Math 437/537—Group Work #10

Tuesday, November 26, 2024

Definition: Let d, m_0, and q_0 be integers satisfying $q_0 \mid (d - m_0^2)$, and define $\xi_0 = (m_0 + \sqrt{d})/q_0$. The *Quadratic Irrational Process* produces sequences of integers as follows: for $j \geq 0$, define

$$a_j = \lfloor \xi_j \rfloor, \quad m_{j+1} = a_j q_j - m_j, \quad q_{j+1} = \frac{d - m_{j+1}^2}{q_j}, \quad \xi_{j+1} = \frac{m_{j+1} + \sqrt{d}}{q_{j+1}}.$$

1.

(a) *Carry out the Quadratic Irrational Process for* $d = 41$, $m_0 = 0$, $q_0 = 1$, *through* $j = 5$. *Have we seen this sequence of* a_j *before?*

(b) *Given the above sequence of* a_j, *calculate* h_j *and* k_j *through* $j = 5$. *For each* $0 \leq j \leq 5$, *calculate* $h_j^2 - 41k_j^2$. *Spot the pattern (you don't have to prove it).*

(c) *Expand out* $(h_2 + k_2\sqrt{41})^2$ *as one integer plus another integer times* $\sqrt{41}$. *Do those integers look familiar?*

(d) *Given integers* x, y, d, *and* N *such that* $x^2 - dy^2 = N$, *define the integers* x_ℓ *and* y_ℓ *by the identity* $x_\ell + y_\ell\sqrt{d} = (x + y\sqrt{d})^\ell$. *Prove that* $x_\ell^2 - dy_\ell^2 = N^\ell$. *Hint: consider* $(x + y\sqrt{d})(x - y\sqrt{d})$.

(e) *Find integers* $x, y > 32$ *such that* $x^2 - 41y^2 = -1$. *Then find integers* $x, y > 2049$ *such that* $x^2 - 41y^2 = 1$. *Using calculators is a good idea.*

(a) We record our calculations (all of which use $d = 41$) in the following table:

j	m_j	q_j	ξ_j	a_j
0	0	1	$\sqrt{41}$	6
1	6	5	$(6+\sqrt{41})/5$	2
2	4	5	$(4+\sqrt{41})/5$	2
3	6	1	$6+\sqrt{41}$	12
4	6	5	$(6+\sqrt{41})/5$	2
5	4	5	$(4+\sqrt{41})/5$	2

Indeed, this sequence of a_j gives the continued fraction for $\sqrt{41}$ that we saw in today's class, namely the periodic continued fraction $\langle 6; \overline{2, 2, 12} \rangle$. (Note that the table above is also periodic, since the $j = 1$ and $j = 4$ rows are identical.)

(b) This sort of calculation is familiar to us already:

j	a_j	h_j	k_j	$h_j^2 - 41k_j^2$
-2		0	1	
-1		1	0	1
0	6	6	1	-5
1	2	13	2	5
2	2	32	5	-1
3	12	397	62	5
4	2	826	129	-5
5	2	2049	320	1

By comparing the two tables above, we observe that $h_{j-1}^2 - 41k_{j-1}^2 = (-1)^j q_j$ for $j \geq 0$.

(c) We have

$$(h_2 + k_2\sqrt{41})^2 = (32 + 5\sqrt{41})^2 = 32^2 + 2 \cdot 32 \cdot 5\sqrt{41} + 5^2 \cdot 41 = 2049 + 320\sqrt{41},$$

which we notice is the same as $h_5 + k_5\sqrt{41}$.

