**Example 4.** Note that the group $G_{pc}$ in Example 3 is closed under the operation of transposition of matrices. It follows that this same group must also be the group of matrices which are perfectly-conditioned with respect to the maximum absolute column sum norm. ($\|A\|_c = \|A^t\|_r$, where $\|\ \|_c$ and $\|\ \|_r$ denote the maximum absolute column and row sum norms respectively.)

**References**

[1] Gene H. Golub and Charles F. Van Loan, Matrix Computations (second edition). Johns Hopkins University Press: Baltimore and London, 1989.

[2] Nathan Jacobson, Basic Algebra I. W. H. Freeman and Co.: San Francisco, 1974.

[3] D. W. Lewis, Matrix Theory. World Scientific Publishing: Singapore-New Jersey-London-Hong Kong, 1991.

D. W. Lewis,
Department of Mathematics,
University College,
Belfield,
Dublin 4.

## AN ITERATION RELATED TO EISENSTEIN'S CRITERION

Eugene Gath and Thomas J. Laffey

The following question appeared in the 1994 Irish Mathematical Olympiad, the competition used to select the team to represent Ireland in the International Olympiad:
*Let $a$, $b$ and $c$ be real numbers satisfying the equations:*

$$b = a(4-a)$$
$$c = b(4-b)$$
$$a = c(4-c).$$

*Find all possible values of $a+b+c$.*

A direct approach to this problem is to write $c$ in terms of $a$, and then obtain an octic polynomial in $a$:

$$f(a) \equiv -a(4-a)(2-a)^2((2-a)^2-2)+a = 0.$$

The octic factorizes over the integers in the form

$$f(a) = a(a-3)(a^3-6a^2+9a-3)(a^3-7a^2+14a-7).$$

Observe that the factors $a^3-6a^2+9a-3$ and $a^3-7a^2+14a-7$ satisfy Eisenstein's irreducibility criterion for the primes 3 and 7, respectively. This, in our experience, was one of the rare occasions when polynomials satisfying the criterion arose in an uncontrived way, and we decided to investigate why they occurred here.

Put $g(x) \equiv x(4-x)$ and let $g^{(r)}(x)$ be the $r$th iterate $g(g(\ldots g(x)\ldots))$. Consider the polynomial $h_r(x) = x - g^{(r)}(x)$.

The octic $f(a)$ above is just $h_3(a)$. Observe that if we put $x = 4\sin^2\theta$ (where for definiteness we take $0 \le \theta \le \frac{\pi}{2}$), then $g(x) = 4\sin^2 2\theta$, and thus

$$\begin{aligned} h_r(x) &= 4\sin^2 2^r\theta - 4\sin^2\theta = 2(\cos 2\theta - \cos 2^{r+1}\theta) \\ &= 4\sin(2^r-1)\theta\sin(2^r+1)\theta. \end{aligned}$$

So, if $(2^r \pm 1)\theta = l\pi$ for some positive integer $l$, we get solutions of the equation $h_r(x) = 0$. The two irreducible cubics dividing $f(x)$ are the irreducible polynomials satisfied by $4\sin^2\frac{\pi}{9}$ and $4\sin^2\frac{\pi}{7}$, respectively. The other factors $x$ and $x-3$ are factors of $h_r(x)$ for all $r$, corresponding to the choices $\theta = 0$ and $\theta = \frac{\pi}{3}$, $l = \frac{1}{3}(2^r - (-1)^r)$, respectively.

In general, for each $k \ge 1$, $2^k+1$ and $2^k-1$ are relatively prime and for each divisor $d$ of $(2^k-1)(2^k+1)$, with $1 < d < (2^k-1)(2^k+1)$, $4\sin^2\frac{\pi}{d}$ satisfies a monic irreducible polynomial $\psi_d(x)$ of degree $\varphi(d)/2$, where $\varphi$ is Euler's function. Also, $\psi_d(x)$ must divide $h_k(x)$ and $x = 0$ is a solution, corresponding to $d = 1$. Thus

$$x \prod_{1<d|2^k-1} \psi_d(x) \prod_{1<d|2^k+1} \psi_d(x)$$

divides $h_k(x)$. The total degree of these polynomials is

$$\frac{1}{2}\left(\sum_{d|2^k-1}\varphi(d) + \sum_{d|2^k+1}\varphi(d)\right) = 2^k = \text{degree } h_k(x).$$

To calculate the irreducible polynomial satisfied by $4\sin^2\frac{\pi}{n}$, $n$ odd, we use the following identity:

$$\frac{\sin n\phi}{\sin\phi} = \sum_{s=0}^{\frac{n-1}{2}} \frac{(-1)^s n(n+2s-1)(n+2s-3)\cdots(n-2s+1)}{(2s+1)!}\sin^{2s}\phi.$$

This may be written more compactly as

$$\frac{\sin n\phi}{\sin\phi} = \sum_{s=0}^{\frac{n-1}{2}}(-1)^s\frac{n}{2s+1}\binom{\frac{n-1}{2}+s}{2s}(4\sin^2\phi)^s.$$



For example, when $n = 5$,

$$\frac{\sin 5\phi}{\sin\phi} = 5 - 5(4\sin^2\phi) + (4\sin^2\phi)^2$$

and when $n = 7$,

$$\frac{\sin 7\phi}{\sin\phi} = 7 - 14(4\sin^2\phi) + 7(4\sin^2\phi)^2 - (4\sin^2\phi)^3.$$

