CYCLOTOMY IN THE GALOIS FIELDS

by

PATRICIA MARGARET PEARSON

A THESIS

submitted to

OREGON STATE COLLEGE

in partial fulfillment of
the requirements for the
degree of

MASTER OF ARTS

June 1951

APPROVED:

Redacted for Privacy

Professor of Mathematics

In Charge of Major

Redacted for Privacy

Head of Department of Mathematics

Redacted for Privacy

Chairman of School Graduate Committee

Redacted for Privacy

Dean of Graduate School

Date thesis is presented May 8, 1951

Typed by Helen Pfeifle

ACKNOWLEDGEMENT

The writer wishes to express her gratitude to Dr. B. W. Brewer for his guidance and patience during the preparation of this thesis.

TABLE OF CONTENTS

CYCLOTOMY IN THE GALOIS FIELDS

INTRODUCTION

The cyclotomic polynomial $g_n(x)=\prod_{d|n}(x^d - 1)^{\mu(n/d)}$ is the polynomial whose roots are the primitive nth roots of unity. Gauss (6, pp.412-436) showed the remarkable connection between this polynomial and the celebrated problem of constructing the regular polygons by straight edge and compass. Since the time of Gauss other writers have discovered many interesting and important properties of $g_n(x)$. The properties to be considered here relate to its decomposition into prime factors and to the magnitude of its coefficients; two aspects which have been studied in some detail in the rational number field and its extensions. Kronecker (8, pp.75-92) was the first to prove that $g_n(x)$ is irreducible in the rational number field. The magnitude of its coefficients in this field has been discussed by Schur, E. Lehmer (11, pp.389-392), Erdos (5, pp.179-184), and Bateman (1, pp.1180-1181). Here, these properties will be discussed in the Galois fields.

Schönemann (16, pp.269-325), Pellet (14, pp.156-167), Dickson (3, pp.1-312), and others have considered certain aspects of the decomposition of $g_n(x)$ in the Galois fields, but all of these results, with one exception to be noted later, appeared prior to Steinitz' (17, pp.1-176) famous paper of 1910 on the algebraic theory of fields which gave such impetus to the present abstract field theory. It seems worthwhile therefore to recast and extend these results on

the decomposition of $g_n(x)$ in the light of the modern theory of Galois fields. We obtain thereby several new proofs of well known theorems and some results which are apparently new. In particular, our results concerning the "magnitude" of the coefficients modulo p do not seem to appear in the literature.

CHAPTER I

FACTORIZATION

1. Factorization of the cyclotomic polynomial. As mentioned above, the cyclotomic polynomial $g_n(x)$ is irreducible in the rational number field, but in the Galois (finite) fields this is not always the case. In 1826 Schönemann (16, p.324) proved that the cyclotomic polynomial $g_q(x)$ where q is prime, $q \neq p$, factors modulo p (i.e., in the Galois field GF[p]) into (q-1)/e irreducible factors each of degree e where p belongs to e modulo q. A century later Rauter (15, p.225) generalized this in a theorem which completely describes the situation for any $g_n(x)$ and any Galois field $GF[p^m]$, subject of course to the restriction that $(n,p) = 1$. Rauter's proof was based on the theory of symmetric functions, but the somewhat simpler proof included here uses only field theory and properties of the cyclotomic polynomial. In this and following proofs, results of elementary group theory, number theory and field theory as given in MacDuffee, "Introduction to Abstract Algebra," or van der Waerden, "Modern Algebra," will be assumed. The theorem follows.

THEOREM 1. The cyclotomic polynomial $g_n(x)$ factors in $GF[p^m]$, $(n,p) = 1$, into $\phi(n)/e$ irreducible factors each of degree e where p^m belongs to e modulo n.

PROOF. Let $g_n(x) = \prod_{i=1}^{r} f_i(x)$ in $GF[p^m]$, where $f_i(x)$ is an irreducible polynomial of degree α_i, $i = 1, 2, \ldots, r$. Then the root field of $f_i(x)$ over $GF[p^m]$ is $GF[p^{m\alpha_i}]$. Thus $GF[p^{m\alpha_i}]$ contains

a primitive nth root of unity ρ , and $\rho^{p^{m\alpha_i}-1} = 1$, a condition met by every non-zero element of $GF[p^{m\alpha_i}]$. Since ρ is a primitive nth root of unity, this implies that $p^{m\alpha_i} - 1 \equiv 0 \pmod{n}$, and this in turn implies that $e|\alpha_i$, since by hypothesis p^m belongs to e modulo n.