(d) The key fact we need is that x_ℓ and y_ℓ also satisfy $x_\ell - y_\ell\sqrt{41} = (x - y\sqrt{41})^\ell$: if we knew that, then

$$\begin{aligned} x_\ell^2 - 41y_\ell^2 = (x_\ell + y_\ell\sqrt{41})(x_\ell - y_\ell\sqrt{41}) &= (x + y\sqrt{41})^\ell(x - y\sqrt{41})^\ell \\ &= ((x + y\sqrt{41})(x - y\sqrt{41}))^\ell = (x^2 + dy^2)^\ell = N^\ell. \end{aligned}$$

There are (at least) three ways to prove that $x_\ell - y_\ell\sqrt{41} = (x - y\sqrt{41})^\ell$:

Proof 1: We have

$$\begin{aligned} x_\ell + y_\ell\sqrt{41} &= (x + y\sqrt{41})^\ell \\ &= \sum_{i=0}^{\ell} \binom{\ell}{i} (y\sqrt{41})^i x^{\ell-i} \\ &= \sum_{\substack{0 \le i \le \ell \\ i \text{ even}}} \binom{\ell}{i} (y\sqrt{41})^i x^{\ell-i} + \sum_{\substack{0 \le i \le \ell \\ i \text{ even}}} \binom{\ell}{i} (y\sqrt{41})^i x^{\ell-i} \\ &= \sum_{\substack{0 \le i \le \ell \\ i \text{ even}}} \binom{\ell}{i} y^i 41^{i/2} x^{\ell-i} + \sqrt{41} \sum_{\substack{0 \le i \le \ell \\ i \text{ even}}} \binom{\ell}{i} y^i 41^{(\ell-1)/2} x^{\ell-i}; \end{aligned}$$

since both sums are manifestly integers, the first sum equals x_ℓ and the second equals y_ℓ (otherwise $\sqrt{41}$ would be rational). On the other hand,

$$\begin{aligned} (x - y\sqrt{41})^\ell &= \sum_{i=0}^{\ell} \binom{\ell}{i} (-y\sqrt{41})^i x^{\ell-i} \\ &= \sum_{\substack{0 \le i \le \ell \\ i \text{ even}}} \binom{\ell}{i} (-y\sqrt{41})^i x^{\ell-i} + \sum_{\substack{0 \le i \le \ell \\ i \text{ even}}} \binom{\ell}{i} (-y\sqrt{41})^i x^{\ell-i} \\ &= \sum_{\substack{0 \le i \le \ell \\ i \text{ even}}} \binom{\ell}{i} y^i 41^{i/2} x^{\ell-i} - \sqrt{41} \sum_{\substack{0 \le i \le \ell \\ i \text{ even}}} \binom{\ell}{i} y^i 41^{(\ell-1)/2} x^{\ell-i} \\ &= x_\ell - y_\ell\sqrt{41}, \end{aligned}$$

since the two resulting sums are exactly the same as before.

Proof 2: We proceed by induction on ℓ; the base case is trivial because $x_1 = x$ and $y_1 = y$. Note that

$$\begin{aligned} x_{\ell+1} + y_{\ell+1}\sqrt{41} = (x + y\sqrt{41})^{\ell+1} = (x + y\sqrt{41})^\ell(x - y\sqrt{41}) &= (x_\ell + y_\ell\sqrt{41})(x + y\sqrt{41}) \\ &= (x_\ell x + 41y_\ell y) + (x_\ell y + y_\ell x)\sqrt{41}, \end{aligned}$$

and so $x_{\ell+1} = x_\ell x + 41 y_\ell y$ and $y_{\ell+1} = x_\ell y + y_\ell x$. On the other hand, under the induction hypothesis that $x_\ell - y_\ell\sqrt{41} = (x - y\sqrt{41})^\ell$, we have

$$(x - y\sqrt{41})^{\ell+1} = (x - y\sqrt{41})^\ell (x - y\sqrt{41}) = (x_\ell - y_\ell\sqrt{41})(x - y\sqrt{41})$$
$$= (x_\ell x + 41 y_\ell y) - (x_\ell y + y_\ell x)\sqrt{41} = x_{\ell+1} - y_{\ell+1}\sqrt{41}$$

as desired.

