MTH6128 Number Theory

Solutions to Assignment 3

---

1 We will apply Euclid's algorithm, which finds the gcd and also, from the successive quotients, the continued fraction.

$$\begin{aligned}
145 &= 0\cdot 229+145,\\
229 &= 1\cdot 145+84,\\
145 &= 1\cdot 84+61,\\
84 &= 1\cdot 61+23,\\
61 &= 2\cdot 23+15,\\
23 &= 1\cdot 15+8,\\
15 &= 1\cdot 8+7,\\
8 &= 1\cdot 7+1,\\
7 &= 7\cdot 1.
\end{aligned}$$

(a) To get the continued fraction, we read off successive quotients:

$$\frac{145}{229}=[0;1,1,1,2,1,1,1,7].$$

(Remember that the first entry in the continued fraction is allowed to be zero or negative but all the others must be positive.)

(b) We have

$$\begin{aligned}
1 &= 8-7\\
&= 8-(15-8)=2\cdot 8-15\\
&= 2\cdot(23-15)-15=2\cdot 23-3\cdot 15\\
&= 2\cdot 23-3\cdot(61-2\cdot 23)=8\cdot 23-3\cdot 61\\
&= 8\cdot(84-61)-3\cdot 61=8\cdot 84-11\cdot 61\\
&= 8\cdot 84-11\cdot(145-84)=19\cdot 84-11\cdot 145\\
&= 19\cdot(229-145)-11\cdot 145=19\cdot 229-30\cdot 145,
\end{aligned}$$

so $x = -30$, $y = 19$ is a solution.

(c) Multiply the last equation by 5:

$$-150 \cdot 145 + 95 \cdot 229 = 5.$$

So $x = -150$, $y = 95$ is a solution.

(d) As in the Hint, suppose that (x_1, y_1) and (x_2, y_2) are solutions; so

$$145x_1 + 229y_1 = 145x_2 + 229y_2 = 5.$$

Then $145(x_1 - x_2) = 229(y_2 - y_1)$. Since the gcd of 145 and 229 is 1, we must have $145 \mid (y_2 - y_1)$, say, $y_2 - y_1 = 145u$. Then $x_1 - x_2 = 229u$. So we have $y_2 = y_1 + 145u$ and $x_2 = x_1 - 229u$. Putting in the solution we found for (x_1, y_1), we have the general solution

$$x = -150 - 229u, \quad y = 95 + 145u \qquad \text{for all } u \in \mathbb{Z}.$$

2 We should obviously do the last part first since it cuts down the amount of work we have to do!

Clearly (iv) $\Rightarrow$ (ii), (iv) $\Rightarrow$ (iii), (iii) $\Rightarrow$ (i), and (ii) $\Rightarrow$ (i).

If α satisfies a polynomial with rational coefficients, say

$$a_0\alpha^n + a_1\alpha^{n-1} + \cdots + a_n = 0,$$

where $a_0, a_1, \ldots, a_n$ are rationals and $a_0 \neq 0$, then

(a) we can divide the equation through by a_0 to get a monic polynomial with rational coefficients satisfied by α, and

(b) we can multiply the equation through by the least common multiple of the denominators of $a_0, a_1, \ldots, a_n$, to get a polynomial with integer coefficients satisfied by α.

So (i) $\Rightarrow$ (ii) and (i) $\Rightarrow$ (iii). We conclude that (i), (ii) and (iii) are all equivalent.

A number α is an *algebraic number* if it satisfies (i)–(iii), and is an *algebraic integer* if it satisfies all four conditions.

Also recall *Gauss's Lemma*: If α satisfies a monic polynomial over the integers then it satisfies an irreducible monic polynomial over the integers; that is, the minimal polynomial of α is a monic integer polynomial. So if the minimal polynomial of α is not a monic integer polynomial then the answer to (iv) is "no" for α.

(a) Let $\alpha = (1 + \sqrt{3})/2$. Then $(2\alpha - 1)^2 = 3$, so α satisfies $4x^2 - 4x - 2 = 0$, or $2x^2 - 2x - 1 = 0$. Thus α satisfies (i)–(iii). It does not satisfy (iv), since $2x^2 - 2x - 1$ is irreducible and so is the minimal polynomial of α.

(b) Let $\alpha = (1+\sqrt{5})/2$. Then $(2\alpha-1)^2 = 5$, so α satisfies $x^2 - x - 1 = 0$; thus α satisfies all four conditions.

(c) Let $\alpha = 1+\sqrt[3]{2}$. Then $(\alpha-1)^3 = 2$, so α satisfies $(x-1)^3 - 2 = 0$. So α satisfies all four conditions.

(d) Let $\alpha = 2\cos(2\pi/7) = \omega + \omega^{-1}$, where $\omega = \mathrm{e}^{2\pi\mathrm{i}/7}$. We have $\omega^7 = 1$, so

$$0 = \omega^7 - 1 = (\omega - 1)(\omega^6 + \omega^5 + \cdots + \omega + 1).$$

Now $\omega \neq 1$, so the second factor is zero. Dividing by ω^3,

$$\omega^3 + \omega^2 + \omega + 1 + \omega^{-1} + \omega^{-2} + \omega^{-3} = 0.$$

Now we have

$$\alpha = \omega + \omega^{-1}, \quad \alpha^2 = \omega^2 + 2 + \omega^{-2}, \quad \alpha^3 = \omega^3 + 3\omega + 3\omega^{-1} + \omega^{-3},$$

so the preceding equation becomes

$$(\alpha^3 - 3\alpha) + (\alpha^2 - 2) + \alpha + 1 = 0,$$

so that α satisfies $x^3 + x^2 - 2x - 1 = 0$. Thus α satisfies all four conditions.

(e) π is *transcendental*, that is, it satisfies no polynomial equation over the rationals. So it satisfies none of (i)–(iv).

Supplementary question Give an alternative solution to (d), using the formulae for $\cos(2\theta)$ and $\cos(3\theta)$ in terms of $\cos\theta$.

3 True. For suppose that $\lceil x \rceil = n$, so that $x = n - y$ where $0 \leq y < 1$. Then $-x = (-n) + y$, where $0 \leq y < 1$; so $\lfloor -x \rfloor = -n$.

4 Recall: we write the product of all the numbers in the square bracket; then we delete consecutive pairs in all possible ways, and take the product of the remaining terms; then we add up all these products.

The number of terms in the expression in Euler's theorem is independent of the entries in the brackets. If all the entries are 1, then each term will evaluate to 1, so the sum is just the number of terms in the expansion.

Let u_n be the value of $[1, 1, \ldots, 1]$ (n ones in the bracket). Then using the inductive definition of the square bracket function,

$$\begin{aligned} u_0 &= [] = 1, \\ u_1 &= [1] = 1, \\ u_n &= 1 \cdot u_{n-1} + u_{n-2} = u_{n-1} + u_{n-2} \text{ for } n \geq 2. \end{aligned}$$

So the numbers u_n are the *Fibonacci numbers* $1, 1, 2, 3, 5, 8, \ldots$