On the other hand, the non-zero elements of $GF[p^{me}]$ form a cyclic group of order $p^{me} - 1$ with respect to multiplication, every element σ satisfying $\sigma^{p^{me}-1} = 1$, and since by hypothesis $p^{me} - 1 \equiv 0 \pmod{n}$, this group contains a cyclic subgroup of order n. But this subgroup contains at least one element of period n, a primitive nth root of unity, so that included among the elements of the subgroup are all the primitive nth roots of unity, of which α_i are roots of $f_i(x)$ by definition. Therefore $GF[p^{m\alpha_i}] \subseteq GF[p^{me}]$ and $\alpha_i | e$.

Hence $\alpha_i = e$. Since $f_i(x)$ was any one of the irreducible factors of $g_n(x)$, $\alpha_1 = \alpha_2 = \ldots = \alpha_r = e$, and consequently $r = \phi(n)/e$.

With the aid of the following lemma, this theorem may be restated in another useful form.

LEMMA 1. If $d = (\phi(n),m)$ and $(n,p) = 1$, p^m and p^d belong to the same exponent modulo n.

PROOF. Let p^m belong to e_1 and p^d belong to e_2 modulo n. The assumption $d = (\phi(n),m)$ may be written $m = k_1 d$, $\phi(n) = k_2 d$, where $(k_1,k_2) = 1$. Substitution in the known congruences $p^{me_1} \equiv 1$ and $p^{\phi(n)} \equiv 1 \pmod{n}$ yields the congruences $p^{k_1 d e_1} \equiv 1$ and $p^{k_2 d} \equiv 1$

(mod n), which imply that $e_2 | k_1 e_1$ and $e_2 | k_2$. Since $(k_1, k_2) = 1$, then $(k_1, e_2) = 1$ and $e_2 | e_1$. Further; $p^{me_2} = p^{k_1 d e_2} \equiv 1 \pmod{n}$, so that $e_1 | e_2$. Hence $e_1 = e_2$.

Thus theorem 1 may be restated: The cyclotomic polynomial $g_n(x)$ factors in $GF[p^m]$, $(n,p) = 1$, into $\phi(n)/e$ irreducible factors each of degree e, where p^d belongs to e modulo n, and $d = (\phi(n), m)$.

2. Factorization of any polynomial. A theorem about the factorization of any polynomial irreducible in a particular Galois field in finite extensions of that field can be proved as a result of theorem 1. This theorem was given by Dickson (3, p.33) who noted that the case for f(x) irreducible in GF[p] was stated without proof by Pellet in 1870.

THEOREM 2. A polynomial f(x) of degree u irreducible in $GF[p^m]$ factors in $GF[p^{mv}]$ into δ irreducible factors each of degree u/δ, where $\delta = (u, v)$.

The proof given here is again much shorter than Dickson's proof. One lemma makes this theorem a direct result of theorem 1.

LEMMA 2. If p^m belongs to e modulo n, then p^{ms} belongs to e/δ modulo n, where $\delta = (e,s)$.

PROOF. Assume $(p^{ms})^r \equiv 1 \pmod{n}$, where $r < e/\delta$. Then $e | sr$, since p^m belongs to e modulo n. Since $e | sr$ and $s | sr$, $[e,s] | sr$ by definition of least common multiple. But $[e,s] = es/(e,s) = es/\delta$. Therefore $es/\delta | sr$ and $e/\delta | r$, contrary to the hypothesis that $r < e/\delta$. Obviously $(p^{ms})^{e/\delta} \equiv 1 \pmod{n}$. Hence p^{ms} belongs to e/δ modulo n.

PROOF OF THEOREM 2. Now f(x) is an irreducible factor of some $g_n(x)$ in $GF[p^m]$, since every non-null element of a Galois field is a root of unity. By theorem 1, p^m belongs to u modulo n, and by lemma 2, p^{mv} belongs to u/δ modulo n. Then again by theorem 1, $g_n(x)$ factors in $GF[p^{mv}]$ into irreducible factors each of degree u/δ. But these must include the irreducible factors of f(x). Thus f(x) factors into δ irreducible factors each of degree u/δ.