Proof 3: Let $f(t) \in \mathbb{Q}[t]$ be irreducible, and let α and β be any two roots of f. Then Galois theory tells us that there exists a field isomorphism from $\mathbb{Q}(\alpha)$ to $\mathbb{Q}(\beta)$ that sends α to β. In particular, if $g(t) \in \mathbb{Q}[t]$ is any polynomial, so that $g(\alpha) = \sum_{i=0}^{I} r_i \alpha^i$ for some rational numbers r_i, then $g(\beta) = \sum_{i=0}^{I} r_i \beta^i$ for the same rational numbers. Our desired identity is the special case where $f(t) = t^2 - 41$, $\alpha = \sqrt{41}$, $\beta = -\sqrt{41}$, and $g(t) = (x + yt)^\ell$.

(e) We define $x = 32$ and $y = 5$, so that $x^2 - 41y^2 = -1$. By part (d), if we define x_ℓ and y_ℓ by $x_\ell + y_\ell\sqrt{41} = (x + y\sqrt{41})^\ell$, we then have $x_\ell^2 - 41 y_\ell^2 = (-1)^\ell$. Indeed, we saw the case $\ell = 2$ in part (c). Taking $\ell = 3$ and $\ell = 4$:

$$\begin{aligned}(32 + 5\sqrt{41})^3 &= 32^3 + 3 \cdot 32^2 \cdot 5\sqrt{41} + 3 \cdot 32 \cdot (5\sqrt{41})^2 + (5\sqrt{41})^3 \\ &= 32768 + 15360\sqrt{41} + 98400 + 5125\sqrt{41} \\ &= 131168 + 20485\sqrt{41} \\ (32 + 5\sqrt{41})^4 &= 32^4 + 4 \cdot 32^3 \cdot 5\sqrt{41} + 6 \cdot 32^2 \cdot (5\sqrt{41})^2 + 4 \cdot 32 \cdot (5\sqrt{41})^3 + (5\sqrt{41})^4 \\ &= 1050625 + 656000\sqrt{41} + 6297600 + 655360\sqrt{41} + 1048576 \\ &= 8396801 + 1311360\sqrt{41};\end{aligned}$$

and indeed $131168^2 - 41 \cdot 20485^2 = -1$ and $8396801^2 - 41 \cdot 1311360^2 = 1$.

(continued on next page)

2.

(a) *Carry out the Quadratic Irrational Process for* $d = 28$, $m_0 = 0$, $q_0 = 1$, *through* $j = 7$.

(b) *Given the above sequence of* a_j, *calculate* h_j *and* k_j *through* $j = 3$. *For each* $0 \le j \le 3$, *calculate* $h_j^2 - 28k_j^2$.

(c) *Can you quickly calculate* h_7, k_7, *and* $h_7^2 - 28k_7^2$?

(a) We record our calculations (all of which use $d = 28$) in the following table:

j	m_j	q_j	ξ_j	a_j
0	0	1	$\sqrt{28}$	5
1	5	3	$(5+\sqrt{28})/3$	3
2	4	4	$(4+\sqrt{28})/4$	2
3	4	3	$(4+\sqrt{28})/3$	3
4	5	1	$5+\sqrt{28}$	10
5	5	3	$(5+\sqrt{28})/3$	3
6	4	4	$(4+\sqrt{28})/4$	2
7	4	3	$(4+\sqrt{28})/3$	3

Indeed, this table is also periodic, since the $j = 1$ and $j = 5$ rows are identical; it seems that $\sqrt{28}$ has the periodic continued fraction $\langle 5; \overline{3, 2, 3, 10} \rangle$.

(b) Again this is a familiar calculation:

j	a_j	h_j	k_j	$h_j^2 - 28k_j^2$
-2		0	1	
-1		1	0	1
0	5	5	1	-3
1	3	16	3	4
2	2	37	7	-3
3	3	127	24	1

(c) It should seem, from our observations in problem #1, that we should have the identity $h_7 + k_7\sqrt{28} = (h_3 + k_3\sqrt{28})^2$; so we calculate

$$(h_3 + k_3\sqrt{28})^2 = (127 + 24\sqrt{28})^2 = 127^2 + 2 \cdot 127 \cdot 24\sqrt{28} + 24^2 \cdot 28 = 32257 + 6096\sqrt{28},$$

so that $h_7 = 32257$ and $k_7 = 6096$. (And indeed, we verify that $32257^2 - 28 \cdot 6096^2 = 1$.)