# MTH5130 Exam

Dr Shu Sasaki

7th December 2020

**Q1** (a) State Fermat's Little Theorem, and use it to prove that 15 is a composite number.

(b) Let $\phi$ be Euler's totient function. What is the parity of $\phi(15841)$? Justify your answer. State clearly any results you use from the lecture material without proofs.

(c) Find all the primitive roots mod 11 in $\{1, 2, \ldots, 10\}$. Justify your answers.

**A1** (a) [Bookwork+ Examples seen in lectures] Fermat's Little Theorem (Theorem 7) asserts that, if $p$ is a prime number, $a^p \equiv a \bmod p$ holds for any natural number (or any integer) $a$.

We simply spot an integer $a$ such that $a^{15}$ is *not* congruent to $a$ mod 15. For example, $a = 2$ does the job. Indeed, Since $2^4 \equiv 1 \bmod 15$,

$$2^{15} = 2^{1+2+4+8} \equiv 2 \cdot 2^2 \cdot 1 \cdot 1 = 8$$

mod 15.

(b) [Examples seen in Example Sheets] $\phi(n)$ is even for any integer $n > 2$ (Example Sheet 2, Q1-a). The 9-th Carmichael number certainly is $> 2$.

(c) [Examples seen in lectures] According to Theorem 22, there are $\phi(11 - 1) = \phi(10) = \phi(5)\phi(2) = 4 \cdot 1 = 4$ primitive roots mod 11 between 1 and 10. By Theorem 15 (a generalisation of Fermat's Little Theorem) and Lemma 19, the order $d$ of an integer $1 \leq z \leq 11$ divides $\phi(11) = 10$, so it is either 2, 5 or 10:

| $z$ | 1 | 2 | 3 | 4 | 5 | 6 | 7 | 8 | 9 | 10 |
|---|---|---|---|---|---|---|---|---|---|---|
| $d$ | 1 | 10 | 5 | 5 | 5 | 10 | 10 | 10 | 5 | 2 |

Hence $\{2, 6, 7, 8\}$ is the set of primitive roots mod 11 in $\{1, \ldots, 10\}$.

**Q2** Using the Chinese Remainder Theorem, solve the following simultaneous congruence equations in $x$. Show all your working.

$$\begin{aligned} 9x &\equiv 3 \mod 15, \\ 5x &\equiv 7 \mod 21, \\ 7x &\equiv 4 \mod 13. \end{aligned}$$

**A2** [Unseen+ Examples seen in Coursework] Firstly, observe that $9x \equiv 3 \bmod 15$ is equivalent to $3x \equiv 1 \bmod 5$, which is equivalent to $x \equiv 2 \bmod 5$ since $2 \cdot 3 - 1 \cdot 5 = 1$.

Since $(-4) \cdot 5 + 1 \cdot 21 = \gcd(5, 21) = 1$, it follows that $x \equiv (-4) \cdot 7 \equiv 14 \bmod 21$. Lastly, since $2 \cdot 7 + (-1) \cdot 13 = \gcd(7, 13) = 1$, it follows that $x \equiv 8 \bmod 13$. To sum up, solving the simultaneous equations above is equivalent to solving

$$\begin{array}{rcll} x & \equiv & 2 & \bmod 5 \\ x & \equiv & 14 & \bmod 21 \\ x & \equiv & 8 & \bmod 13 \end{array}$$

We make appeal to the Chinese Remainder Theorem twice. As $(-4) \cdot 5 + 1 \cdot 21 = \gcd(5, 21) = 1$,

$$x \equiv 5 \cdot (-4) \cdot 14 + 21 \cdot 1 \cdot 2 = -238 \equiv 77$$

mod 105 solves the first equation. We are reduced to solving

$$\begin{array}{rcll} x & \equiv & 77 & \bmod 105 \\ x & \equiv & 8 & \bmod 13 \end{array}$$

As $1 \cdot 105 + (-8) \cdot 13 = \gcd(105, 13) = 1$,

$$x \equiv 105 \cdot 1 \cdot 8 + (-8) \cdot 13 \cdot 77 = -7168 \equiv 1022$$

mod 1365.

**Q3** (a) Assume that 3083 and 3911 are prime numbers. Using properties of Legendre symbols, compute the Legendre symbol $\left(\frac{3083}{3911}\right)$. Justify your answer.

(b) Which of the following congruences are soluble? If soluble, find a positive solution less than 79; if insoluble, explain why.