3. The irreducible case. It is evident from theorem 1 that a necessary and sufficient condition for $g_n(x)$ to be irreducible in $GF[p^m]$ is that p^m belong to $\phi(n)$ modulo n, i.e., that p^m be a primitive root modulo n. Some facts about the number of fields in which $g_n(x)$ is irreducible or reducible may be discovered by examining this condition more closely. It is known that n has a primitive root if and only if it is of the form 2, 4, q^r, or $2q^r$, where q is an odd prime (4, p.33). Thus unless n has one of these forms, $g_n(x)$ is reducible in every $GF[p^m]$. Consider now an n which has at least one primitive root. It remains to be shown that such an n has at least one prime or prime power primitive root. Let r be a primitive root of n. Then (r,n) = 1 and the numbers $s \equiv r \pmod{n}$ are also primitive roots. But by Dirichlet's theorem (9, p.96) there is an infinite number of primes among the numbers congruent to r modulo n, and thus an infinite number of GF[p] in which $g_n(x)$ is irreducible. Obviously $g_2(x)$ is always irreducible. For n of the other three types there is also an infinite number of GF[p] in which $g_n(x)$ is

reducible, since among the numbers $s \equiv 1 \pmod{n}$ there is an infinite number of primes which are not primitive roots of n. If p belongs to e modulo n, then $p^{e+1} \equiv p \pmod{n}$ and p^{e+1} is or is not a primitive root of n according as p is or is not a primitive root. Thus there is an infinite number of $GF[p^m]$ in which $g_n(x)$ is irreducible and an infinite number in which $g_n(x)$ is reducible for $m > 1$ as well as for $m = 1$. These results may be summarized in a theorem.

THEOREM 3. If n is 4, q^r, or $2q^r$, where q is an odd prime, $g_n(x)$ is irreducible in an infinite number of $GF[p^m]$ and reducible in an infinite number of $GF[p^m]$. The $g_2(x)$ is always irreducible. All other $g_n(x)$ are reducible in every $GF[p^m]$.

4. Distribution of roots. Another question of interest regarding the factorization of the cyclotomic polynomial is that of the distribution of the roots among the factors. If ρ is a primitive nth root of unity, it is well known that the other primitive nth roots are $\rho^{r_1}, \rho^{r_2}, \ldots, \rho^{r_{\phi(n)-1}}$, where $1 < r_i < n$, $(r_i, n) = 1$ for $i = 1, 2, \ldots, \phi(n)-1$. Now if $g_n(x)$ factors in $GF[p^m]$ into $\phi(n)/e$ irreducible factors, i.e., $g_n(x) = \prod_{i=1}^{\phi(n)/e} f_i(x)$, and ρ is one root of $f_1(x)$, which of the powers of ρ will be included among the roots of $f_1(x)$, which will be included among those of $f_2(x)$, etc.? The answer to this question is contained in the following theorem.

THEOREM 4. If $g_n(x) = \prod_{i=1}^{\phi(n)/e} f_i(x)$ where $f_i(x)$ is irreducible

of degree e in $GF[p^m]$, and if all the roots of $g_n(x)$ are expressed as powers of a single root ρ, then the roots are distributed among the factors in sets of e roots each such that set-wise, the exponents of the powers to which ρ is raised are the $\phi(n)/e$ cosets of the group of reduced residues modulo n relative to the cyclic group generated by p^d, where $d = (\phi(n), m)$.

PROOF. By theorem 1, p^d belongs to e modulo n. Then $f_1(x)$ factors in $GF[p^{me}]$ into $(x - \rho)(x - \rho^{p^d})(x - \rho^{p^{2d}}) \ldots (x - \rho^{p^{(e-1)d}})$, where ρ is any root of $f_1(x)$ (7, p.136). As noted above, the other roots of $g_n(x)$ are ρ^{r_1}, ρ^{r_2}, ..., $\rho^{r_{\phi(n)-1}}$. Pick any one of these, say ρ^{s_2}, which does not appear in $f_1(x)$, and call the factor of which it is a root $f_2(x)$. Then $f_2(x)$ factors in $GF[p^{me}]$ thus: $f_2(x) = (x - \rho^{s_2})(x - \rho^{s_2 p^d}) \ldots (x - \rho^{s_2 p^{(e-1)d}})$. Similarly choose another ρ^{s_3} which does not appear in $f_1(x)$ or $f_2(x)$ and call the factor of which it is a root $f_3(x)$. Then $f_3(x) = (x - \rho^{s_3})(x - \rho^{s_3 p^d}) \ldots (x - \rho^{s_3 p^{(e-1)d}})$. The process may be continued until all $\phi(n)/e$ of the factors have been accounted for. Now the exponents $1, r_1, r_2, \ldots, r_{\phi(n)-1}$ form a reduced set of residues modulo n, and thus an Abelian group $G_{\phi(n)}$ with respect to multiplication and reduction modulo n. The exponents $1, p^d, \ldots, p^{(e-1)d}$ are a subset of $G_{\phi(n)}$, and this subset is in fact a cyclic subgroup, G_e, since p^d belongs to e modulo n. The sets of exponents:

