So, for the same value of h, namely, $\bar{h}$, there are two values of θ, namely, $\bar{\theta}$ and $\bar{\theta}'$, which is absurd, since θ is single-valued.

(b) If the discontinuity is of the second kind, then there must be a sequence $\{h_n\}$, tending to $\bar{h}$, for which the corresponding sequence $\{\xi_n\}$ does not tend to any limit. Therefore two values k_1 and k_2 of h can always be found as near as we please to $\bar{h}$ such that the corresponding values η_1 and η_2 of ξ differ from each other by a quantity greater than a suitably prescribed positive quantity δ. But, from (M), $f(h)/h$ and, consequently, $f'(\xi)$ are continuous functions of h at $\bar{h}$. Therefore ξ must be multiple-valued at $\bar{h}$, which is absurd, since θ is single-valued.

THE UNIVERSITY OF CALCUTTA

A NUMERICAL FUNCTION APPLIED TO CYCLOTOMY

BY EMMA T. LEHMER

A function $\phi_2(n)$ giving the number of pairs of consecutive integers each less than n and prime to n, was considered first by Schemmel.* In applying this function to the enumeration of magic squares, D. N. Lehmer† has shown that if one replaces consecutive pairs by pairs of integers having a fixed difference λ prime to $n = \prod_{i=1}^{t} p_i^{\alpha_i}$, then the number of such pairs (mod n) whose elements are both prime to n is also given by

$$\phi_2(n) = \prod_{i=1}^{t} p_i^{\alpha_i - 1}(p_i - 2) .$$

As is the case for Euler's totient function $\phi(n)$, the function $\phi_2(n)$ obviously enjoys the multiplicative property $\phi_2(m)\phi_2(n) = \phi_2(mn)$, $(m, n) = 1$, $\phi_2(1) = 1$. *In what follows we call an integer simple if it contains no square factor* > 1. For a simple number n we have the following analog of Gauss' theorem:

$$\sum_{\delta \mid n} \phi_2(\delta) = \phi(n), \tag{1}$$

---

* Journal für Mathematik, vol. 70 (1869), pp. 191–2.

† Transactions of this Society, vol. 31 (1929), pp. 538–9.

where n is simple and where the summation extends over all the divisors of n.* Using Dedekind's inversion formula, we can write

$$\sum_{\delta|n}\phi(n/\delta)\mu(\delta) = \phi_2(n), \tag{2}$$

where n is simple and where $\mu(n)$ is Merten's inversion function.*

It is the purpose of this note to develop another property of $\phi_2(n)$, true only for simple numbers, and apply it to the evaluation of the discriminants and resultants of cyclotomic equations.

Let $\{\lambda_k\}$ denote the set of numbers less than n and prime to n, and let λ be any number of this set. Then it follows at once from D. N. Lehmer's result, that there are $\phi_2(n)$ numbers prime to n in the set $\{\lambda+\lambda_k\}$. Let us inquire how many numbers in the set $\{\lambda+\lambda_k\}$ have with n a greatest common divisor Δ.

THEOREM 1. *If Δ is a divisor of the simple number n, and if λ is any fixed number prime to n, and if $\lambda_k(k=1, 2, \cdots, \phi(n))$ runs over a complete set of numbers $<n$ and prime to n, then there are $\phi_2(n/\Delta)$ multiples of Δ prime to n/Δ in the set $\{\lambda+\lambda_k\}$.*

PROOF. Let $n=\Delta\prod_{i=1}^{h}p_i$. Instead of the set $\{\lambda_k\}$ consider the set

$$1, 2, 3, \cdots, n. \tag{I}$$

The set

$$\lambda + 1, \lambda + 2, \lambda + 3, \cdots, \lambda + n, \tag{II}$$

taken modulo n, is the set (I) in some order. In the set (II) there are n/Δ multiples of Δ, $\phi(n/\Delta)$ of which are prime to n/Δ. But this result applies to the set (II) instead of the desired set $\{\lambda+\lambda_k\}$. We must therefore exclude those multiples of Δ from the set (II) which have arisen from the addition of λ to those numbers of the set (I) which do not belong to the set $\{\lambda_k\}$. It is clear that none of the $\phi(n/\Delta)$ multiples of Δ mentioned above were obtained by adding λ to numbers not prime to Δ. We have then to exclude only multiples of Δ obtained by adding λ to numbers not prime to $\prod_{i=1}^{h}p_i$.

