Let the join of C to the center of circle $\mathscr{C}$ intersect this circle in P and Q. Then C is a fixed point on the fixed segment PQ, or PQ produced, where P moves on OP and Q moves on the perpendicular line OQ. Hence C describes an ellipse with principal axes OP and OQ. If triangle ABC is such that C lies either on OP or OQ, then C moves on that line.

Reference

1. Dan Pedoe, Geometry and the Liberal Arts, Penguin Books, London, in the press.

AN EXPLICIT FORMULA FOR THE kth PRIME NUMBER

STEPHEN REGIMBAL, Billings, Montana

This paper will develop an explicit formula for the kth prime, where k is any positive integer. The formula will be elementary, finite, and dependent only upon the choice of k.

First consider the function

$$g(n)=\sum_{i=1}^{n-1}\left[\frac{\left[\frac{n}{i}\right]}{\frac{n}{i}}\right]$$

where $[x]$ in all cases denotes the greatest integer $\leqq x$, and $n \geqq 2$. Now the terms in this finite sum are equal either to 0 or to 1 since for any $x>0$,

$$0<\frac{[x]}{x}\leqq 1 \Rightarrow \left[\frac{[x]}{x}\right]=0 \quad \text{or} \quad 1.$$

Therefore, $g(n)=1$ if and only if there exists exactly one $i \in \{1,2,3,\cdots,n-1\}$ such that

$$\left[\frac{\left[\frac{n}{i}\right]}{\frac{n}{i}}\right]=1 \Leftrightarrow \left[\frac{n}{i}\right]=\frac{n}{i} \Leftrightarrow i \mid n;$$

but since $i=1$ divides n for all positive integers n, then $g(n)=1$ if and only if $i=1$ is the only value of $i \in \{1,2,3,\cdots,n-1\}$ such that i divides n. But this means that n is prime. Thus, $g(n)=1$ if and only if n is prime. Now if n is composite, then there exists some $i \in \{2,3,4,\cdots,n-1\}$ such that i divides n, and this implies that $g(n)>1$. Therefore,

$$g(n)\begin{cases} =1, & n \text{ prime} \\ >1, & n, \text{ composite.}\end{cases}$$

Now let $f(n)=[1/(g(n))]$, then it is clear that for $n \geqq 2$,

$$f(n)=\begin{cases}1, & n \text{ prime}\\ 0, & n \text{ composite.}\end{cases}$$

Note that $f(n)$ is the characteristic function of the set of primes.

Consider for $m \geqq 2$,

$$\pi(m)=\sum_{n=2}^{m} f(n);$$

since $f(n)$ is the characteristic function of the set of primes, then $\pi(m)$ is the number of primes less than or equal to m, and thus for $m \geqq 2$,

$$f(m)\pi(m)=\begin{cases}\text{number of primes } \leqq m, \ m \text{ prime,}\\ 0, \ m \text{ composite.}\end{cases}$$

Let k be any positive integer, and the following equality holds:

$$\left[\frac{1}{1+|k-f(m)\pi(m)|}\right] m=\begin{cases}m, \ m \text{ the } k\text{th prime,}\\ 0, \text{ otherwise.}\end{cases}$$

This is true since the above function is equal to m if and only if $k=f(m)\pi(m)$, which implies that m is prime and there are k primes less than or equal to m; but this means that m is the kth prime. If m is not the kth prime of if m is composite, then $|k-f(m)\pi(m)|>0$, and the above function equals 0.

