The Numerical Factors of the Arithmetic Forms $\Pi_{i=1}^{n}(1 \pm \alpha_i^m)$
Author(s): Tracy A. Pierce
Source: *Annals of Mathematics*, Second Series, Vol. 18, No. 2 (Dec., 1916), pp. 53-64
Published by: Mathematics Department, Princeton University
Stable URL: https://www.jstor.org/stable/2007169
Accessed: 18-01-2020 09:00 UTC

THE NUMERICAL FACTORS OF THE ARITHMETIC FORMS $\prod_{i=1}^{n}(1 \pm \alpha_i^m)$.

By Tracy A. Pierce.

1. Introduction. The object of the present investigation is to study the arithmetic properties of the numbers given by the forms $\Pi_{i=1}^{n}(1 \pm \alpha_i^m)$ where $\alpha_1, \alpha_2, \cdots, \alpha_i, \cdots, \alpha_n$ are the roots of the equation

$$f(x) = x^n + a_1x^{n-1} + a_2x^{n-2} + \cdots + a_n = 0, \tag{1}$$

whose coefficients are integers. It is readily seen that $\Pi_{i=1}^{n}(1 \pm \alpha_i^m)$ represents an integer, for since it is a rational integral symmetric function of the roots of (1) it may be rationally and integrally expressed in terms of the integer coefficients of (1).

As m takes different positive integer values the forms $\Pi_{i=1}^{n}(1 - \alpha_i^m)$ and $\Pi_{i=1}^{n}(1 + \alpha_i^m)$ generate two series of integers. The numbers of these series will be designated by Δ_m and S_m respectively.

Using different arithmetic forms, namely $(\alpha^m - \beta^m)/(\alpha - \beta)$ and $\alpha^m + \beta^m$, Lucas* and Carmichael† have done work of a somewhat similar character but for the case of a quadratic equation only. The properties of Δ_m and S_m which depend on the principles of algebraic divisibility are almost identical with the corresponding properties of the forms used by Lucas and Carmichael. In § 2 we develop these properties of Δ_m and S_m.

In § 3 by the use of the dialytic method of elimination applied to congruences a condition for real solutions of $f(x) \equiv 0 \pmod{p}$ is obtained. The condition is expressed in terms of Δ_{p-1} calculated for the equation $f(x) = 0$.

In § 4 we investigate the factors of Δ_m corresponding to real solutions of $f(x) \equiv 0 \pmod{p^m}$.

In §§ 5, 6, and 7 algebraic number-theory is applied to determine the forms of the factors of Δ_p. The cases of the quadratic, cubic, and the general equation are treated separately.

In § 8 the forms of the factors of Δ_m where m is composite are determined.

---

* Am. Journ. of Math., vols. 1 and 2, 1878–79.

† Annals of Math., Second Series, vol. 15 (1913) p. 30. References to other works are given in this paper as well as in the Encyk. der Math. Wiss., 1:2, p. 596.

2. **Properties of Δ_m and S_m depending on algebraic divisibility.** Since

$$\prod_{i=1}^{n}(1-\alpha_i^{2m}) = \prod_{i=1}^{n}(1+\alpha_i^{m})\prod_{i=1}^{n}(1-\alpha_i^{m}),$$

$$\Delta_{2m} = S_m \cdot \Delta_m. \tag{2}$$

Continued application of this decomposition gives

$$\Delta_{2^\lambda k} = S_{2^{\lambda-1}k} \cdot S_{2^{\lambda-2}k} \cdots S_k \cdot \Delta_k.$$

Also since

$$\frac{\Delta_{md}}{\Delta_d} = \frac{\prod_{i=1}^{n}(1-\alpha_i^{md})}{\prod_{i=1}^{n}(1-\alpha_i^{d})} = \prod_{i=1}^{n}(1+\alpha_i^{d}+\alpha_i^{2d}+\cdots+\alpha_i^{(m-1)d})$$

is a rational integral symmetric function of the roots of (1) it is an integer and therefore Δ_{md} is divisible by Δ_d and similarly by Δ_m. Hence in general the Δ's of composite subscript are factorable immediately.

As a particular case of the result above, every Δ_m is divisible by

$$\Delta_1 = \prod_{i=1}^{n}(1-\alpha_i) = 1 - \Sigma\alpha_i + \Sigma\alpha_i\alpha_j - \cdots \pm \Pi\alpha_i$$
$$= 1 + a_1 + a_2 + \cdots + a_n.$$

Or, in other words, every Δ_m is divisible by the sum of the coefficients of equation (1).