$$1,\ p^d,\ p^{2d},\ \ldots,\ p^{(e-1)d}$$
$$s_2,\ s_2p^d,\ s_2p^{2d},\ \ldots\ s_2p^{(e-1)d}$$
$$\ldots\ldots$$
$$s_{\phi(n)/e},\ s_{\phi(n)/e}p^d,\ \ldots,\ s_{\phi(n)/e}p^{(e-1)d}$$

thus are the $\phi(n)/e$ cosets of $G_{\phi(n)}$ relative to G_e.

Since the factorization of $g_q(x)$, for q an odd prime, into two irreducible factors modulo p will be investigated in some detail in the next chapter, it is of interest to apply theorem 4 to this case. By theorem 1, $g_q(x)$ factors in GF[p] into two irreducible factors if and only if p belongs to $\phi(q)/2$ which equals $(q-1)/2$, since q is prime. This implies that p must be a quadratic residue of q. By theorem 4 the roots of one factor are $\rho, \rho^p, \rho^{p^2}, \ldots, \rho^{p^{(q-3)/2}}$ and the roots of the other are $\rho^s, \rho^{sp}, \rho^{sp^2}, \ldots, \rho^{sp^{(q-3)/2}}$. But since p is a quadratic residue of q, the numbers $1, p, p^2, \ldots, p^{(q-3)/2}$ are the quadratic residues, and the exponents of the powers of ρ in the other factor are the quadratic non-residues of q. This result may be stated as a corollary to theorem 4.

COROLLARY 1. If the cyclotomic polynomial $g_q(x)$, with q prime, factors in GF[p] into two irreducible factors of equal degree, and if all the roots of $g_q(x)$ are expressed as powers of a single root ρ, then the exponents of the powers to which ρ is raised are divided between the factors so that the quadratic residues of q appear as exponents in one factor, the quadratic non-residues in the other.

CHAPTER II

COEFFICIENTS

5. The coefficients of $g_n(x)$. As noted in the introduction, the magnitude of the coefficients of the cyclotomic polynomial $g_n(x)$ in the rational number field has been studied by several writers. It was first shown by Schur in a letter to Landau that there exist cyclotomic polynomials with coefficients arbitrarily large in absolute value. The proof for this theorem together with another theorem restricting n to the product of three distinct primes was published by E. Lehmer in 1936 (11, pp.389-392). More recently Erdös (5, pp.179-184) and Bateman (1, pp.1180-1181) have extended these results.

Of course, magnitude is meaningless in the Galois fields. But we may ask under what conditions $g_n(x)$ and its irreducible factors will have coefficients different from 0 or $\pm$ 1 modulo p, and this problem will be considered here.

We first ask the following question: For a given prime p, is there a $g_n(x)$ with some coefficient which is not congruent to 0 or $\pm$ 1 modulo p? This question can be answered in the affirmative, and fortunately the above-mentioned proof of Schur's theorem needs to be modified only slightly to serve as a proof for this theorem.

THEOREM 5. Given any prime $p > 3$, there exists a $g_n(x)$ with at least one coefficient $a_i \not\equiv 0$ or $\pm 1 \pmod{p}$.

First a statement used by E. Lehmer without proof will here

be proved as a lemma.

LEMMA 3. For any odd number t, there exists a set of odd primes $p_1 < p_2 < \ldots < p_t$ such that $p_1 + p_2 > p_t$.

PROOF. The proof of this lemma depends on the following theorem from number theory. "For any positive $\epsilon > 0$, there exists a positive integer N such that for $x \geq N$ there is at least one prime between x and $(1 + \epsilon)x$ (2, p.436). Choose $\epsilon = 2^{1/(t-1)} - 1$. This determines an N such that for $x \geq N$, there is at least one prime between x and $2^{1/(t-1)}x$. Let p_1 be the first prime greater than or equal to N. There exists at least one prime between p_1 and $2^{1/(t-1)}p_1$, and call one of these p_2. Similarly there exists at least one prime between $2^{1/(t-1)}p_1$ and $2^{2/(t-1)}p_1$. Let one of these be p_3. If this process is continued, a set of primes $p_1, p_2, \ldots, p_t$ is obtained such that $p_1 < p_2 < 2^{1/(t-1)}p_1 < p_3 < 2^{2/(t-1)}p_1 < p_4 < \ldots < 2^{(t-2)/(t-1)}p_1 < p_t < 2^{(t-1)/(t-1)}p_1 = 2p_1$. These primes satisfy the first condition. Furthermore $p_1 + p_2 > 2p_1 > p_t$, so this is a set of primes with the desired properties.

