$$
\begin{aligned}
(25)\quad & E\{(x_1 - a_1)^k(x_2 - a_2)^l \cdots (x_r - a_r)^m\} \\
& = (p_1e^{D_1} + p_2e^{D_2} + \cdots + p_re^{D_r})^n \cdot x_1^k x_2^l \cdots x_r^m \Big]_{x_1=-a_1,\ \ldots,\ x_r=-a_r},
\end{aligned}
$$

where $D_1 = \partial/\partial x_1$.

WASHINGTON, D. C.

ON A RESULTANT CONNECTED WITH FERMAT'S LAST THEOREM

BY EMMA LEHMER

E. Wendt* seems to have been the first to introduce the resultant of $x^n = 1$ and $(x+1)^n = 1$ in connection with Fermat's Last Theorem. This resultant can be expressed by means of the following circulant of binomial coefficients

$$
\Delta_n = \begin{vmatrix} 1 & C_{n,1} & C_{n,2} \cdots C_{n,n-1} \\ C_{n,n-1} & 1 & C_{n,1} \cdots C_{n,n-2} \\ \cdot & \cdot & \cdot \cdots \cdot \\ C_{n,1} & C_{n,2} & C_{n,3} \cdots 1 \end{vmatrix}.
$$

In his book on Fermat's Last Theorem Bachmann† proved that if p is an odd prime and if Δ_{p-1} is not divisible by p^3, then Fermat's equation $x^p + y^p + z^p = 0$ has no solution (x, y, z) prime to p.

S. Lubelsky‡ proved in a recent paper, using the distribution of quadratic residues, that if $p \geqq 7$, Δ_{p-1} is not only divisible by p^3, but by p^8, thus annulling Bachmann's criterion except for $p=3$ and $p=5$.

We shall now show how, by a straightforward manipulation with the above determinant, one can prove much more.

THEOREM 1. *Δ_{p-1} is divisible by $p^{p-2}q_2$ for every prime p, where q_2 is the Fermat quotient* $(2^{p-1}-1)/p$.

---

* Journal für Mathematik, vol. 113 (1894), pp. 335–347.

† *Das Fermatproblem*, 1919, p. 59.

‡ Prace Matematyczno-Fizyczne, vol. 42 (1935), pp. 11–44.

PROOF. First add to each element of the last column of Δ_{p-1} the corresponding element of all the other columns. The elements of the last column now become equal to

$$1 + C_{p-1,1} + C_{p-1,2} + \cdots + C_{p-1,p-2} = 2^{p-1} - 1.$$

Next increase each element of the first $p-3$ columns by the element immediately to the right of it. All the elements of the first $p-3$ columns are now of the form

$$C_{p-1,k} + C_{p-1,k+1} = C_{p,k+1} = pI_k, \qquad (k = 0, 1, \cdots, p-2).$$

Since, as is well known, I_k is an integer for p a prime, it follows that p is a factor of each of the first $p-3$ columns. Also $(2^{p-1}-1)$ comes out of the last column, and hence Δ_{p-1} is divisible by $(2^{p-1}-1)p^{p-3}=p^{p-2}q_2$, which is the theorem.

For example, if $p=5$,

$$\Delta_4 = \begin{vmatrix} 1 & 4 & 6 & 4 \\ 4 & 1 & 4 & 6 \\ 6 & 4 & 1 & 4 \\ 4 & 6 & 4 & 1 \end{vmatrix} = \begin{vmatrix} 1 & 4 & 6 & 15 \\ 4 & 1 & 4 & 15 \\ 6 & 4 & 1 & 15 \\ 4 & 6 & 4 & 15 \end{vmatrix}$$

$$= \begin{vmatrix} 5 & 10 & 6 & 15 \\ 5 & 5 & 4 & 15 \\ 10 & 5 & 1 & 15 \\ 10 & 10 & 4 & 15 \end{vmatrix} = 15\cdot 5^2 \begin{vmatrix} 1 & 2 & 6 & 1 \\ 1 & 1 & 4 & 1 \\ 2 & 1 & 1 & 1 \\ 2 & 2 & 4 & 1 \end{vmatrix} = -\,5^3\cdot 3.$$

It is interesting to notice that although Theorem 1 is in no way dependent on the solvability of Fermat's equation, nevertheless it enables us to replace Bachmann's criterion by the following one.

If Δ_{p-1} is not divisible by p^{p-1}, then $x^p+y^p+z^p=0$ has no solution (x, y, z) prime to p.

This in fact is merely a restatement of Wiefrich's criterion,* which states that if p does not divide q_2, Fermat's equation has no solution in integers prime to p.