In as much as

$$\frac{S_{(2m+1)d}}{S_d} = \frac{\prod_{i=1}^{n}(1+\alpha_i^{(2m+1)d})}{\prod_{i=1}^{n}(1+\alpha_i^{d})} = \prod_{i=1}^{n}(1-\alpha_i^{d}+\alpha_i^{2d}-\cdots\pm\alpha_i^{2md})$$

is a rational integral symmetric function of the roots of (1) we see that $S_{(2m+1)d}$ is divisible by S_d. In particular, every S_m whose subscript is odd is divisible by

$$S_1 = \prod_{i=1}^{n}(1+\alpha_i) = 1 + \Sigma\alpha_i + \Sigma\alpha_i\alpha_j + \cdots + \Pi\alpha_i$$
$$= 1 - a_1 + a_2 - \cdots \pm a_n.$$

We shall now develop formulæ for partially factoring Δ_m and S_m. To this end let $Q_m(x) = 0$ be the algebraic equation, with leading coefficient unity, whose roots are the primitive mth roots of unity; then

$$x^m - 1 = \prod_d Q_d(x),$$

where d ranges over all the divisors of m.*

* Bachmann, Kreistheilung, 3d lecture.

By means of the equation above we may express Δ_m in terms of the Q-function. Thus, we have

$$\pm \Delta_m = \prod_{i=1}^{n}(1 - \alpha_i^m) = \prod_{i=1}^{n}\prod_{d} Q_d(\alpha_i) = \prod_{d}\prod_{i=1}^{n} Q_d(\alpha_i). \tag{3}$$

For any particular divisor d_1 of m we see that $\Pi_{i=1}^{n} Q_{d_1}(\alpha_i)$ is an integer; hence (3) gives a partial arithmetic factorization of Δ_m when m is composite.

The corresponding factorization of S_m may be obtained as follows. Since

$$\pm \Delta_m = \prod_{i=1}^{n}\prod_{d} Q_d(\alpha_i),$$

d running over all divisors of m, and

$$\pm \Delta_{m/v} = \prod_{i=1}^{n}\prod_{d'} Q_{d'}(\alpha_i),$$

d' running over all divisors of m/v, it follows that

$$\pm \frac{\Delta_m}{\Delta_{m/v}} = \prod_{i=1}^{n}\prod_{\delta} Q_\delta(\alpha_i),$$

where δ ranges over all the divisors of m which are not at the same time divisors of m/v. Now replace m by $2m$ and give v the value 2; then we have by means of (2)

$$\pm \frac{\Delta_{2m}}{\Delta_m} = \pm S_m = \prod_{i=1}^{n}\prod_{\delta} Q_\delta(\alpha_i),$$

where δ ranges over those divisors of $2m$ which contain 2 to the same power as $2m$ itself. This last formula furnishes the partial factorization of S_m when m is composite.

It is a property of the Q-function that

$$Q_m(x) = \frac{(x^m - 1)\Pi(x^{m/p_ip_j} - 1)\cdots}{\Pi(x^{m/p_i} - 1)\Pi(x^{m/p_ip_jp_k} - 1)\cdots}.$$

By substituting $\alpha_1, \alpha_2, \cdots, \alpha_n$ successively for x in this equation and multiplying together the corresponding members of the resulting equations we obtain

$$\prod_{i=1}^{n} Q_m(\alpha_i) = \pm \frac{\Delta_m \Pi \Delta_{m/p_ip_j}\cdots}{\Pi\Delta_{m/p_i}\Pi\Delta_{m/p_ip_jp_k}\cdots}, \tag{4}$$

where the factors denoted by Π in the right-hand member extend over the combinations 2, 4, 6, $\cdots$ at a time of the prime factors $p_i, p_j, p_k, \cdots$ of m in the numerator and over the combinations 1, 3, 5, $\cdots$ at a time in the denominator.

Now if d is a divisor of m we have by means of (3) and (4),

$$\pm \Delta_m = \prod_d \prod_{i=1}^{n} Q_d(\alpha_i) = \pm \prod_d \frac{\Delta_d \Pi \Delta_{d/p_i p_j} \cdots}{\Pi \Delta_{d/p_i} \Pi \Delta_{d/p_i p_j p_k} \cdots},$$

the product extending over all divisors d of m, the p's being the prime factors of d for each d. The corresponding formula for S_m is

$$\pm S_m = \prod_\delta \prod_{i=1}^{n} Q_\delta(\alpha_i) = \pm \prod_\delta \frac{\Delta_\delta \Pi \Delta_{\delta/p_i p_j} \cdots}{\Pi \Delta_{\delta/p_i} \Pi \Delta_{\delta/p_i p_j p_k} \cdots},$$

where δ ranges over those divisors of $2m$ which contain 2 to the same power as $2m$ itself, and the p's are the prime factors of δ for each δ.