In (I) there are n/p_ν multiples of p_ν. Adding λ to each of these, we obtain a subset (II$_\nu$) of (II),

* Dickson, *History of the Theory of Numbers*, Chap. 19.

$$(\mathrm{II}_\nu) \qquad p_\nu + \lambda,\ 2p_\nu + \lambda,\ 3p_\nu + \lambda,\ \cdots,\ \frac{n}{p_\nu}p_\nu + \lambda.$$

Taken modulo n/p_ν, the set (II_ν) is a complete set of incongruent residues. Hence in this set there are $(n/p_\nu)\Delta$ multiples of Δ, not all of which, however, are prime to n/Δ. In fact in the set (II_ν) there are $n/(p_\nu\Delta p_1)$ multiples of p_1, $n/(p_\nu\Delta p_2)$ multiples of p_2 etc. to be excluded. But this excludes twice the multiples of p_1p_2, p_1p_3, $\cdots$, etc. These have to be restored once. By the well known principle of cross-classification, we find that the number of multiples of Δ prime to n/Δ in the set (II_ν) is

$$\frac{n}{p_\nu\Delta} - \sum\frac{n}{p_\nu\Delta p_i} + \sum\frac{n}{p_\nu\Delta p_ip_j} - \cdots = \phi\left(\frac{n}{p_\nu\Delta}\right).$$

As ν runs from 1 to h, we get subsets (II_1), (II_2), $\cdots$, (II_h) of the set (II). The total amount we must subtract, at this stage, from $\phi(n/\Delta)$ to allow for numbers in the set (I) not prime to n is

$$\sum_{\nu=1}^{h}\phi\left(\frac{n}{p_\nu\Delta}\right).$$

But again this excludes twice those multiples of Δ in the set (II) which correspond to multiples of p_1p_2, p_1p_3, $\cdots$, in the set (I). These multiples must be restored once and, using once more the principle of cross-classification, we find that the number of multiples of Δ prime to n/Δ in the set $\{\lambda+\lambda_k\}$ is given by

$$\phi\left(\frac{n}{\Delta}\right) - \sum\phi\left(\frac{n}{p_i\Delta}\right) + \sum\phi\left(\frac{n}{p_ip_j\Delta}\right) - \cdots$$

$$= \sum_{\delta\mid n/\Delta}\phi\left(\frac{n}{\Delta\delta}\right)\mu(\delta) = \phi_2\left(\frac{n}{\Delta}\right),$$

by (2). Hence the theorem is proved.

The preceding theorem is not true for non-simple numbers. The corresponding theorem for Euler's $\phi(n)$ states that the number of numbers $m<n$ such that $(m, n)=\Delta$, is $\phi(n/\Delta)$. This is true for all n. The simple proof of this theorem cannot be extended to Theorem 1.

It is important to notice that the result of Theorem 1 is independent of the choice of λ. As λ runs over all the numbers

in the set $\{\lambda_k\}$ one obtains a matrix $\|a_{ij}\| = \|\lambda_i + \lambda_j\|$ in which by Theorem 1 there are $\phi(n)\ \phi_2(n/\Delta)$ multiples of Δ prime to n/Δ.

The above result furnishes a ready method of obtaining the explicit formula for the discriminant* of the cyclotomic equation $Q_n(x) = 0$, whose roots are the primitive nth roots of unity without repetition, for n a simple number. The following lemma will enable us to obtain the discriminant for a general n.

LEMMA. *If $f(x) = g(x^m)$ is a polynomial of degree k in x^m, and if the discriminant of $g(x)$ is D_g, then the discriminant of $f(x)$ is*

$$D_f = a_k^2 \cdot m^{mk} D_g^m,$$

where a_k is the constant term of $g(x)$.