Note: The above proof will not be affected if p_1 is chosen greater than p, so that such a set of primes which does not include p can always be found.

PROOF OF THEOREM 5. Let $n = p_1p_2 \ldots p_t$, where t is odd with $p_1 < p_2 < \ldots < p_t$ being odd primes such that $p_1 + p_2 > p_t$ and $p_1 > p$ as in the lemma. Since the coefficient of x^{p_t} in $g_n(x)$ is to be considered, $g_n(x)$ will be reduced modulo x^{p_t+1}. The cyclotomic polynomial can be expanded by the formula $g_n(x) = \prod_{d|n}(x^d-1)^{\mu(n/d)}$

where $\mu(k)$ is the Mobius function defined as follows:

$$\mu(k) = \begin{cases} 0 & \text{, if } p^2 \mid k \text{ for any } p \\ (-1)^{\lambda} & \text{, if } k = p_1 p_2 \cdots p_\lambda \text{ (i.e., if } p \text{ is square-free)} \\ 1 & \text{, if } k = 1 \end{cases}$$

The divisors of n besides 1 are numbers of the form $p_{i_1} p_{i_2} \cdots p_{i_k}$, where the subscripts are some k of the numbers 1, 2, ..., t, and $k = 1, 2, \ldots, t$. Thus the product may be written: $\prod_{d \mid n} (x^d - 1)^{\mu(n/d)} =$

$$(x^1 - 1)^{\mu(n)} \prod_{i=1}^{t} (x^{p_i} - 1)^{\mu(n/p_i)} \prod_{k \geq 2} (x^{p_{i_1} p_{i_2} \cdots p_{i_k}} - 1)^{\mu(n/p_{i_1} \cdots p_{i_k})} .$$

Since $n = p_1 p_2 \cdots p_t$, $n/p_{i_1} p_{i_2} \cdots p_{i_k}$ is the product of an even or odd number of primes according as k is odd or even, and $\mu(n/p_{i_1} p_{i_2} \cdots p_{i_k}) = \pm 1$ according as k is odd or even. Therefore we may write

$$\prod_{\substack{k \geq 2 \\ k \text{ even}}} (x^{p_{i_1} p_{i_2} \cdots p_{i_k}} - 1)\, g_n(x)$$

$$= (x-1)^{\mu(n)} \prod_{i=1}^{t} (x^{p_i} - 1)^{\mu(n/p_i)} \prod_{\substack{k \geq 2 \\ k \text{ odd}}} (x^{p_{i_1} p_{i_2} \cdots p_{i_k}} - 1).$$

Now by hypothesis, $p_1 + p_2 > p_t$, and $p_1 < p_2 < \cdots < p_t$. Thus $d = p_{i_1} p_{i_2} \cdots p_{i_k} > p_t$ for all $k \geq 2$. Furthermore there is an even number of such divisors of n, and the above identity reduces modulo x^{p_t+1} to the following:

$$g_n(x) \equiv (x-1)^{\mu(n)} \prod_{i=1}^{t} (x^{p_i} - 1)^{\mu(n/p_i)} \pmod{x^{p_t+1}}$$

Since n is the product of an odd number of primes, $\mu(n) = -1$ and

$\mu(n/p_i) = 1$. Thus

$$g_n(x) \equiv \prod_{i=1}^{t} \frac{(x^{p_i}-1)}{(x-1)} \pmod{x^{p_t+1}}.$$

Division of $(x^{p_t}-1)$ by $(x-1)$ gives:

$$g_n(x) \equiv (x^{p_t-1} + x^{p_t-2} + \ldots + x+1)\prod_{i=1}^{t-1}(x^{p_i}-1) \pmod{x^{p_t+1}}.$$