In consideration of equation (3) we may state the following theorem:

If $m_1, m_2, \cdots, m_s$ and $n_1, n_2, \cdots, n_r$ be two sets of positive integers such that any positive integer d which is a factor of just t integers of the second set is also a factor of at least t integers of the first set, then the number

$$\frac{\Delta_{m_1} \cdot \Delta_{m_2} \cdots \Delta_{m_s}}{\Delta_{n_1} \cdot \Delta_{n_2} \cdots \Delta_{n_r}}$$

is an integer.

*It follows that the product of any n consecutive terms of the series of numbers $\Delta_1, \Delta_2, \Delta_3, \cdots$ is divisible by the product of the first n terms.**

The corresponding theorems for the series $S_1, S_2, S_3, \cdots$ are:

If $m_1, m_2, m_3, \cdots, m_s$ and $n_1, n_2, n_3, \cdots, n_r$ be two sets of positive integers such that every positive integer d which is a factor of just t integers of the second set with odd quotient is a factor of at least t integers of the first set with odd quotient, then the number

$$\frac{S_{m_1} \cdot S_{m_2} \cdots S_m}{S_{n_1} \cdot S_{n_2} \cdots S_{n_r}}$$

is an integer.

The product of any $2n - 1$ consecutive terms of the series $S_1, S_2, S_3, \cdots$ is divisible by the product of the first n terms.

3. **Condition for real solutions of $f(x) \equiv 0 \pmod{p}$.** The factors of the Δ's furnish valuable information concerning the existence of real solutions of the congruence

$$f(x) = x^n + a_1 x^{n-1} + a_2 x^{n-2} + \cdots + a_n \equiv 0 \pmod{p} \qquad (5)$$

whose left-hand member is the left-hand member of equation (1) and whose modulus is an odd prime p ($p > n$). Indeed we may consider in connection with the above congruence the following

$$x^{\phi(p)} - 1 \equiv 0 \pmod{p},$$

* Compare the corresponding theorems in Carmichael's and Lucas's works (already cited).

where φ is the ordinary totient function. It is well known that this last congruence has its full complement of real roots. If congruence (5) be multiplied by $x, x^2, \cdots, x^{\phi(p)}$ successively and reduced each time by means of the second congruence we shall obtain $\varphi(p)$ congruences. Now regarding the various powers of x as indeterminates of the first degree a necessary condition that the $\varphi(p)$ linear congruences be consistent, and consequently that congruence (5) have a real solution, is that

$$\begin{vmatrix} 1, & a_1, & a_2, & \cdots, & a_n, & 0, & \cdots, & 0 \\ 0, & 1, & a_1, & \cdots, & a_{n-1}, & a_n, & \cdots, & 0 \\ \cdot & \cdot & \cdot & \cdot & \cdot & \cdot & \cdot & \cdot \\ \cdot & \cdot & \cdot & \cdot & \cdot & \cdot & \cdot & \cdot \\ a_1, & a_2, & a_3, & \cdots, & 0, & 0, & \cdots, & 1 \end{vmatrix} \equiv 0 \pmod{p}$$

where the determinant is formed so that the elements in the leading diagonal are unity and the other elements in each row are formed from the $p - 1$ quantities $1, a_1, \cdots, a_n, 0, \cdots, 0$ in cyclical order.

This circulant-determinant of order $\varphi(p) = p - 1$ is known* to be equal to the product

$$f(r_1) \cdot f(r_2) \cdots f(r_{p-1}),$$

where $r_1, r_2, \cdots, r_{p-1}$ are the roots of the equation $x^{p-1} - 1 = 0$. The last product, from the properties of algebraic resultants, is equal numerically to

$$\prod_{i=1}^{n}(1 - \alpha_i^{p-1}) = \Delta_{p-1}.$$

Hence a necessary condition that $f(x) \equiv 0$ *(mod* p*) shall have a real solution is that* $\Delta_{p-1} \equiv 0$ *(mod* p*), or that* Δ_{p-1} *be divisible by* p. Conversely it is not difficult to prove that if $f(x) \equiv 0 \pmod{p}$ has a real root then $\Delta_{p-1} \equiv 0 \pmod{p}$.

If equation (1) has as one of its roots an rth root of unity, then

$$\Delta_r = \prod_{i=1}^{n}(1 - \alpha_i^r) = 0$$

and also

$$\Delta_{r \cdot k} = 0.$$

By the results of the preceding paragraph, the congruence $f(x) \equiv 0 \pmod{p}$ has in this case a real solution for every prime of the form $rk + 1$.

We shall exclude from further consideration the special case when equation (1) has among its roots any root of unity. We shall also assume that (1) is irreducible in the field of rational integers.

* Scott: Theory of Determinants, p. 81.