PROOF. Let $\rho_i (i = 1, 2, \cdots, k)$ be the roots of $g(x) = 0$, and let one of the values of $\rho_i^{1/m}$ be θ_i. Then all the roots of $f(x) = 0$ are given by $\theta_i \epsilon^\tau$, where ϵ is a primitive mth root of unity and $\tau = 1, 2, \cdots, m$. Then the discriminant of $f(x)$ can be written

$$D_f = \prod_{i<j\leqq k} \prod_{\tau,\nu=1}^{m} (\theta_i \epsilon^\nu - \theta_j \epsilon^\tau)^2 \cdot \prod_{i=1}^{k} \prod_{\tau<\nu\leqq m} (\theta_i \epsilon^\nu - \theta_i \epsilon^\tau)^2.$$

The first product is

$$\prod_{i<j\leqq k} \prod_{\nu=1}^{m} [(\theta_i \epsilon^\nu)^m - \theta_j{}^m]^2 = \prod_{i<j\leqq k} (\theta_i{}^m - \theta_j{}^m)^{2m}$$
$$= \prod_{i<j\leqq k} (\rho_i - \rho_j)^{2m} = D_g^m.$$

For the second product we have

$$\prod_{i=1}^{k} \theta_i{}^{2m} \prod_{\tau<\nu\leqq m} (\epsilon^\nu - \epsilon^\tau)^2 = \prod_{i=1}^{k} \rho_i^2 \prod_{\tau<\nu\leqq m} (\epsilon^\nu - \epsilon^\tau)^2$$
$$= a_k^2 \prod_{\tau<\nu\leqq m} (\epsilon^\nu - \epsilon^\tau)^{2k}.$$

The product

$$\prod_{\tau<\nu\leqq m} (\epsilon^\nu - \epsilon^\tau)^2$$

* Rados, Journal für Mathematik, vol. 131 (1906), pp. 49–55, has calculated the discriminant using the derivative definition. The reduction to a simple number would have simplified his proof considerably.

is the discriminant of x^m-1, which is known to be m^m. Hence the lemma follows at once.

We shall proceed to find the discriminant of Q_n for n a simple number.

THEOREM 2. *If n is simple, the discriminant of $Q_n(x)=0$ is given by*

$$D_n = (-1)^{\phi(n)/2} \prod_{i=1}^{t} p_i^{\phi(n/p_i)\phi_2(p_i)}.$$

PROOF. Since the roots of $Q_n(x)=0$ are $e^{2\pi i\lambda_k/n}$ we have

$$\begin{aligned} D_n &= \prod_{\lambda_k<\lambda_m} (e^{2\pi i\lambda_k/n} - e^{2\pi i\lambda_m/n})^2 \\ &= (-1)^{\phi(n)/2} \prod_{\lambda_k\neq\lambda_m} (e^{2\pi i\lambda_k/n} - e^{2\pi i\lambda_m/n}) \\ &= [\prod e^{2\pi i\lambda_k/n}]^{\phi(n)-1} \prod_{\lambda_k\neq\lambda_m} (1 - e^{2\pi i\lambda_m/n}). \end{aligned}$$

The first product is unity, since $Q_n(0)=1$. To evaluate the second product we observe that there is a one to one correspondence between the numbers $\{\lambda_m-\lambda_k\}$ (mod n) and the elements of the matrix discussed above. The condition $\lambda_m\neq\lambda_k$ excludes from the matrix all the multiples of n. For a divisor Δ of n, the factors of the second product may be grouped into sets of $\phi(n/\Delta)$ elements each, in which $\lambda_m-\lambda_k$ runs over all the numbers prime to n/Δ. By Theorem 1 there are $\phi(n)\phi_2(n/\Delta)/\phi(n/\Delta)=\phi(\Delta)\phi_2(n/\Delta)$ such sets for each $\Delta<n$. Hence

$$D_n = (-1)^{\phi(n)/2} \prod_{\Delta\neq n} [Q_{n/\Delta}(1)]^{\phi(\Delta)\phi_2(n/\Delta)}.$$

It is known* that $Q_n(1)$ is p or 1 according as m is a power of a prime p, or not. Accordingly we have

$$D_n = (-1)^{\phi(n)/2} \prod_{i=1}^{t} p_i^{\phi(n/p_i)\phi_2(p_i)},$$

which is the theorem.

---

* N. Trudi, Atti Accademia Napoli, vol. 3 (1866–8), pp. 20–29; Netto, *Vorlesungen über Algebra*, vol. 1, p. 357.