Putting $z \equiv 4\sin^2\phi$, then if $\sin\phi \ne 0$ and $\sin n\phi = 0$, we get a monic polynomial $f_n(x)$ with integer coefficients and degree $\frac{n-1}{2}$ with $f_n(z) = 0$. The constant term of $f_n(z)$ is $\pm n$. This is obtained explicitly from the trigonometric identity above, using binomial identities, giving

$$f_n(x) = \sum_{i=0}^{\frac{n-1}{2}}(-1)^i\frac{n}{n-i}\binom{n-i}{i}x^{\frac{n-1}{2}-i}.$$

Suppose now that $n = p^k$, where $p$ is an odd prime and $k \ge 1$. The expression for $f_n(x)$ above shows that all of the coefficients are divisible by $p$ except the coefficient of $x^{\frac{n-1}{2}}$ and the constant term is $\pm p^k$. But the irreducible polynomials satisfied by $4\sin^2\frac{\pi}{p}$, $4\sin^2\frac{\pi}{p^2}, \ldots, 4\sin^2\frac{\pi}{p^k}$ must all divide $f_n(x)$ and the sum of the degrees of these polynomials is $\frac{n-1}{2}$. Thus

$$f_n(x) = \psi_p(x)\psi_{p^2}(x)\cdots\psi_{p^k}(x).$$

We now show by induction on $k$ that $\psi_{p^k}$ satisfies Eisenstein's criterion for the prime $p$. Since $f_p(x) = \psi_p(x)$, this is clear when $k = 1$. The equation

$$f_{p^k}(x) = f_{p^{k-1}}(x)\psi_{p^k}(x)$$

yields

$$x^{\frac{(p^k-1)}{2}} \equiv x^{\frac{(p^{k-1}-1)}{2}}\psi_{p^k}(x) \bmod p,$$

so all coefficients of $\psi_{p^k}$ except its leading coefficient are divisible by $p$. Furthermore, the constant term of $f_{p^k}(x)$ is $\pm p^k$, and that of $f_{p^{k-1}}(x)$ is $\pm p^{k-1}$, so the constant term of $\psi_{p^k}(x)$ is $\pm p$. Hence $\psi_{p^k}(x)$ satisfies Eisenstein's criterion for $p$. This explains our initial observations concerning the polynomials

$$\psi_7(x) = x^3 - 7x^2 + 14x - 7$$

and

$$\psi_9(x) = x^3 - 6x^2 + 9x - 3.$$

Let $\omega$ be a primitive $p^k$th root of unity (for definiteness, we can take $\omega = \exp(\frac{2\pi i}{p^k})$) and let $K = \mathbf{Q}(\omega)$ be the corresponding cyclotomic field. Let $L = \mathbf{Q}(\omega+\omega^{-1})$ be the maximal real subfield of $K$ and let $A$ be the ring of algebraic integers in $L$. One can show that $\mathbf{Z}[4\sin^2(\frac{\pi}{p^k})]$ has finite index $p^c$ in $A$ for some integer $c \geq 0$. But now the fact that the irreducible polynomial $\psi_{p^k}(x)$ satisfied by $4\sin^2(\frac{\pi}{p^k})$ is of Eisenstein type enables us to apply Lemma 2.3 of [1, p.61] to conclude that $c = 0$. So

$$A = \mathbf{Z}[4\sin^2(\frac{\pi}{p^k})] = \mathbf{Z}[2\cos(\frac{2\pi}{p^k})] = \mathbf{Z}[\omega + \omega^{-1}].$$

Finally, we briefly consider the orbit length of the iteration of the map $a \to a(4-a)$, beginning with $a = 4\sin^2(\frac{\pi}{n})$, where $n$ is an odd integer. We obtain successively $4\sin^2(\frac{\pi}{n})$, $4\sin^2(\frac{2\pi}{n})$, $4\sin^2(\frac{2^2\pi}{n})$, ... and the period is $r$, where $r$ is the least positive integer such that

$$\frac{2^{r+1}\pi}{n} \pm \frac{2\pi}{n}$$

is an integral multiple of $2\pi$. (For example, when $n = 17$, $r = 4$ and when $n = 19$, $r = 9$.) Note that $r$ is the least positive integer such that $2^r \equiv \pm 1 \bmod n$. So, if the equation $2^t \equiv -1 \bmod n$ is solvable, then $r$ is half the order of 2 mod $n$ while, if it is not solvable, $r$ is the order of 2 mod $n$. If $n = p^k$, where $p$ is an odd prime and $k$ is a positive integer, the equation $2^t \equiv -1 \bmod n$ is solvable if and only if the order of 2 mod $n$ is even, so in particular,



$2^t \equiv -1 \bmod n$ is solvable if 2 is not a quadratic residue modulo $p$, that is if $p \equiv \pm 3 \bmod 8$.

**Reference**

[1] W. Narkiewicz, Elementary and Analytic Theory of Algebraic Numbers. Scientific Publ. Warsaw: 1991.

Eugene Gath,
Department of Mathematics and Statistics,
University of Limerick,
Limerick.

T. J. Laffey,
Department of Mathematics,
University College,
Belfield,
Dublin 4.