_{-1}}{t_{-1}} &= \frac{1}{0}, \\
\frac{s_0}{t_0} &= \frac{a}{1} = \frac{4}{1}, \\
\frac{s_1}{t_1} &= \frac{a_1 s_0 + s_{-1}}{a_1 t_0 + t_{-1}} = \frac{1\cdot 4+1}{1\cdot 1+0} = \frac{5}{1}, \\
\frac{s_2}{t_2} &= \frac{a_2 s_1 + s_0}{a_2 t_1 + t_0} = \frac{3\cdot 5+4}{3\cdot 1+1} = \frac{19}{4}, \\
\frac{s_3}{t_3} &= \frac{a_3 s_2 + s_1}{a_3 t_2 + t_1} = \frac{1\cdot 19+5}{1\cdot 4+1} = \frac{24}{5}.
\end{aligned}
$$

**[+1 each]**

(c) [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 $N = 1, 2, \dots$, 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** (a) [Similar to examples seen in lectures] 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]**

(b) [Similar to examples seen in lectures] Using (a), write 137 as a sum of two squares. Show your working. State clearly any results you are using from lectures. **[9]**

**A5** (a) Since $137 \equiv 1 \mod 4$, 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]**

(b) 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,

$$\begin{array}{lcl}
a = \lfloor \frac{37}{137} \rfloor = 0 & \longrightarrow & \rho_1 = \frac{1}{\frac{37}{137} - 0} = \frac{137}{37} \\
 & \swarrow & \\
a_1 = \lfloor \frac{137}{37} \rfloor = 3 & \longrightarrow & \rho_2 = \frac{1}{\frac{137}{37} - 3} = \frac{37}{26} \\
 & \swarrow & \\
a_2 = \lfloor \frac{37}{26} \rfloor = 1 & \longrightarrow & \rho_3 = \frac{1}{\frac{37}{26} - 1} = \frac{26}{11} \\
 & \swarrow & \\
a_3 = \lfloor \frac{26}{11} \rfloor = 2 & \longrightarrow & \rho_4 = \frac{1}{\frac{26}{11} - 2} = \frac{11}{4} \\
 & \swarrow & \\
a_4 = \lfloor \frac{11}{4} \rfloor = 2 & \longrightarrow & \rho_5 = \frac{1}{\frac{11}{4} - 2} = \frac{4}{3} \\
 & \swarrow & \\
a_5 = \lfloor \frac{4}{3} \rfloor = 1 & \longrightarrow & \rho_6 = \frac{1}{\frac{4}{3} - 1} = 3 \in \mathbb{N} \\
 & \swarrow & \\
a_6 = \lfloor 3 \rfloor = 3, & &
\end{array}$$

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]**

**Q6** What are the units of $\mathbb{Z}[\sqrt{15}]$? Describe them all. Justify your answer. **[10]**

**A6**. [Similar to examples seen in lectures] Since $15 \equiv 3 \bmod 4$, the units are of the form $s + t\sqrt{15}$ such that $s^2 - 15t^2 = \pm 1$. Since the continued fraction for $\sqrt{15}$ is $[\alpha; \overline{\alpha_1, \alpha_2}] = [3; \overline{1, 6}]$:

$$\begin{array}{lcl}
\alpha = \lfloor \sqrt{15} \rfloor = 3 & \longrightarrow & \rho_1 = \frac{1}{\sqrt{15}-3} = \frac{\sqrt{15}+3}{6} \\
& \swarrow & \\
\alpha_1 = \lfloor \frac{\sqrt{15}+3}{6} \rfloor = 1 & \longrightarrow & \rho_2 = \frac{1}{\frac{\sqrt{15}+3}{6} - 1} = \sqrt{15}+3 \\
& \swarrow & \\
\alpha_2 = \lfloor \sqrt{15}+3 \rfloor = 6 & \longrightarrow & \rho_3 = \frac{1}{(\sqrt{15}+3)-6} = \frac{1}{\sqrt{15}-3} = \rho_1 \\
& \swarrow & \\
\alpha_3 = \alpha_1 & \cdots &
\end{array}$$

with convergents:

$$\begin{aligned}
\frac{s_{-1}}{t_{-1}} &= \frac{1}{0}, \\
\frac{s_0}{t_0} &= \frac{\alpha}{1} = \frac{3}{1}, \\
\frac{s_1}{t_1} &= \frac{\alpha_1 s_0 + s_{-1}}{\alpha_1 t_0 + t_{-1}} = \frac{1 \cdot 3 + 1}{1 \cdot 1 + 0} = \frac{4}{1}, \\
\frac{s_2}{t_2} &= \frac{\alpha_2 s_1 + s_0}{\alpha_2 t_1 + t_0} = \frac{6 \cdot 4 + 3}{6 \cdot 1 + 1} = \frac{27}{7}, \\
&\cdots
\end{aligned}$$

the fundamental solution is $(s_1, t_1) = (4, 1)$. The units are of the form $s_n + t_n\sqrt{15}$, $s_n - t_n\sqrt{15}$, $-s_n + t_n\sqrt{15}$, $-s_n - t_n\sqrt{15}$ where $s_n$ and $t_n$ are defined by $s_n + t_n\sqrt{15} = (4 + \sqrt{15})^n$.

**[+3 for observing that it suffices to solve the equation $x^2 - 15y^2 = \pm 1$; +2 for finding the fundamental solution; +1 for observing that $s_n + t_n\sqrt{15}$ is a solution; +4 for spotting the rest]**