4. **Properties of the Δ's depending on real solutions of $f(x) \equiv 0 \pmod{p}$.** If we form the equation whose roots are the mth powers of the roots of equation (1) and, following the notation of Gauss, designate this equation by $(f, \alpha^m) = 0$ we have

$$(f, \alpha^m) = \Pi(x - \alpha_i^m) = x^n - \Sigma\alpha_i^m x^{n-1} + \Sigma\alpha_i^m\alpha_j^m x^{n-2} - \cdots \pm \Pi\alpha_i^m$$

and

$$(f, \alpha^m)_{x=1} = \Pi(1 - \alpha_i^m) = 1 - \Sigma\alpha_i^m + \Sigma\alpha_i^m\alpha_j^m - \cdots \pm \Pi\alpha_i^m = \Delta_m. \quad (6)$$

Now it is easy to see that if the original congruence $(f, \alpha) \equiv 0 \pmod{p}$ has the solution $x \equiv k \pmod{p}$ then the congruence $(f, \alpha^m) \equiv 0 \pmod{p}$ has the solution $x \equiv k^m \pmod{p}$. For since $(f, \alpha) = \Pi(x - \alpha_i)$ and $(f, \alpha^m) = \Pi(x - \alpha_i^m)$ it follows that if $\Pi(k - \alpha_i) \equiv 0 \pmod{p}$ then $\Pi(k^m - \alpha_i^m) \equiv 0 \pmod{p}$; for $\Pi(k^m - \alpha_i^m)$ is algebraically divisible by $\Pi(k - \alpha_i)$ which is itself a multiple of p by hypothesis.

It follows that if k belongs to the exponent e modulo p then $x \equiv k^e \equiv 1 \pmod{p}$ is a solution of $(f, \alpha^e) \equiv 0 \pmod{p}$; whence by means of (6) we see that Δ_e is divisible by p.

The S's may be treated in a similar manner by use of the equation

$$(f, \alpha^m)_{x=-1} = \pm (1 + \Sigma\alpha_i^m + \cdots + \Pi\alpha_i^m) = \pm \Pi(1 + \alpha_i^m) = \pm S_m.$$

Thus whenever Δ_{p-1} is divisible by p and $x \equiv k \pmod{p}$ is a solution of $(f, \alpha) \equiv 0 \pmod{p}$ such that $k^{e_1} \equiv -1 \pmod{p}$ then $(f, \alpha^{e_1}) \equiv 0 \pmod{p}$ has the solution $x \equiv -1 \pmod{p}$, or in other words S_{e_1} is divisible by p. If the exponent e to which k belongs modulo p is even, then $k^{e/2} \equiv -1 \pmod{p}$.* Furthermore if $k^e \equiv 1 \pmod{p}$ then assuming e less than $p - 1$ we have $e \leqq \frac{1}{2}(p - 1)$. In view of this fact, we may state the theorem: *If in the sequence* $\Delta_1, \Delta_2, \cdots, \Delta_{\frac{1}{2}(p-1)}, S_1, S_2, \cdots, S_{\frac{1}{2}(p-1)}$ *the prime* p *appears only as a factor of* $S_{\frac{1}{2}(p-1)}$ *then the real solution of* $(f, \alpha) \equiv 0 \pmod{p}$ *is a primitive root of* p.

When the congruence $(f, \alpha) = \Pi(x - \alpha_i) \equiv 0 \pmod{p}$ has m incongruent solutions $k_1, k_2, \cdots, k_m$ and no multiple solutions, thus implying that p does not divide the discriminant of $(f, \alpha) = 0$, the congruence

$$(f, \alpha) \equiv 0 \pmod{p^m}$$

also has m solutions $K_1, K_2, \cdots, K_m$ all of which are distinct.† Thus if

$$(f, \alpha) \equiv (x - k_1)(x - k_2) \cdots (x - k_m)\psi(x) \pmod{p} \quad (7)$$

then

$$(f, \alpha) \equiv (x - K_1)(x - K_2) \cdots (x - K_m)\Psi(x) \pmod{p^m}. \quad (8)$$

Furthermore if this last congruence holds, then

* Wertheim: Elemente der Zahlentheorie, Lehrsatz II, p. 124.

† H. J. S. Smith: Report on the Theory of Numbers, Collected Math. Papers, Vol. I, p. 157.

$(f, \alpha^{p-1}) \equiv (x - K_1{}^{p-1})(x - K_2{}^{p-1}) \cdots (x - K_m{}^{p-1})\Phi(x) \pmod{p^m}$; (9)
for if K is a root of $(f, \alpha) = \Pi(x - \alpha_i) \equiv 0 \pmod{M}$ then K^l is a root of $(f, \alpha^l) = \Pi(x - \alpha_i{}^l) \equiv 0 \pmod{M}$ because $\Pi(K^l - \alpha_i{}^l)$ is a multiple of $\Pi(K - \alpha_i)$ which is itself a multiple of M. From (6) and (9) we see that $\Delta_{p-1} = (f, \alpha^{p-1})_{x=1} \equiv (1 - K_1{}^{p-1})(1 - K_2{}^{p-1}) \cdots (1 - K_m{}^{p-1})\Phi(1) \pmod{p^m}$. Since each factor on the right except $\Phi(1)$ is divisible by at least the first power of p, it follows that

$$\Delta_{p-1} \equiv 0 \pmod{p^m}.$$

If m_1 of the roots K_i belong to the exponent e modulo p then $\Delta_e \equiv 0 \pmod{p^{m_1}}$, and if m_2 of the roots are such that $K^{e_1} \equiv -1 \pmod{p}$ then $S_{e_1} \equiv 0 \pmod{p^{m_2}}$.