- $x^2 \equiv 41 \bmod 79$.
- $41x^2 \equiv 43 \bmod 79$.

(c) Using Hensel's Lemma, find an integer $1 \leq z \leq 125$ satisfying $z^3 \equiv 2 \bmod 125$. Explain your answer.

**A3** (a) [Examples seen in lectures]

$$\begin{aligned}
& \left(\frac{3083}{3911}\right) \\
= & -\left(\frac{3911}{3083}\right) \\
= & -\left(\frac{828}{3083}\right) \\
= & -\left(\frac{207}{3083}\right) \\
= & -\left(\frac{3^2}{3083}\right)\left(\frac{23}{3083}\right) \\
= & -\left(\frac{23}{3083}\right) \\
= & \left(\frac{3083}{23}\right) \\
= & \left(\frac{1}{23}\right) \\
= & \ 1
\end{aligned}$$

(b) [Examples seen in lectures] The first congruence is insoluble. Indeed,

$$\left(\frac{41}{79}\right) = \left(\frac{79}{41}\right) = \left(\frac{38}{41}\right) = \left(\frac{2}{41}\right)\left(\frac{19}{41}\right) = \left(\frac{19}{41}\right) = \left(\frac{41}{19}\right) = \left(\frac{3}{19}\right) = -1.$$

The second congruence is soluble. Firstly, by the Euclid's algorithm, we find $27 \cdot 41 + (-14) \cdot 79 = 1$, hence

$$x^2 = 1 \cdot x^2 \equiv 27 \cdot 41 \equiv 27 \cdot 43 = 1161 \equiv 55$$

mod 79. Since $79 \equiv 3 \bmod 4$, we make appeal to Proposition 28 to solve the equation. Firstly, we check $\left(\frac{55}{79}\right) = 1$. Hence $55^{(79+1)/4} = 55^{20}$ is a solution mod 79. It remains to calculate the residue of $55^{20}$ when divided by 79. Note that $55^2 = 3025 \equiv 23 \bmod 79$, hence $55^4 \equiv 23^2 = 529 \equiv 55 \bmod 79$. Therefore,

$$55^{20} \equiv 55^5 \equiv 55^2 \equiv 23$$

mod 79. Hence $x = 23$ is the solution we are looking for.

(c) [Examples seen in lectures] Of course, trial-and-error is one way of doing this.

Let $P(x) = x^3 - 2$. We use Hensel's lemma to find a solution mod 125. Firstly, $z_1 = 3$ is the solution mod 5 to $P(x) \equiv 0 \bmod 5$. Since the derivative $P'(x)$ of $P(x)$ with respect to $x$ is $3x^2$, we have $P'(z_1) = 3 \cdot 3^2 = 27$, which is evidently not divisible by 5. The inverse $Q'(z_1)$ of $P'(z_1)$ mod 5 is 3 (as $3 \cdot 27 = 81 \equiv 1 \bmod 5$). It then follows from Hensel's lemma (Theorem 30) that

$$z_2 = z_1 - P(z_1)Q'(z_1) = 3 - 25 \cdot 3 = -72 \equiv 3$$

mod $5^2$ defines a solution to $P(x) \equiv 0$ mod 25. Since $P'(z_2) = P'(z_1) = 27$ is prime to 5 and the inverse $Q'(z_2)$ of $P'(z_2)$ mod 5 again is 3,

$$z_3 = z_2 - P(z_2)Q'(z_2) = -72 \equiv 53$$

mod 125. In conclusion, 53 does the job.

**Q4** (a) Compute the continued fraction expression of $\sqrt{11}$.

(b) Compute the convergents $\frac{s_0}{t_0}, \frac{s_1}{t_1}, \frac{s_2}{t_2}, \frac{s_3}{t_3}$ to $\sqrt{11}$.

(c) Find the smallest and the fourth smallest positive integer solutions to the equation

$$x^2 - 11y^2 = \pm 1.$$

(d) Compute the convergent $\frac{s_7}{t_7}$.

