MTH5130 2022-2023 January exam

Shu Sasaki

1st December 2022

A1 [A similar example seen]

Firstly, we observe that

$$35x + 55y + 77z = 35x + 11 \cdot (5y + 7z) = 1.$$

We solve $35X + 11Y = 1$ and $5y + 7z = Y$ [**5**].

By Euclid's algorithm or otherwise, we find that a solution to $35X + 11Y = 1$ is given for example by $(X, Y) = (-5, 16)$ [**3**].

On the other hand, to solve $5y + 7z = Y = 16$, we solve $5y + 7z = 1$ and multiply its solution (not necessarily unique, of course) by 16. It is easy to spot a solution to $5y + 7z = 1$; by Euclid's algorithm or otherwise, we see that $(y, z) = (3, -2)$ does the job,. It therefore follows that $(y, z) = (48, -32)$ is a solution to $5y + 7z = 16$ [**3**].

Combining all these together, $(x, y, z) = (-5, 48, -32)$ is a solution to $35x + 55y + 77z$ [**4**].

A2

(a) [A similar example seen] Yes, 7 is a primitive root mod 11 [**1**].

It follows from Fermat's Last Theorem that $7^{p-1} = 7^{10} \equiv 1 \bmod p$. By Lemma 19 that the order of 7 mod 11 is a divisor of 10, i.e. either $1, 2, 5$ or 10. Since

$$7^2 = 49 \equiv 5, \;\; 7^4 \equiv 5^2 = 25 \equiv 3, \;\; 7^5 \equiv 3 \cdot 7 = 21 \equiv 10,$$

the order of 7 mod 11 would have to 10 [**3**]. This means that 7 is a primitive root mod 11.

(b) [A similar example seen] Yes, 25 is a quadratic residue mod 11 [**1**].

This simply follows from observing that 25 is a square whether it is modulo 11 or not, or computing the Legendre symbol

$$\left(\frac{25}{11}\right) \overset{R1}{=} \left(\frac{5}{11}\right)^2 = 1$$

[**3**].

(c) [A similar example seen] No, 2 is not a square mod 9 [**1**].

Since 9 is not a prime number, it is not possible to use Legendre symbol to answer the question. We simply list all square numbers mod 9:

z	0	1	2	3	4	5	6	7	8
z^2	0	1	4	0	7	7	0	4	1

Since 2 is not in the list mod 9, it is not a square mod 9 [**3**].

(d) [A similar example seen] Yes [**1**]. Firstly, observe that $1013 \equiv 1 \bmod 3$ and $\left(\dfrac{17}{1013}\right) = -1$. It therefore follows from Proposition 29 ([**2**] for the reference) that $17^{\frac{1013-1}{4}} = 17^{253}$ is a solution to $x^2 \equiv -1 \bmod 1013$ [**1**].

Q3. (a) [A similar example seen] We firstly compute $r = [\overline{1;2}]$:

$$r = [1;2,r] = 1 + \cfrac{1}{2 + \cfrac{1}{r}} = 1 + \frac{r}{2r+1} = \frac{3r+1}{2r+1}$$

[**3**].

Hence r satisfies the quadratic equation

$$2r^2 - 2r - 1 = 0$$

[**1**].

By the quadratic formula, r is $\dfrac{1 \pm \sqrt{3}}{2}$, but by definition $r > 1$, hence $r = \dfrac{1+\sqrt{3}}{2}$ [**2**].

Substituting this into

$$[1;1,r] = 1 + \cfrac{1}{1 + \cfrac{1}{r}},$$

we obtain $1 + \dfrac{\sqrt{3}}{3}$ [**2**].

(b) [A similar example seen] Theorem 42 ([**2**]) asserts that any convergent r_n, with $n \geq 2$, defines a good (rational) approximation to a given number. For example, $r_2 = [2;1,2] = \dfrac{8}{3}$ is a good approximation to $[2;1,2,1,1,4,\ldots]$ [**4**].

(c)[partly seen] This is Theorem 45. Suppose that the given irrational number r has continued fraction $[\overline{\alpha;\alpha_1,\ldots,\alpha_{l-1}}]$ of cycle length $l \geq 1$ (to clarify, by $l = 1$, we mean $[\overline{\alpha}]$).

By assumption, we know that $r = [\alpha;\alpha_1,\ldots,\alpha_{l-1},r]$ for $l \geq 1$. It then follows from Lemma 40 (which can be proved by induction) [**6**] (reference to the lemma qualifies for the full 6 marks) that

$$r = \frac{rs_{l-1} + s_{l-2}}{rt_{l-1} + t_{l-2}}$$

where $\dfrac{s_n}{t_n}$ denote the n-th convergent to r. It follows from this that r satisfies

$$t_{l-1}r^2 + (t_{l-2} - s_{l-1})r - s_{l-2} = 0,$$

where, by definition, $t_{l-1} > 0$ [**3**]. Since the continued fraction is infinite, r is not rational and this forces r to be irrational (i.e. the discriminant is non-zero) [**1**].

A4.