5. **Forms of the Factors of Δ_q for the Quadratic Equation.** As already noted a Δ_m of composite subscript m is divisible by Δ_d where d is a divisor of m. In this section we shall discuss the factors of Δ_q where q is a prime.

We are able to determine the exact forms of the factors of Δ_q for the case when (1) is a quadratic equation. In other cases we may set up tentative methods whereby the factors are readily found. The case of the quadratic equation will first be considered.

Equation (1) is then an irreducible equation of the form

$$x^2 + a_1x + a_2 = 0. \tag{10}$$

A root of this equation generates a quadratic number field which is indeed a Galois field.* In this field the rational primes, exception being made of those which divide the discriminant of (10), separate into two classes according as the congruence

$$x^2 + a_1x + a_2 \equiv 0 \pmod{p}, \tag{11}$$

where p is the prime in question, has or has not real solutions. If the prime p belongs to the first class it will decompose in the quadratic number field into the product of two prime ideals whose norms are the original prime p. Thus if $(p) = \mathfrak{p}_1\mathfrak{p}_2$ then $n(\mathfrak{p}_1) = p$, $n(\mathfrak{p}_2) = p$ and also $\varphi(\mathfrak{p}_1) = p - 1$ where φ is the totient function in the quadratic field. If the prime p belongs to the second class then the ideal (p) is a prime ideal not decomposable in the field and $n(p) = p^2$, $\varphi(p) = p^2 - 1$.

If the roots of (10) are α_1 and α_2 Fermat's theorem for a prime ideal $\mathfrak{p}_1$ which divides (p), where p is a rational prime of the first class, gives

$$\alpha_1{}^{(p-1)} - 1 \equiv 0 \pmod{\mathfrak{p}_1},$$
$$\alpha_2{}^{(p-1)} - 1 \equiv 0 \pmod{\mathfrak{p}_2}.$$

* Hilbert: Jahresbericht der Deutsch. Math. Vereinigung, Vol. 4, 1894–95, Kapitel XVI.

The second modulus may be changed to $\mathfrak{p}_1$ since the conjugate fields are identical in a Galois field. Then since $\alpha_1^{p-1} - 1$ and $\alpha_2^{p-1} - 1$ are both numbers of the ideal $\mathfrak{p}_1$ their product $\Pi_{i=1,\ 2}(1 - \alpha_i^{p-1}) = \Delta_{p-1}$ is also a number of $\mathfrak{p}_1$. Now it is known that all rational numbers of $\mathfrak{p}_1$ are multiples* of the rational prime p and since $\Delta_{(p-1)}$ is a rational number of $\mathfrak{p}_1$ we may write in the ordinary sense of a congruence,

$$\Delta_{p-1} \equiv 0 \pmod{p}.$$

It is necessary now to see that the conjugate numbers α_1 and α_2 belong to the same exponent modulo the corresponding conjugate ideals $\mathfrak{p}_1$ and $\mathfrak{p}_2$ respectively. Indeed one conjugate ideal is constructed from the other by simply substituting conjugate numbers. Hence, if $\alpha_1^e \equiv 1 \pmod{\mathfrak{p}_1}$, where e is the smallest exponent for which this occurs, then $\alpha_2^e \equiv 1 \pmod{\mathfrak{p}_2}$ and we could not have $\alpha_2^{e_1} \equiv 1 \pmod{\mathfrak{p}_2}$ where $e_1 < e$ for if so we could pass back to $\mathfrak{p}_1$ by substituting α_1 for α_2 and we should have $\alpha_1^{e_1} \equiv 1 \pmod{\mathfrak{p}_1}$ contrary to hypothesis.

Since the theory of power residues for an algebraic number field is precisely similar to the ordinary theory† we see that the prime p (when not a factor of Δ_1) can only appear as a factor of those Δ's having prime subscripts for which the subscripts are divisors of $p - 1$. In particular if p is not a factor of Δ_1 but is a factor of Δ_q, where q is a prime, then $k'q = p - 1$ and therefore

$$p = k'q + 1. \tag{12}$$

Similarly for a prime p of the second class $\Delta_{p^2-1} \equiv 0 \pmod{p}$. If p is not a factor of Δ_1 but is a factor of Δ_q where q is a prime then q must divide $p^2 - 1 = (p - 1)(p + 1)$. Now q cannot divide $p - 1$, for then Δ_{p-1} would be divisible by p and congruence (11) would be solvable, which is not the case for primes of the second class. Hence q must divide $p + 1$ and therefore $kq = p + 1$. Hence $p = kq - 1$.