**A4** (a) [Examples seen in lectures] We run the algorithm:

$$\begin{array}{ccc}
\alpha = \lfloor \sqrt{11} \rfloor = 3 & \Rightarrow & \rho_1 = \dfrac{1}{\sqrt{11}-3} = \dfrac{\sqrt{11}+3}{2} \\
 & \swarrow & \\
\alpha_1 = \lfloor \dfrac{\sqrt{11}+3}{2} \rfloor = 3 & \Rightarrow & \rho_2 = \dfrac{1}{(\frac{\sqrt{11}+3}{2}) - 3} = \sqrt{11}+3 \\
 & \swarrow & \\
\alpha_2 = \lfloor \sqrt{11}+3 \rfloor = 6 & \Rightarrow & \rho_3 = \dfrac{1}{(\sqrt{11}+3)-6} = \dfrac{1}{\sqrt{11}-3} = \rho_1 \\
 & \swarrow & \\
\alpha_3 = \alpha_1 & \Rightarrow & \rho_4 = \rho_2 \\
 & \swarrow & \\
\alpha_4 = \alpha_2 & \Rightarrow & \rho_5 = \rho_3 = \rho_1 \\
 & \swarrow & \\
 & \vdots &
\end{array}$$

Hence $\sqrt{11} = [3; 3, 6, 3, 6, \dots] = [3; \overline{3, 6}]$.

(b) [Examples seen in lectures] Simply follows from the definition:

$$\begin{array}{rcl}
s_{-1} & = & 1 \\
s_0 & = & 3 \\
s_1 & = & \alpha_1 s_0 + s_{-1} = 3 \cdot 3 + 1 = 10 \\
s_2 & = & \alpha_2 s_1 + s_0 = 6 \cdot 10 + 3 = 63 \\
s_3 & = & \alpha_3 s_2 + s_1 = 3 \cdot 63 + 10 = 199.
\end{array}$$

On the other hand,

$$\begin{array}{rcl}
t_{-1} & = & 0 \\
t_0 & = & 1 \\
t_1 & = & \alpha_1 t_0 + t_{-1} = 3 \cdot 1 + 0 = 3 \\
t_2 & = & \alpha_2 t_1 + t_0 = 6 \cdot 3 + 1 = 19 \\
t_3 & = & \alpha_3 t_2 + t_1 = 3 \cdot 19 + 3 = 60.
\end{array}$$

(c) [Examples seen in lectures] It follows from Theorem 48 that the $(x, y) = (s_{2N-1}, t_{2N-1})$, $N = 1, 2, \dots,$ are the solutions for

$$x^2 - 11y^2 = (-1)^{2N} = 1.$$

The fundamental solution, therefore, is $(x, y) = (s_1, t_1) = (10, 3)$. It follows from Theorem 51 that the 4-th solution to the Pell equation is given by $(x, y) = (s, t)$ where

$$s + t\sqrt{11} = (10 + 3\sqrt{11})^4,$$

i.e. $(s, t) = (199^2 + 11 \cdot 60^2, 2 \cdot 199 \cdot 60) = (79201, 23880)$.

(d) [Examples seen in lectures] The pair $(s, t)$ in (c) is nothing other than $(s_{2\cdot4-1}, t_{2\cdot4-1}) = (s_7, t_7)$. It is certainly possible to do this by following the definitions.

**Q5** Use $67^2 \equiv -1 \bmod 449$ and Hermite's algorithm to find a pair of positive integers $s$ and $t$ such that

$$s^2 + t^2 = 449.$$

**A5** [Examples seen in lectures] Use Hermite's algorithm to solve the equation $x^2 + y^2 = 449$ in $x, y$. To this end, we find the continued fraction for $\frac{67}{449}$:

$$\frac{67}{449} = [0; 6, 1, 2, 2, 1, 6]$$

and the first few convergent are

$$\begin{aligned}
s_{-1} &= 1 \\
s_0 &= 0 \\
s_1 &= \alpha_1 s_0 + s_{-1} = 6 \cdot 0 + 1 = 1 \\
s_2 &= \alpha_2 s_1 + s_0 = 1 \cdot 1 + 0 = 1 \\
s_3 &= \alpha_3 s_2 + s_1 = 2 \cdot 1 + 1 = 3 \\
s_4 &= \alpha_4 s_3 + s_2 = 2 \cdot 3 + 1 = 7
\end{aligned}$$

while

$$\begin{aligned}
t_{-1} &= 0 \\
t_0 &= 1 \\
t_1 &= \alpha_1 t_0 + t_{-1} = 6 \cdot 1 + 0 = 6 \\
t_2 &= \alpha_2 t_1 + t_0 = 1 \cdot 6 + 1 = 7 \\
t_3 &= \alpha_3 t_2 + t_1 = 2 \cdot 7 + 6 = 20 \\
t_4 &= \alpha_4 t_3 + t_2 = 2 \cdot 20 + 7 = 47.
\end{aligned}$$

Since $t_3 = 20 < \sqrt{449} < 47 = t_4$, it follows from Hermite's algorithm that $(s, t) = (20, 449 \cdot 3 - 67 \cdot 20) = (20, 7)$.