(a) [A similar example seen] We run the algorithm to find $\sqrt{23} = [4;\overline{1,3,1,8}]$:

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

[**8**]

(b) [A similar example seen] From (a), the cycle length is $l = 4$, hence (s_3, t_3) is the fundamental solution [**1**].

As the convergents are:

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

we see that the fundamental solution is $(24, 5)$ [**3**].

(c) [A similar example seen] Since $7 = 2l - 1$ (with cycle length $l = 4$), it follows from Theorem 48 [**3**] that the 7-th convergent are given by

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

[**4**], i.e. $(1151, 240)$ [**1**].

A5 [A similar example seen]

Observe that since

$$x^2 + y^2 = 116 = 5^2 \cdot 29,$$

[**2**] it suffices to solve $x^2 + y^2 = 29$ (and multiply a solution by 5).

Step 1: Find z such that $z^2 \equiv -1 \bmod 29$. By trial and error, we find that $\left(\dfrac{2}{29}\right) = -1$ by $R3$ for example ($29 \equiv 5 \bmod 8$). Hence it follows from Proposition 29 that

$$z = 2^{\frac{29-1}{4}} = 2^7 = 128 \equiv 12$$

mod 29 satisfies $z^2 \equiv -1 \bmod 29$ [**2**].

Step 2:

$$\begin{array}{lcl}
\alpha = \lfloor \frac{12}{29} \rfloor = 0 & \Rightarrow & \rho_1 = \frac{1}{\frac{12}{29} - 0} = \frac{29}{12} \\
 & \swarrow & \\
\alpha_1 = \lfloor \frac{29}{12} \rfloor = 2 & \Rightarrow & \rho_2 = \frac{1}{\frac{29}{12} - 2} = \frac{12}{5} \\
 & \swarrow & \\
\alpha_2 = \lfloor \frac{12}{5} \rfloor = 2 & \Rightarrow & \rho_3 = \frac{1}{\frac{12}{5} - 2} = \frac{5}{2} \\
 & \swarrow & \\
\alpha_3 = \lfloor \frac{5}{2} \rfloor = 2 & \Rightarrow & \rho_4 = \frac{1}{\frac{5}{2} - 2} = 2 \\
 & \swarrow & \\
\alpha_4 = \lfloor 2 \rfloor = 2 & &
\end{array}$$

Hence $\dfrac{12}{29} = [0; 2, 2, 2, 2]$ [**2**].

It follows from this that the convergents to $\dfrac{z}{p} = \dfrac{12}{29}$ are:

$$r_1 = [0; 2] = \frac{1}{2},\ r_2 = [0; 2, 2] = \frac{2}{5},\ r_3 = [0; 2, 2, 2] = \frac{5}{12},\ r_4 = [0; 2, 2, 2, 2] = \frac{12}{29}$$

[**2**].

Step 3: Since $t_2 = 5 < \sqrt{29} < t_3 = 12$, we see that $(x, y) = (5, 29 \cdot 2 - 12 \cdot 5) = (5, -2)$ is a solution to $x^2 + y^2 = 29$. It therefore follows that a solution to $x^2 + y^2 = 725$ is $(25, -10)$ [**2**].

A6

(a) [A similar example seen] $\dfrac{26}{3}$ lies in $\mathbb{Q} - \mathbb{Z}$, hence it is not an algebraic integer. [**1**]. It is proved in lectures that the algebraic integers in $\mathbb{Q}$ are exactly $\mathbb{Z}$ [**2**] .

(b) [A similar example seen] π is a transcendental number [**2**], therefore not algebraic [**1**].

(c) [A similar example seen] If $d \equiv 1 \bmod 4$, the subring of algebraic integers in $\mathbb{Q}(\sqrt{d})$ is $\mathbb{Z}[\dfrac{1+\sqrt{d}}{2}]$ (Proposition 62) [**1**], but there is no pair of integers (a, b) that satisfies

$$1 + \frac{\sqrt{21}}{2} = a + b\left(\frac{1+\sqrt{21}}{2}\right)$$

(necessarily $b = 1$) [**1**]. Hence $1 + \dfrac{\sqrt{21}}{2}$ is not an algebraic integer [**1**].

(d) [A similar example seen] Yes [**1**], as it is a root of the monic polynomial x^2+x+1 [**2**]. Alternatively, one can make appeal to Proposition 62 that the ring of integers in $\mathbb{Q}(\sqrt{-3})$ is $\mathbb{Z}[\frac{1+\sqrt{-3}}{2}]$ (as $-3 \equiv 1 \bmod 4$) and

$$-\frac{1}{2}+\frac{\sqrt{-3}}{2}=(-1)+1\cdot\frac{1+\sqrt{-3}}{2}\in\mathbb{Z}[\frac{1+\sqrt{-3}}{2}].$$

(e). [not seen] If we let $\alpha = 1+\sqrt[3]{3}$, we see that $\alpha^3-3\alpha^2+3\alpha-4=0$ [**2**]. This is a monic polynomial with integer coefficients, hence α is an algebraic integer [**1**].