

**Extra Solutions 4**

7. If  $x^i$  satisfies the given recurrence relation then  $x^i = 4x^{i-1} - x^{i-2}$  for all  $i \geq 2$ . In particular, putting  $i = 2$ , we see that  $x$  must satisfy the quadratic equation  $x^2 - 4x - 1$ . So  $a$  and  $b$  must be the roots of this, namely  $2 \pm \sqrt{3}$ . By multiplying through by  $x^{i-2}$  we see that if  $x^2 - 4x - 1 = 0$  then  $x^i = 4x^{i-1} - x^{i-2}$  holds for all  $i \geq 2$ ; so  $a^i$  and  $b^i$  are solutions of the recurrence relation, and it follows readily that  $s_i = \lambda a^i + \mu b^i$  is a solution for all constants  $\lambda$  and  $\mu$ . We want  $s_0 = 2$  and  $s_1 = 4$ , giving us the two equations  $\lambda + \mu = 2$  and  $\lambda a + \mu b = 4$ . Elimination  $\mu$  we obtain  $\lambda a + (2 - \lambda)b = 4$ , whence  $\lambda(a - b) = 4 - 2b = (a + b) - 2b = a - b$ . So  $\lambda = 1$ , and hence  $\mu = 1$  also.

Suppose now that we define integers  $r_i$  by  $r_0 = 4$  and  $r_{i+1} = r_i^2 - 2$  for all  $i \in \mathbb{N}$ . (The Lucas-Lehmer test can then be formulated as follows: if  $p$  is a prime then the Mersenne number  $m = 2^p - 1$  is prime if and only if  $r_{p-2} \equiv 0 \pmod{m}$ .) Let us use induction on  $i$  to show that  $r_i = s_{2^i}$  for all  $i \in \mathbb{N}$ .

To start the induction,  $s_{2^0} = s_1 = a^1 + b^1 = (2 + \sqrt{3}) + (2 - \sqrt{3}) = 4 = r_0$ , as required. Now assume that  $i > 0$  and that  $r_{i-1} = s_{2^{i-1}}$ . Then

$$r_i = r_{i-1}^2 - 2 = s_{2^{i-1}}^2 + 2 = (a^{2^{i-1}} + b^{2^{i-1}})^2 - 2. \quad (*)$$

Now  $(a^{2^{i-1}})^2 = a^{2^{i-1}} a^{2^{i-1}} = a^{2^{i-1}+2^{i-1}} = a^{2^i}$ , and  $(b^{2^{i-1}})^2 = b^{2^i}$  similarly. Moreover,  $ab = 1$ , and so  $a^{2^{i-1}} b^{2^{i-1}} = 1$ . So expanding the right hand side of (\*) we find that  $r_i = (a^{2^i} + 2 + b^{2^i}) - 2 = s_{2^i}$ , completing the induction.

For the last part, let  $r$  be prime and apply the binomial theorem to expand the right hand side of  $s_r = (2 + \sqrt{3})^r + (2 - \sqrt{3})^r$ . We find that

$$\begin{aligned} s_r &= \left( \sum_{i=0}^r \binom{r}{i} 2^{r-i} (\sqrt{3})^i \right) + \left( \sum_{i=0}^r \binom{r}{i} 2^{r-i} (-\sqrt{3})^i \right) \\ &= \sum_{i=0}^r \binom{r}{i} 2^{r-i} ((\sqrt{3})^i + (-\sqrt{3})^i) \\ &= \sum_{\substack{i=0 \\ i \text{ even}}}^r \binom{r}{i} 2^{r-i+1} (\sqrt{3})^i \end{aligned}$$

since  $(\sqrt{3})^i + (-\sqrt{3})^i$  is  $2(\sqrt{3})^i$  if  $i$  is even and zero if  $i$  is odd. If  $r = 2$  then  $s_r = s_2 = 4$ , which is indeed divisible by  $r$ . Otherwise  $r = 2h + 1$  is for some  $h \in \mathbb{Z}^+$ , and the above expression for  $s_r$  can be reformulated as  $s_r = \sum_{j=0}^h \binom{r}{2j} 2^{r-2j+1} 3^j$ . The term corresponding to  $j = 0$  is  $\binom{r}{0} 2^{r+1} 3^0 = 2 \times 2^r$ , which is congruent module  $r$  to  $2 \times 2$ , by Fermat's Little Theorem, so all that remains is to observe that the binomial coefficients  $\binom{r}{2j}$  are divisible by  $r$  whenever  $1 \leq j \leq h$  (given that  $r$  is prime). In fact, if  $1 \leq i \leq r - 1$  then  $i! \binom{r}{i} = r(r-1)(r-2) \cdots (r-i+1)$ , which is certainly a multiple of  $r$ , since  $i \geq 1$ . Since  $r$  is prime it follows that  $r$  must divide one of the factors of  $i! \binom{r}{i}$ . But the factors in  $i! = \prod_{\ell=1}^i \ell$  are not divisible by  $r$  since they are less than  $r$ ; so  $r \mid \binom{r}{i}$ , as required.