To get the discriminant for a general n we make use of the relation*

$$Q_n(x) = Q_{n_0}(x^m), \tag{3}$$

where $n = n_0 m$, and n_0 is the largest simple factor of n. Hence applying our lemma with $k = \phi(n_0)$ and $a_k = 1$, we have

$$D_n = D_{n_0}^m \cdot m^{m\phi(n_0)} = (-1)^{m\phi(n_0)/2} m^{m\phi(n_0)} \prod_{i=1}^{t} P_i^{m\phi(n_0/p_i)\phi_2(p_i)}.$$

But, since $\phi(n_0/p_i)\phi_2(p_i) = \phi(n_0) - \phi(n_0)/(p_i - 1)$ and $m\phi(n_0) = \phi(n)$, the discriminant can be written in the following general form:

$$D_n = (-1)^{\phi(n)} \frac{n^{\phi(n)}}{\prod_{i=1}^{t} P_i^{\phi(n)/(p_i-1)}}.$$

We shall next consider the resultant $R_{m,n}$ of any Q_m and Q_n. First let m and n be simple numbers ($m \neq n$). Then we have

THEOREM 3. *If m, n are simple numbers,† and $m < n$, then*

$$R_{m,n} = \begin{cases} p^{\phi(m)}, & \text{if } n/m = p, \\ 1, & \text{if } n/m \neq p, \end{cases}$$

where p is a prime.

PROOF. Let $(m, n) = d$, and $m = m_1 d$, $n = n_1 d$. Then if λ and λ' run over numbers prime to m and n, respectively, we have

$$R_{m,n} = \prod (e^{2\pi i\lambda/m} - e^{2\pi i\lambda'/n}) = [\prod e^{2\pi i\lambda/n}]^{\phi(n)} \cdot \prod (1 - e^{2\pi i(\lambda' m - \lambda n)/(mn)}).$$

The product $[\prod e^{2\pi i\lambda/m}]^{\phi(n)}$ is equal to 1. The fractions occurring in the last product may be written $(\lambda' m_1 - \lambda n_1)/(m_1 n_1 d)$. The numerators are all prime to $m_1 n_1$ but may not be prime to d. Modulo d, the numbers $\lambda' m$ and λn run, respectively, $\phi(m_1)$ and $\phi(n_1)$ times over the complete set of numbers prime to d. If δ is any divisor of d, then by Theorem 1, there are

* Trudi, Annali di Matematica, (2), vol. 2 (1868–9), pp. 160–2; Netto, loc. cit.

† $R_{1,2} = -R_{2,1} = 2$. For all other values of m, n, $R_{m,n} = R_{n,m}$.

$\phi(m_1)\phi(n_1)\phi(d)\phi_2(d/\delta)$ multiples of δ prime to d/δ in the set $\lambda' m_1 - \lambda n_1$. Hence

$$R_{m,n} = \prod_{\delta \mid d} [Q_{m_1 n_1 d/\delta}(1)]^{\phi(\delta)\phi_2(d/\delta)}.$$

But, by Trudi's theorem quoted above concerning $Q(1)$, the factors of the above product are equal to unity for $\delta < d$. For dm_1n_1/δ cannot be a prime. Hence

$$R_{m,n} = Q_{m_1 n_1}^{\phi(d)}(1).$$

Again, by Trudi's theorem, this expression is unity except when $m_1 n_1$ is a prime p, that is, when $n/m = p$. In this case $R_{m,n} = p^{\phi(m)}$. Hence the theorem.

To find the resultant $R_{m,n}$, where m and n are any distinct integers, we may proceed as follows. Let $m = m_0\mu$ and $n = n_0\nu$ where m_0 and n_0 are the largest simple divisors of m and n. Let also $(\mu, \nu) = d$, $(m_0, \nu/d) = d_1$ and $(n_0, \mu/d) = d_2$. Finally let r_k and s_l be the roots of $Q_{m_0}(x) = 0$ and $Q_{n_0}(x) = 0$; let ρ_k be one of the values of $r_k^{1/\mu}$ and σ_l be one of the values of $s_l^{1/\nu}$. Then, by (3), all the roots of $Q_m(x) = 0$ are given by $\rho_k \epsilon_\mu^i$, where ϵ_μ is a primitive μth root of unity, $k = 1, 2, \cdots, \phi(m_0)$, and $i = 1, 2, \cdots, \mu$. Similarly the roots of $Q_n(x) = 0$ are given by $\sigma_l \epsilon_\nu^j$, where ϵ_ν is a primitive νth root of unity, $l = 1, 2, \cdots, \phi(n_0)$, and $j = 1, 2, \cdots, \nu$. Hence we may write

