Puzzler 1. Consider running the Euclidean Algorithm on $a, b \in \mathbb{Z}, a > b > 0$ with $b \not| a$. Denote the remainders by r_1, r_2, $\cdots$, r_n, with $r_{n+1} = 0$. (Symbols as in textbook 2.22.) Show that $\forall k$, $r_{k+2} < r_k/2$. Derive an upper bound on the number of iterations n needed for the EA (or the EEA) to terminate.

Puzzler 2. Let $x = x_0 + \frac{b}{d}n$, $y = y_0 - \frac{a}{d}n$ $\forall n \in \mathbb{Z}$ be the complete solution to the LDE $ax + by = c$ (for which solutions exist and $d = \gcd(a, b)$). Show that there is no other LDE with complete solution 4 times the complete solution given above. (You should see that your proof stays valid when replacing 4 by any $k \in Z$, $k \geq 2$.)

Answer 1. The basic idea is obtained from
(1) the recursive relation $r_k = q_{k+2}\, r_{k+1} + r_{k+2}$ and
(2) the chain of inequality $0 < r_n < r_{n-1} < \cdots < r_2 < r_1 < b < a$.

Considering (1) and (2) together, we conclude $q_1, q_2, \cdots, q_{n+1} \geq 1$ (else some $q_k \leq 0$ and the chain of inequality (2) will be contradicted).

Using (1) again, we have $r_k = q_{k+2}\, r_{k+1} + r_{k+2} > q_{k+2}\, r_{k+2} + r_{k+2} = (q_{k+2} + 1)\, r_{k+2} \geq 2r_{k+2}$.
Dividing by 2 gives $r_k/2 > r_{k+2}$.

You may need to treat the boundary values for k more carefully (say, by defining $r_{-1} = a, r_0 = b$ etc but I leave you to give the proof a finishing touch.

Answer 2. We will prove by contradiction. (That is, we assume the statement false [negation of the statement true] and derive something known to be false. Thus the negation must be false and the initial statement true.)

Thus there's an LDE' $a'x + b'y = c'$ with complete solution $x = 4x_0 + \frac{4b}{d}n$, $y = 4y_0 - \frac{4a}{d}n$ $\forall n \in \mathbb{Z}$ — (1).

Choose $n = 0$ in (1) to get the particular solution $(4x_0, 4y_0)$ for LDE'. Then, according to the LDE Thm 2.31, and letting $d' = \gcd(a', b')$, the complete solution of LDE' has to be $x = 4x_0 + \frac{b'}{d'}n$, $y = 4y_0 - \frac{a'}{d'}n$ $\forall n \in \mathbb{Z}$ — (2).

Now we have 2 expressions (1) and (2) for the complete solution to LDE' and they have to be the same (in the sense they represent the same infinite set of solutions to LDE'). We consider the 2 particular solutions closest to $(4x_0, 4y_0)$. They are given by $n = \pm 1$ in each of (1) and (2).

(We know that the $n = 1$ point in (1) corresponds to one of the $n = \pm 1$ points in (2) but we cannot tell which one. Same vice versa.)

Matching these solutions, $\frac{4b}{d} = \pm \frac{b'}{d'}$, $\frac{4a}{d} = \pm \frac{a'}{d'}$. So, $4 | \frac{b'}{d'}$ and $4 | \frac{a'}{d'}$. This contradicts what Prop. 2.27 says, that $\gcd(\frac{a'}{d'}, \frac{b'}{d'}) = 1$.