Combining this result with that of (12) *we see that if q is a prime number the prime factors of* Δ_q, *other than those which divide* Δ_1 *or the discriminant of* (10), *are of the forms* $kq \pm 1$.

It is remarkable to note that $-\Delta_q$ calculated for the particular quadratic equation $x^2 - 2 = 0$ is the number $2^q - 1$ and hence that the Mersenne numbers $2^q - 1$ are included among the Δ's of this equation. Similarly $-\Delta_q$ of the equation $x^2 - a = 0$ is a number of the form $a^q - 1$. The methods of factorization given above may then be applied to numbers of these forms.

6. **Forms of the factors of Δ_q for a cubic equation.** A similar situ-

* Sommer: Vorlesungen ueber Zahlentheorie, p. 59.

† Hilbert: l. c., Kapitel III, § 9.

ation to that of a quadratic equation arises when (1) is a cubic or higher degree equation. The problem here must be treated somewhat differently since here the conjugate number fields are not in general identical.

If we consider the irreducible cubic equation

$$x^3 + a_1x^2 + a_2x + a_3 = 0, \tag{13}$$

each of the roots α_1, α_2, and α_3 generates a cubic number field. The three fields thus generated are conjugate. Between these fields there is a one-to-one correspondence of ideals, the ideals of one field being obtained from those of another by substituting for the numbers of the latter the corresponding conjugate numbers of the former.* Furthermore, if $\mathfrak{a}_1$, $\mathfrak{a}_2$, and $\mathfrak{a}_3$, be three conjugate ideals the norm of each is equal to the product $\mathfrak{a}_1 \cdot \mathfrak{a}_2 \cdot \mathfrak{a}_3$, which is a principal ideal all of whose numbers are multiples of a rational integer.

The rational primes in this cubic field, other than the prime factors of the discriminant of (13), separate into three classes according as the congruence

$$x^3 + a_1x^2 + a_2x + a_3 \equiv 0 \pmod{p}, \tag{14}$$

whose modulus is the prime in question, has three real solutions, one real solution, or no real solution.†

Considering p to be a prime of the first class it decomposes in each of the three conjugate fields into the product of three prime ideals all of whose norms are equal to p. Thus

$$(p) = \mathfrak{p}_1\mathfrak{p}_2\mathfrak{p}_3, \qquad (p) = \mathfrak{p}_1'\mathfrak{p}_2'\mathfrak{p}_3', \qquad (p) = \mathfrak{p}_1''\mathfrak{p}_2''\mathfrak{p}_3'',$$
$$n(\mathfrak{p}_1) = n(\mathfrak{p}_2) = n(\mathfrak{p}_3) = n(\mathfrak{p}_1') = \text{etc.} = p,$$

$$\varphi(\mathfrak{p}_1) = n(\mathfrak{p}_1)\left(1 - \frac{1}{n(\mathfrak{p}_1)}\right) = p - 1, \qquad \varphi(\mathfrak{p}_2) = \varphi(\mathfrak{p}_3) = \varphi(\mathfrak{p}_1') = \text{etc.} = p - 1.$$

By Fermat's theorem

$$\alpha_1^{p-1} - 1 \equiv 0 \pmod{\mathfrak{p}_1},$$
$$\alpha_2^{p-1} - 1 \equiv 0 \pmod{\mathfrak{p}_1'},$$
$$\alpha_3^{p-1} - 1 \equiv 0 \pmod{\mathfrak{p}_1''}.$$

Multiplying the left-hand members together gives a number $\Pi_{i=1}^{3}(1 - \alpha_i^{p-1}) = \Delta_{p-1}$, which belongs to an ideal which is the product of the three moduli, namely $\mathfrak{p}_1\mathfrak{p}_1'\mathfrak{p}_1'' = n(\mathfrak{p}_1) = p$. Hence

$$\Delta_{p-1} \equiv 0 \pmod{p}. \tag{15}$$

Consideration of the ideals $\mathfrak{p}_2$, $\mathfrak{p}_2'$, $\mathfrak{p}_2''$ and also of $\mathfrak{p}_3$, $\mathfrak{p}_3'$, $\mathfrak{p}_3''$ yields congruence (15) again in both cases.

* Hilbert: l. c., p. 191.

† Sommer: l. c., §§ 44–46.