**Q6** (a) What is the definition of a unit in a ring $R$?

(b) How many units are there in the following rings? If finitely many, list them all; if infinitely many, describe them all.

- $\mathbb{Z}[\sqrt{-1}]$,
- $\mathbb{Z}[\sqrt{11}]$.

**A6** (a) [Bookwork] An element $r$ in a ring $R$ is said to be a unit if there exists $s$ such that $rs = 1 = sr$.

(b) [Examples seen in lectures] The units in $\mathbb{Z}[\sqrt{-1}]$ are $\pm 1, \pm\sqrt{-1}$. On the other hand, we know from **Q4**, or otherwise that the fundamental solution to the Pell's equation $x^2 - 11y^2 = \pm 1$ is $(x, y) = (10, 3)$; and Proposition 66 therefore shows that $s_n + t_n\sqrt{11} = (10 + 3\sqrt{11})^n$ is a unit for any $n \geq 1$. These are the infinitely many units in $\mathbb{Z}[\sqrt{11}]$.

## Appendix: key assertions from lectures mentioned above

A1(c)

**Theorem 22** Let $p$ be a prime. For every number $d$ dividing $p-1$, let $S_d$ denote the elements in $\{1,\dots,p-1\}$ of order $d$ mod $p$. Then $|S_d| = \phi(d)$.

**Theorem 15** Let $n$ be a positive integer and $z$ be an integer such that $\gcd(z,n) = 1$. Then $z^{\phi(n)} \equiv 1 \bmod n$.

A3(b)

**Proposition 28** Let $p$ be a prime congruent to 3 mod 4. Suppose that $\left(\dfrac{a}{p}\right) = 1$. Then $z = a^{(p+1)/4}$ is a solution to the equation $x^2 \equiv a \bmod p$.

A3(c)

**Hensel's lemma (Theorem 30)** Let $p$ be a prime and $N \geq 1$ be an integer. Suppose that there exists $z \in \mathbb{Z}$ such that $P(z) \equiv 0 \bmod p^N$. If $P'(z)$ is not congruent to 0 mod $p$, then there exists an integer $r$ (congruent to $-\dfrac{P(z)}{p^N}Q'(z) \bmod p$, where $Q'(z)$ is the inverse of $P'(z) \bmod p$), unique mod $p$, such that $z + rp^N = z - P(z)Q'(z)$ defines a solution to the equation $P(x) \equiv 0 \bmod p^{N+1}$.

A4(c)

**Theorem 48** Suppose that $d \in \mathbb{N}$ is not a square. Suppose that $\sqrt{d} = [\alpha; \overline{\alpha_1,\dots,\alpha_l}]$. Let $\dfrac{s_n}{t_n}$ be the $n$-th convergent of the continued fraction of $\sqrt{d}$. Then $s_n^2 - dt_n^2 = \pm 1$ if and only if $n = Nl - 1$ for some $N = 1, 2, 3, \dots$. Moreover, $s_{Nl-1}^2 - dt_{Nl-1}^2 = (-1)^{Nl}$.

**Theorem 51** Let $(s,t) = (s_1,t_1)$ be the fundamental solution to the equation $x^2 - dy^2 = \pm 1$ and let $\epsilon = s^2 - dt^2 \in \{\pm 1\}$. For $n = 1, 2, \dots$, define $(s_n, t_n) \in \mathbb{N} \times \mathbb{N}$ by the equation $s_n + t_n\sqrt{d} = (s + t\sqrt{d})^n$. Then $s_n^2 - dt_n^2 = \epsilon^n$.

A6(b)

**Proposition 66** Suppose that $d$ is a square-free integer and $d \equiv 2, 3 \bmod 4$. An integer $\alpha = s + t\sqrt{d} \in \mathbb{Z}[\sqrt{d}]$ is a unit if and only if $|\alpha\overline{\alpha}| = 1$, or equivalently, $s^2 - dt^2 = \pm 1$, i.e., $(s,t)$ is a solution of Pell's equation $x^2 - dy^2 = \pm 1$.