$$\begin{aligned} R_{m,n} &= \prod_{k=1}^{\phi(m_0)} \prod_{l=1}^{\phi(n_0)} \prod_{i=1}^{\mu} \prod_{j=1}^{\nu} (\rho_k \epsilon_\mu^i - \sigma_l \epsilon_\nu^j) \\ &= \prod_{k,l} \prod_{i=1}^{\mu} (\rho_k^{\nu} \epsilon_\mu^{i\nu} - \sigma_l^{\nu}) = \prod_{k,l} \prod_{i=1}^{\mu/d} (\rho_k^{\nu i d} \epsilon_\mu^{\nu i d} - s_l)^d \\ &= \prod_{k,l} (r^{\nu/d} - s^{\mu/d})^d = \prod_{k=1}^{\phi(m_0/d_1)} \prod_{l=1}^{\phi(n_0/d_2)} (\bar{r}_k - \bar{s}_l)^{d\phi(d_1)\phi(d_2)}, \end{aligned}$$

where $\bar{r}$ and $\bar{s}$ are respectively the roots of $Q_{m_0/d_1}(x) = 0$ and $Q_{n_0/d_2}(x) = 0$. Hence

$$R_{m,n} = R_{m_0/d_1,\, n_0/d_2}^{d\phi(d_1)\phi(d_2)}.$$

Since m_0/d_1 and n_0/d_2 are simple numbers we may apply Theorem 3 and obtain the following result.

THEOREM 4. *Let $m=m_0\mu$ and $n=n_0\nu$ be any positive integers, where m_0 and n_0 are the largest simple divisors of m and n. Let $(\mu, \nu)=d$, $(m_0, \nu/d)=d_1$, $(n_0, \mu/d)=d_2$, and* $m_0d_2<n_0d_1$. Then*

$$R_{m,n} = \begin{cases} p^{d\phi(m_0)\phi(d_2)}, & \text{if } n_0d_1/(m_0d_2) = p, \\ 1, & \text{if } n_0d_1/(m_0d_2) \neq p. \end{cases}$$

Since

$$\prod_{\delta/n} Q_\delta(x) = x^n - 1,$$

and since the discriminant of a product of several polynomials is equal to the product of their discriminants times the product of the squares of the resultants of the polynomials taken two at a time, we have the following identity for n a simple number:

$$n^n = \prod_{\delta/n}\left[\left(\frac{n}{\delta}\right)^{2\phi(\delta)} \prod_{p_i/\delta} p_i^{\phi(\delta/p_i)\phi_2(p_i)}\right].$$

If n is not a simple number, the conditions of Theorem 4 are so complicated that the corresponding identity cannot be easily expressed. The following table which gives the discriminants and the resultants belonging to the divisors of 72 illustrates this identity, and gives some idea of the magnitudes under discussion.

δ	1	2	3	4	6	8	9	12	18	24	36	72	D_δ
1		2	3	2	1	2	3	1	1	1	1	1	1
2			1	2	3	2	1	1	3	1	1	1	1
3				1	2^2	1	3^2	2^2	1	2^2	1	1	3
4					1	2^2	1	3^2	1	1	3^2	1	2^2
6						1	1	2^2	3^2	2^2	1	1	3
8							1	1	1	3^4	1	3^4	2^8
9								1	2^6	1	2^6	2^6	3^9
12									1	2^4	3^4	1	$2^4 3^2$
18										1	2^6	2^6	3^9
24											1	3^8	$2^{16} 3^4$
36												2^{12}	$2^{12} 3^{18}$
72													$2^{48} 3$

$R_{m,n}$ is found in the row marked m and the column marked n. The product of the discriminants times the squares of the resultants listed above is found to be $2^{216}\, 3^{144} = 72^{72}$.

BROWN UNIVERSITY

* This inequality is imposed merely for definiteness and may be reversed at will by interchanging m and n. See the previous footnote.