If the prime p is of the second class, then

$$(p) = \mathfrak{p}_1\mathfrak{p}_2, \quad (p) = \mathfrak{p}_1'\mathfrak{p}_2', \quad (p) = \mathfrak{p}_1''\mathfrak{p}_2'',$$
$$n(\mathfrak{p}_1) = n(\mathfrak{p}_1') = n(\mathfrak{p}_1'') = p, \quad n(\mathfrak{p}_2) = n(\mathfrak{p}_2') = n(\mathfrak{p}_2'') = p^2,$$
$$\varphi(\mathfrak{p}_1) = \varphi(\mathfrak{p}_1') = \varphi(\mathfrak{p}_1'') = p - 1, \quad \varphi(\mathfrak{p}_2) = \varphi(\mathfrak{p}_2') = \varphi(\mathfrak{p}_2'') = p^2 - 1.$$

Just as in the two preceding paragraphs the prime ideals $\mathfrak{p}_1$, $\mathfrak{p}_1'$, $\mathfrak{p}_1''$ yield congruence (15) again, but for $\mathfrak{p}_2$, $\mathfrak{p}_2'$, $\mathfrak{p}_2''$ we have

$$\alpha_1^{p^2-1} - 1 \equiv 0 \pmod{\mathfrak{p}_2},$$
$$\alpha_2^{p^2-1} - 1 \equiv 0 \pmod{\mathfrak{p}_2'},$$
$$\alpha_2^{p^2-1} - 1 \equiv 0 \pmod{\mathfrak{p}_2''}.$$

Multiplying together the left-hand members we see that Δ_{p^2-1} must be a number of the ideal $\mathfrak{p}_2\mathfrak{p}_2'\mathfrak{p}_2'' = n(\mathfrak{p}_2) = p^2$, hence

$$\Delta_{p^2-1} \equiv 0 \pmod{p^2}. \tag{16}$$

Finally if p be a prime number of the third class the congruence (14) is not solvable and p is not decomposable in the conjugate fields and is itself a principal ideal of these fields. The norm of (p) is p^3. Then

$$\alpha_1^{p^3-1} - 1 \equiv 0 \pmod{(p)},$$
$$\alpha_2^{p^3-1} - 1 \equiv 0 \pmod{(p)},$$
$$\alpha_3^{p^3-1} - 1 \equiv 0 \pmod{(p)},$$

and hence

$$\Delta_{p^3-1} \equiv 0 \pmod{p^3}. \tag{17}$$

In view of (15), (16), and (17) we see that if a prime p, which does not divide Δ_1 or the discriminant of (13), enters Δ_q as a factor, where q is a prime, then q must divide either $p - 1$, $p^2 - 1$, or $p^3 - 1$. *Thus* $kq + 1$ *equals either* p, p^2, *or* p^3.

When testing for prime factors of Δ, we form the even multiples of q, add unity and use as trial divisors those primes p for which $2kq + 1$ equals either p, p^2, or p^3.

The upper limit to which the form $2kq + 1$ must be calculated may be determined as follows. If a prime p_1 is a factor of Δ_q (and not a factor of Δ_1 since Δ_1 is a factor of every Δ_m), then p_1 will enter Δ_q in the first, second, or third power according as p_1 is of the first, second, or third class, and p_1 raised to the power in which it occurs will be of the form $2kq + 1$. The same will be true of a second prime which enters Δ_q. Thus $\Delta_q \div \Delta_1$ will have a decomposition such as $p_1p_2^2p_3^3p_4^2 \cdots$ where each factor as printed will be of the form $2kq + 1$. At least one of these factors will be less than the square root of $\Delta_q \div \Delta_1$, hence we calculate the values of $2kq + 1$ only as far as the square root of $\Delta_q \div \Delta_1$. We must also assure ourselves that $\Delta_q \div \Delta_1$ is not the square or the cube of a single prime.

As an illustration $\Delta_{61} \div \Delta_1$ calculated for the equation $x^3 + x + 1 = 0$ is equal to 4459734401. We form the values of $2k \cdot 61 + 1$ less than the square root of the number in question and according to the above criterion have 113 trial divisions to make. Since none of these divisions are exact we know that 4459734401 is a prime number. If we tested as trial divisors all primes less than the square root of the number above we should have to make 6,675 trials.

