Roots of $x^2 - 6x + 1 = 0$

The USSR Olympiad Problem Book, by D. O. Shklarski, N . N. Chentzov, and I. M. Yaglom.

#178.* Prove that if x_1 and x_2 are roots of the equation $x^2 - 6x + 1 = 0$, then $x_1^n + x_2^n$ is, for any natural number n, an integer not divisible by 5.

Proof. Re-label the roots α and β. Then by repeatedly multiplying each equation by α:

$$\begin{aligned} \alpha^2 &= 6\alpha - 1 \\ \alpha^3 &= 6\alpha^2 - \alpha \\ \alpha^4 &= 6\alpha^3 - \alpha^2 \\ \alpha^5 &= 6\alpha^4 - \alpha^3 \\ &\vdots \end{aligned}$$

Therefore $\{u_n\} = \{\alpha^n\}$ satisfies a Fibonacci-like recurrence — namely:

$$\begin{aligned} u_0 &= 1 \\ u_1 &= \alpha \\ u_n &= 6u_{n-1} - u_{n-2}, \quad n \geq 2. \end{aligned} \tag{1}$$

$\{v_n\} = \{\beta^n\}$ satisfies the same recurrence and so does any linear combination $\{s \cdot \alpha^n + t \cdot \beta^n\}$. Putting $s = t = 1$ results in $w_n = \{\alpha^n + \beta^n\}$. Note:

$$\begin{aligned} x^2 - 6x + 1 &= 0 \\ (x - \alpha)(x - \beta) &= 0. \end{aligned}$$

implies that $\alpha + \beta = 6$, so:

$$\begin{aligned} w_0 &= \alpha^0 + \beta^0 = 2 \\ w_1 &= \alpha^1 + \beta^1 = 6. \end{aligned}$$

Therefore $\{w_n\} = \{2, 6, 34, 198, 1154, \ldots\}$. In particular, all the w_n are integers. Next is to show that none of them is a multiple of 5. w_2 below is calculated from the recursive formula, and so too for the rest of them:

$$\begin{aligned} w_{n+2} &= 6w_{n+1} - w_n \\ w_0 &\equiv 2 \pmod 5 \\ w_1 &\equiv 1 \pmod 5 \\ w_2 &\equiv 4 \pmod 5 \\ w_3 &\equiv 3 \pmod 5 \\ w_4 &\equiv 4 \pmod 5 \\ w_5 &\equiv 1 \pmod 5 \\ w_6 &\equiv 2 \pmod 5 \\ w_7 &\equiv 1 \pmod 5. \end{aligned}$$

Since $w_6 \equiv w_0 \pmod 5$ and $w_7 = w_1 \pmod 5$, the values repeat after that in cycles of 6, proving that none of them is a multiple of 5. **QED.**

This problem merits further discussion. The roots are:

$$\alpha = 3 + 2\sqrt{2} = 5.82843$$
$$\beta = 3 - 2\sqrt{2} = 0.17157.$$

β^n decreases monotonically to 0, and fairly rapidly, so α^n approaches the integer $\alpha^n + \beta^n$ from below, getting almost six times closer at every step:

n	α^n	α^n	β^n	β^n	$w_n = \alpha^n + \beta^n$
0	$1 + 0\sqrt{2}$	1	$1 - 0\sqrt{2}$	1	2
1	$3 + 2\sqrt{2}$	5.82843	$3 - 2\sqrt{2}$	0.17157	6
2	$17 + 12\sqrt{2}$	33.97056	$17 - 12\sqrt{2}$	0.02944	34
3	$99 + 70\sqrt{2}$	197.99495	$99 - 70\sqrt{2}$	0.00505	198
4	$577 + 408\sqrt{2}$	1153.99913	$577 - 408\sqrt{2}$	0.00087	1154
5	$3363 + 2378\sqrt{2}$	6725.99985	$3363 - 2378\sqrt{2}$	0.00015	6726

There are a number of striking things in this chart. One is that if $\alpha^n = a_n + b_n\sqrt{2}$, then $\beta^n = a_n - b_n\sqrt{2}$. Proceed as follows to prove this in general:

$$\alpha^n = a_n + b_n\sqrt{2}$$
$$\beta^n = c_n + d_n\sqrt{2}$$
$$\therefore \alpha^n + \beta^n = (a_n + c_n) + (b_n + d_n)\sqrt{2}$$
$$(\alpha^n + \beta^n) - (a_n + c_n) = (b_n + d_n)\sqrt{2}. \tag{2}$$