For example, since we have seen that Δ_4 is not divisible by 5^4, it follows from our criterion that $x^5+y^5+z^5=0$ has no solutions (x, y, z) prime to 5.

---

* Journal für Mathematik, vol. 136 (1909), pp. 293–302.

Before proceeding further it may be of interest to give a short, though perhaps less elementary proof of Theorem 1, based directly on the definition of the resultant of two polynomials as the product $f(\alpha_1)\cdot f(\alpha_2)\cdots f(\alpha_n)$, where f is one polynomial and the α's are roots of the other.

$$\Delta_{p-1} = \prod_{j=1}^{p-1}[(\epsilon_j + 1)^{p-1} - 1],$$

where ϵ_j are all the $(p-1)$st roots of unity.

For $\epsilon_j = 1$, we get the factor $2^{p-1}-1$, and for $\epsilon_j = -1$, we get -1. For $\epsilon_j = \epsilon$, any complex root of unity, we have

$$(\epsilon + 1)^{p-1} - 1 = C_{p-1,1}\epsilon + C_{p-1,2}\epsilon^2 + \cdots + \epsilon^{p-1}.$$

But since, for p a prime,

$$C_{p-1,k} = (-1)^k + pc_k,$$

where the c's are integers,* we have

$$\begin{aligned}(\epsilon + 1)^{p-1} - 1 &= -\epsilon + \epsilon^2 - \epsilon^3 + \cdots + \epsilon^{p-1} + pf(\epsilon)\\ &= \epsilon(\epsilon^{p-1} - 1)/(\epsilon + 1) + pf(\epsilon) = pf(\epsilon),\end{aligned}$$

where $f(x)$ is a polynomial with integral coefficients. Hence

$$\Delta_{p-1} = -(2^{p-1} - 1)\prod_{\epsilon_j \neq \pm 1} pf(\epsilon_j) = -(2^{p-1} - 1)\cdot p^{p-3}\prod f(\epsilon_j),$$

where $\prod f(\epsilon_j)$ is an integral symmetric function of the roots of $(x^{p-1}-1)/(x^2-1)$ and hence an integer. Hence Δ_{p-1} is divisible by $p^{p-2}q_2$.

In comparing Theorem 1 with that of Lubelsky we see that Theorem 1 says more, except for $p=7$, in which case Theorem 1 guarantees divisibility of Δ_6 by 7^5 instead of 7^8. On examining this case more closely we find that as a matter of fact $\Delta_6 = 0$. Indeed, we have in general the following theorem.

THEOREM 2. $\Delta_n = 0$ *if and only if* $n = 6k$.

PROOF. In order that $\Delta_n = 0$ it is both necessary and sufficient that $x^n = 1$ and $(x+1)^n = 1$ have a root ρ in common. But the roots of $x^n = 1$ are the nth roots of unity. Hence we can write

* Lucas, American Journal of Mathematics, vol. 1 (1878), pp. 229–230.

$\rho = \cos\theta + i\sin\theta$, but since at the same time ρ is a root of $(x+1)^n = 1$, we have

$$|\rho + 1| = 1 = (\cos\theta + 1)^2 + \sin^2\theta = 2 + 2\cos\theta,$$

or $\cos\theta = -1/2$ and $\theta = \pm 2\pi/3$. This condition will be satisfied if and only if $\rho = \omega$ or ω^2, while $(\rho+1) = -\omega^2$ or $-\omega$, and hence $(\rho+1)^n = 1$ if and only if n is a multiple of 6.

One can easily show by adding to each element of the first and second column of Δ_{6k} (written in determinant form) the corresponding elements of every third column, that the elements of the two resulting columns will be equal and hence that $\Delta_{6k} = 0$, but the writer has not been able to show from the circulant definition of Δ_n that $\Delta_n \neq 0$ if n is not a multiple of 6.

In conclusion we give a short table of Δ_{p-1}.

p	Δ_{p-1}
3	$-3 = -(2^2-1)$
5	$-375 = -(2^4-1)\cdot 5^2$
7	0
11	$-210\ 736\ 858\ 987\ 743 = -(2^{10}-1)\cdot 11^8\cdot 31^2$
13	0
17	$-1\ 562\ 716\ 604\ 038\ 367\ 719\ 196\ 682\ 456\ 673\ 375 =$ $-(2^{16}-1)\cdot 17^{14}\cdot(3^3\cdot 5\cdot 7^3\cdot 257)^2$
19	0

It appears from this table of Δ_{p-1}, and can be shown without difficulty for any even n, that Δ_n is $-(2^n-1)$ times a perfect square. It can also be shown that Δ_d divides Δ_n if d divides n.

BETHLEHEM, PENNSYLVANIA