April Monthly Problem Set Solution

1. Since 43 is relatively prime to 100, we have that $31x + 73y \equiv 18 \pmod{100}$ is equivalent to $43(31x + 73y) \equiv 43 \cdot 18 \pmod{100}$, which is equivalent to $1333x + 3139y \equiv 774 \pmod{100}$, or—equivalently—$33x + 39y \equiv 74 \pmod{100}$.

2.

3.

4. The given condition gives us that $F_3 = 4$ and $F_4 = 7$. We claim that $F_{n+2} = F_{n+1} + F_n$ for all natural numbers n. Suppose that $F_{n+1} = F_n + F_{n-1}$ and $F_n = F_{n-1} + F_{n-2}$ for some n. We then have that

$$\begin{aligned} F_n F_{n+2} &= F_{n+1}^2 + (-1)^n \cdot 5 = (F_n + F_{n-1})^2 + (-1)^n \cdot 5 \\ &= F_n^2 + 2F_nF_{n-1} + F_{n-1}^2 + (-1)^n \cdot 5 \\ &= F_n^2 + 2F_nF_{n-1} + F_{n-2}F_n. \end{aligned}$$

We thus have that

$$F_{n+2} = F_n + 2F_{n-1} + F_{n-2} = (F_n + F_{n-1}) + (F_{n-1} + F_{n-2}) = F_{n+1} + F_n,$$

as claimed.

5.

6.

7. (a) The intermediate value theorem confirms that h has three real roots. By the rational root test, the only possible rational roots of $h(x)$ are ± 1, but they are not. Hence $\alpha,\ f(\alpha)$ and the third root of $h(x)$ are all irrational; and $h(x)$ is irreducible in $\mathbb{Q}[x]$.

   (b) Suppose for a contradiction that α is a root of a quadratic $g(x) \in \mathbb{Q}[x]$. Then we can write

$$h(x) = g(x) \cdot q(x) + r(x)$$

with $r(x)$ a linear member of $\mathbb{Q}[x]$. Then

$$0 = h(\alpha) = g(\alpha) \cdot q(\alpha) + r(\alpha) = r(\alpha)$$

and so $r(\alpha) = 0$. Since $r(x) \in \mathbb{Q}[x]$ and α is irrational, we must have that r is constantly 0. Thus $h(x) = g(x) \cdot q(x)$, a contradiction to the irreducibility of $h(x)$.

Alternative:

If α is the root of a quadratic, then we can write $\alpha = r + \sqrt{s}$ where $r,\ s \in \mathbb{Q}$ and s is not a perfect square. The other root of the quadratic, $r - \sqrt{s}$, will be denoted $\overline{\alpha}$.

We argue that both α and $\overline{\alpha}$ are roots of h. For this, note that since $(r+\sqrt{s})^3-3(r+\sqrt{s})+1 = 0$, we have (by separating rational and irrational parts) that $r^3+3rs-3r+1=0$ and $3r^2+s-3=0$. It follows that $(r-\sqrt{s})^3-3(r-\sqrt{s})+1=0$.[1]

This gives a contradiction, because it follows that the quadratic is a divisor of h.

(c) Suppose inductively that $h(f^n(\alpha))=0$. We show that $h(x)$ is a factor of $h(f^n(x))$. We can write

$$h(f^n(x)) = h(x)\cdot s(x) + g(x)$$

with $s(x),\ g(x)$ members of $\mathbb{Q}[x]$ with the degree of $g(x)$ less than or equal to 2. Then

$$0 = h(f^n(\alpha)) = h(\alpha)\cdot s(\alpha) + g(\alpha)$$

and so $g(\alpha)=0$. From the previous paragraph g then cannot be a quadratic, and clearly cannot be linear, and so we get that g is constantly 0.

Hence $h(f^n(x)) = h(x)\cdot s(x)$, and so by substitution $h(f^{n+1}(x)) = h(f(x))\cdot s(f(x))$. Thus $h(f^{n+1}(\alpha)) = h(f(\alpha))\cdot s(f(\alpha)) = 0$, completing the inductive step.

8.

[1] All we have done here is reinvent a little of the theory of conjugate surds. The conjugate surd of a number of the form $\alpha = r+\sqrt{s}$, where $r,\ s\in\mathbb{Q}$ and s is not a perfect square, is defined to be $\overline{\alpha} = r-\sqrt{s}$. Given any polynomial $p(x)\in\mathbb{Q}[x]$, if $p(\alpha)=0$, then $p(\overline{\alpha})=0$.

This is quite similar to the well known fact that the complex roots of a polynomial with real coefficients occur in complex conjugate pairs.