Considering that the left side of (2) is an integer, (2) is of the form $A = B\sqrt{2}$, where A and B are integers. Either both A and B are zero or neither of them is — the latter is precluded, because it would imply that $\sqrt{2}$ is rational. Therefore the coefficient on the right side of (2) is zero; that is, $d_n = -b_n$. Furthermore, $\{\alpha^n - \beta^n\}$ follows recurence (1) as a linear combination of two other sequences that do, namely $\{\alpha^n\}$ and $\{\beta^n\}$. Since $\alpha^0 - \beta^0 = 0$ and $\alpha^1 - \beta^1 = 4\sqrt{2}$, $\alpha^n - \beta^n = C_n\sqrt{2}$ for some integer C_n no matter the value of n. It follows that:

$$\alpha^n - \beta^n = (a_n - c_n) + 2b_n\sqrt{2}$$
$$\therefore C_n\sqrt{2} = (a_n - c_n) + 2b_n\sqrt{2}$$
$$a_n - c_n = (C_n - 2b_n)\sqrt{2}.$$

As before, this implies that $c_n = a_n$, so:

$$\alpha^n = a_n + b_n\sqrt{2}$$
$$\beta^n = a_n - b_n\sqrt{2}$$
$$\therefore 2a_n = \alpha^n + \beta^n$$
$$a_n = \frac{1}{2}\alpha^n + \frac{1}{2}\beta^n$$
$$2\sqrt{2}b_n = \alpha^n - \beta^n$$
$$b_n = \frac{1}{2\sqrt{2}}\alpha^n - \frac{1}{2\sqrt{2}}\beta^n. \tag{3}$$

Therefore $\{a_n\} = \{1, 3, 17, 99, 577, \ldots\}$ also follows recursion (1), as does $\{b_n\} = \{0, 2, 12, 70, 408, \ldots\}$. As for parity:

$$\begin{aligned} a_0 &= 1 \equiv 1 \pmod 2 \\ a_1 &= 3 \equiv 1 \pmod 2 \\ \therefore a_2 &\equiv (6a_1 - a_2) \pmod 2 \\ &\equiv (6 \cdot 1 - 1) \equiv 1 \pmod 2. \end{aligned}$$

By induction, all the rest of the a_n are odd. Similarly, all the b_n are even. The integer $\alpha^n + \beta^n$ is even, since it is twice a_n.

$a_n - b_n\sqrt{2} = \beta^n \to 0$, so:

$$\begin{aligned} a_n - b_n\sqrt{2} &= \epsilon_n \to 0 \\ \therefore \frac{a_n}{b_n} - \sqrt{2} &= \frac{\epsilon_n}{b_n} \to 0. \end{aligned}$$

considering that $b_n \to \infty$. Note that the convergence is from above since $\beta^n > 0$ and it is rapid, where $\delta_n = a_n/b_n - \sqrt{2}$ (note that $\sqrt{2} = 1.4142\ 13562$):

n	a_n	b_n	a_n/b_n	$\delta_n = a_n/b_n - \sqrt{2}$
1	3	2	1.5000 00000	0.0857 86438
2	17	12	1.4166 66667	0.0024 53104
3	99	70	1.4142 85714	0.0000 72152
4	577	408	1.4142 15686	0.0000 02124
5	3363	2378	1.4142 13625	0.0000 00063

δ_n is decreasing by over a factor of 30 at each step in this chart. The key to showing this generally is to note from (3) that b_n is very close to $\alpha^n/(2\sqrt{2})$, so:

$$\begin{aligned} \delta_n &= \frac{a_n}{b_n} - \sqrt{2} \\ &= \frac{\beta^n}{b_n} \\ &\approx \frac{\beta^n}{\alpha^n/(2\sqrt{2})} \\ &= \left(\frac{\beta}{\alpha}\right)^n \cdot 2\sqrt{2} \\ &= \left(\frac{3 - 2\sqrt{2}}{3 + 2\sqrt{2}}\right)^n \cdot 2\sqrt{2} \\ &= \left(17 - 12\sqrt{2}\right)^n \cdot 2\sqrt{2} \\ &= 0.02944^n \cdot 2\sqrt{2}. \end{aligned}$$

The second to last step results from rationalizing the fraction on the previous line. This shows that δ_n decreases by a factor of almost $34 \approx 1/0.02944$ at each step.

Finally, $\alpha \cdot \beta = 1$ implies that for every positive integer n:

$$\begin{aligned}
(\alpha \cdot \beta)^n &= 1 \\
\alpha^n \cdot \beta^n &= 1 \\
(a_n + b_n\sqrt{2}) \cdot (a_n - b_n\sqrt{2}) &= 1 \\
a_n^2 - 2b_n^2 &= 1.
\end{aligned}$$

That is, $(x, y) = (a_n, b_n)$ is a solution of the Diophantine equation $x^2 - 2y^2 = 1$ for every positive integer n: $17^2 - 2 \cdot 12^2 = 1,\ 99^2 - 2 \cdot 70^2 = 1$, and so on.

– Mike Bertrand
May 20, 2024