7. **Forms of the factors of Δ_q for the general equation.** Returning now to the general equation (1), namely,

$$f(x) = x^n + a_1x^{n-1} + a_2x^{n-2} + \cdots + a_n = 0 \tag{1}$$

it is known* that when

$$f(x) \equiv P_1^{e_1}(x)P_2^{e_2}(x) \cdots P_r^{e_r}(x) \pmod{p}, \tag{18}$$

where $P_1(x), \cdots, P_r(x)$ are prime functions of degrees $f_1, f_2, \cdots, f_r$, then p in the field generated by α has the decomposition

$$p = \mathfrak{p}_1^{e_1}\mathfrak{p}_2^{e_2} \cdots \mathfrak{p}_r^{e_r}, \tag{19}$$

where $n(\mathfrak{p}_1) = p^{f_1}, \cdots, n(\mathfrak{p}_r) = p^{f_r}$ and p has a similar decomposition in each of the conjugate fields. By a proof analogous to that given for the cubic equation,

$$\Delta_{\phi(p)} \equiv 0 \pmod{p}$$

where

$$\varphi(p) = p^{(e_1-1)f_1+(e_2-1)f_2+\cdots}(p^{f_1} - 1)(p^{f_2} - 1) \cdots.$$

If p is a divisor of Δ_q, and if it does not divide Δ_1 or the discriminant of (1), then q must be a divisor of $\varphi(p)$. Therefore q must either be equal to p (a case which we shall exclude presently) or otherwise, $kq + 1 = p^{f_i}$ and we thus have a tentative method of determining the factors of Δ_q similar to that given for quadratic and cubic equations.

The prime q can be equal to p only when it divides Δ_1, or in other words Δ_p cannot be divisible by p unless Δ_1 is divisible by p. This may be shown by proving that unless Δ_1 is divisible by p the number $\Delta_p \div \Delta_1$ is of the form $kp + 1$ and is therefore not a multiple of p. Thus for equation (1)

$$\Delta_p = 1 - \Sigma\alpha_i^p + \Sigma\alpha_i^p\alpha_j^p - \cdots.$$

We also have

$$(\Sigma\alpha_i)^p = (-a_1)^p, \qquad (\Sigma\alpha_i\alpha_j)^p = (a_2)^p, \qquad \text{etc.}$$

Hence expanding the left-hand members of these equations by the multinomial theorem and deleting integral multiples of p we obtain

$$\Sigma\alpha_i^p \equiv -a_1^p \equiv -a_1 \pmod{p}, \qquad \Sigma\alpha_i^p\alpha_j^p \equiv a_2^p \equiv a_2 \pmod{p}, \text{ etc.},$$

* Hilbert: l. c., p. 198; Bachmann: Allgemeine Arithmetik der Zahlenkoerper, p. 273.

therefore

$$\Delta_p \equiv 1 + a_1 + a_2 + \cdots + a_n \pmod{p}$$

or by § 2 we have $\Delta_p \equiv \Delta_1 \pmod{p}$. If now Δ_1 is not divisible by p then $\Delta_p/\Delta_1 \equiv 1 \pmod{p}$ or $\Delta_p/\Delta_1 = kp + 1$ as was to be proved.

If one of the prime ideals $\mathfrak{p}_i$ of (19) is of the first degree then one of the functions $P_i(x)$ of (18) is of the first degree and conversely. Under these conditions $f(x) \equiv 0 \pmod{p}$ has a real solution. We have

$$\begin{array}{lll} \alpha_1^{p-1} - 1 \equiv 0 & \pmod{\mathfrak{p}_i} \\ \alpha_2^{p-1} - 1 \equiv 0 & \pmod{\mathfrak{p}_i'} \\ \cdot \quad \cdot \quad \cdot & \cdot \quad \cdot \end{array}$$

where $\mathfrak{p}_i'$, $\mathfrak{p}_i''$, $\cdots$ are prime ideals conjugate to $\mathfrak{p}_i$. Then $\Pi(1 - \alpha_i^{p-1}) = \Delta_{p-1}$ must be a number of the ideal

$$\mathfrak{p}_i\mathfrak{p}_i'\mathfrak{p}_i'' \cdots = n(\mathfrak{p}_i) = p$$

and hence

$$\Delta_{p-1} \equiv 0 \pmod{p}.$$

This is another proof that the condition for a real solution of $f(x) \equiv 0 \pmod{p}$ is that Δ_{p-1} be divisible by p.

8. **Characteristic Factors of Δ_m.** A very similar state of affairs exists for the divisors of Δ_m where m is composite, as for the divisors of Δ_q. For simplicity we shall confine ourselves to the cubic equation; the method of argument however is applicable to an equation of any degree.

Let us consider any prime factor p of Δ_m which is not a factor by virtue of being a factor of Δ_r where r divides m; such a factor we shall call a characteristic factor of Δ_m. The prime p will be of the first, second, or third class in the number fields generated by α_1, α_2, and α_3 and $\varphi(p)$ will be equal to $p - 1$, $p^2 - 1$, or $p^3 - 1$. Furthermore since p enters Δ_m as a factor and does not divide Δ_r where r divides m then α_1, α_2, and α_3 will belong to the exponent m. Thus m must divide $p - 1$, $p^2 - 1$, or $p^3 - 1$ and hence p, p^2, or p^3 is of the form $km + 1$.

Hence the characteristic factors p of Δ_m have the property that p, p^2, or p^3 is of the form $km + 1$.