Now by Bertrand's postulate as proved by Hardy and Wright **[1]**, there exists at least one prime p such that for all positive integers n, $n<p \leqq 2n$. Therefore, it follows that if p_k denotes the kth prime, then for all positive integers k, $p_k<p_{k+1} \leqq 2p_k$ and this supplies the induction step to prove that for all positive integers k, $2^k \geqq p_k$. Now with this result it follows that for all $k \geqq 1$, the kth prime is given by the formula

$$p_k=\sum_{m=2}^{2^k}\left[\frac{1}{1+|k-f(m)\pi(m)|}\right] m$$

since summing to 2^k guarantees that we have summed past the kth prime. Now rewriting in terms of the original expressions, we have:

$$p_k=\sum_{m=2}^{2^k}\left[\frac{1}{1+\left|k-\left[\dfrac{1}{\sum_{i=1}^{m-1}\left[\dfrac{\left[\frac{m}{i}\right]}{\frac{m}{i}}\right]}\right]\sum_{n=2}^{m}\left[\dfrac{1}{\sum_{i=1}^{n-1}\left[\dfrac{\left[\frac{n}{i}\right]}{\frac{n}{i}}\right]}\right]\right|}\right] m.$$

Note that this method can be generalized to yield an expression for the kth smallest element of an arbitrary infinite subset A of the positive integers. The finiteness of this extended formula will depend not only upon the possibility of writing a finite expression for the characteristic function of the set A, but also upon the existence of a finitely expressible function $h(k)$ such that $h(k) \geqq$ the kth smallest element of A for all $k \geqq 1$.

Reference

1. G. H. Hardy and E. M. Wright, An Introduction to the Theory of Numbers, Oxford University Press, London, 1960, pp. 343–4.

THE GENERAL CAYLEY-HAMILTON THEOREM VIA THE EASIEST REAL CASE

J. DENMEAD SMITH, College of the Resurrection, Mirfield, Yorkshire, England.

Let A be a square matrix with elements in a field, and let $G(\lambda)$ denote the characteristic polynomial $\det(\lambda I - A)$. When A can be reduced to diagonal form by a similarity transformation, the proof that A satisfies its characteristic equation is particularly transparent, since each eigenspace is annihilated by a factor $A - \lambda_0$ in $G(A)$, where λ_0 is the characteristic value of the eigenspace. As it stands, this method is capable of giving the result only when a complete set of eigenspaces for A can be found, and general proofs usually depend either on canonical forms or on the use of adjoint matrices.

The proof of the Cayley-Hamilton theorem that we give here demonstrates how the simplest and most transparent method of diagonalization can be used to provide a proof in the general case of a square matrix A with elements that belong to an arbitrary commutative ring R. Apart from some elementary algebra, the only result that is required is the easy proof of the theorem for real matrices which have real and distinct characteristic roots.

Suppose that A is the $n \times n$ matrix $[a_{ij}]$, where $a_{ij} \in R$ for $1 \leqq i, j \leqq n$. Now let $X = [x_{ij}]$, $1 \leqq i, j \leqq n$, where each x_{ij} is an *indeterminate*, and let P denote the domain of polynomials which are generated over the integers by $\{x_{ij}\}$ and contain no 'constant' terms. A ring homomorphism $\phi: P \to R$ may be defined which 'evaluates' each polynomial at the point $x_{11} = a_{11}, x_{12} = a_{12}, \cdots, x_{nn} = a_{nn}$. Thus if $f(x_{11}, x_{12}, \cdots, x_{nn}) \in P$, this is mapped to $f(a_{11}, a_{12}, \cdots, a_{nn}) \in R$. The characteristic polynomials of X and A are defined over P and R as follows:

$$F(\lambda) = \det(\lambda I - X) = \lambda^n - p_1\lambda^{n-1} + \cdots + (-)^n p_n \quad \text{and}$$

$$G(\lambda) = \det(\lambda I - A) = \lambda^n - r_1\lambda^{n-1} + \cdots + (-1)^n r_n,$$

where each $p_j \in P$ and $r_j \in R$. If $f_{kl} \in P$ and $g_{kl} \in R$ denote the entries in the kl-position of the matrices $F(X)$ and $G(A)$, it follows from the relations $r_j = \phi(p_j)$ that $g_{kl} = \phi(f_{kl})$, and hence that $G(A)$ is zero if $F(X)$ is zero. Thus, to