Then if the product $\prod_{i=1}^{t-1}(x^{p_i}-1)$ is expanded, all terms $x^{p_{i_1}+p_{i_2}+\ldots+p_{i_k}}$, where $k \geq 2$, are divisible by x^{p_t+1} since by definition $p_{i_1} + p_{i_2} + \ldots + p_{i_k} > p_t$ for $k \geq 2$. Therefore the congruence may be written:

$$g_n(x) \equiv (x^{p_t-1} + x^{p_t-2} + \ldots + x+1)(1 - x^{p_1} - x^{p_2} - \ldots - x^{p_{t-1}}) \pmod{x^{p_t+1}}.$$

It is now evident that if this product is expanded, the coefficient of x^{p_t} will be $-(t-1) = 1 - t$. Since $g_n(x)$ is to be considered modulo p, it remains to be shown that for every prime $p > 3$ there exists an odd number t such that $1 - t \not\equiv 0$ or $\pm 1 \pmod{p}$. It suffices to take $t = p - 2$, for certainly $p - 2$ is odd if p is an odd prime, and $1 - (p - 2) = 3 - p \not\equiv 0$ or $\pm 1 \pmod{p}$ for $p > 3$. Thus $g_{p_1 p_2 \ldots p_t}(x)$ is the desired polynomial. The condition $(n,p) = 1$ was satisfied at the outset since p_1 was taken greater than p.

An extension of lemma 3 leads to the following corollary.

COROLLARY 2. For any prime $p > 3$ there is an infinite number of cyclotomic polynomials with at least one coefficient $a_i \not\equiv 0$ or $\pm 1 \pmod{p}$.

PROOF. In lemma 3, p_1 could have been chosen as any one of the infinite number of primes equal to or greater than N_1 and p, rather than the first such prime. Then a set of t primes could be generated from each p_1 as in the lemma, the sets being distinct since their smallest elements are distinct. Thus for any odd number t, there exists not just one, but an infinite number of distinct sets of odd primes $p_1 < p_2 < \ldots < p_t$. Hence for each t there is an infinite number of n, defined as above from the sets of primes, such that the coefficient of x^{p_t} in $g_n(x)$ is 1 - t, which can be chosen $\not\equiv 0$ or ± 1 modulo p as shown in the theorem.

It is interesting to note that any $g_n(x)$ which does contain such a coefficient is reducible modulo p, for every p. The following theorem establishes this fact.

THEOREM 6. If $g_n(x)$ is irreducible modulo p, every coefficient is 0 or ± 1.

PROOF. As noted before, $g_n(x)$ can be irreducible modulo p only if n is 2, 4, q^r, or $2q^r$, where q is an odd prime. The theorem is satisfied for n = 2 and n = 4, since $g_2(x) = x + 1$, and $g_4(x) = x^2 + 1$. Furthermore, $g_{q^r}(x) = 1 + x^{q^r-1} + x^{2q^r-1} + \ldots + x^{(q-1)q^r-1}$ (18, p.115). From the fact that $g_{2n}(x) = g_n(-x)$ for odd n (10, p.73) it follows that

$$q_{2q^r}(x) = g_{q^r}(-x) = 1 + (-x)^{q^r-1} + (-x)^{2q^r-1} + \ldots + (-x)^{(q-1)q^r-1}.$$

Thus in every case the coefficients are 0 or ± 1.

6. The coefficients in the irreducible factors of $g_n(x)$. Let now $g_n(x)$, $n > 2$, be irreducible in $GF[p]$. Then all the coefficients of $g_n(x)$ are 0 or ± 1. However, according to theorem 3, $g_n(x)$ will be reducible in $GF[q_i]$ for a certain infinite set of q_i ($i = 1, 2, \ldots$). If $g_n(x)$ is completely reducible in $GF[q_i]$ ($q_i > 3$), each linear factor of $g_n(x)$ will contain a coefficient different from 0 or ± 1. Between the two extremes of irreducibility and factorization into linear factors one may ask if there can be a factorization of $g_n(x)$ into two or more irreducible factors in some $GF[q_i]$ ($q_i > 3$) such that all of the coefficients in these factors are 0 or ± 1. Evidently no such factorization is possible for $g_4(x)$. Some interesting results bearing on this question will be obtained for the case of factorization into two irreducible factors of equal degree, but a complete answer to the question will not be given. A lemma will first be proved.

LEMMA 4. Let $g_n(x)$ be irreducible in $GF[p]$. Then there exists an infinite number of primes q_i such that $g_n(x)$ factors into two irreducible factors of equal degree in $GF[q_i]$.

PROOF. Since $g_n(x)$ is irreducible in $GF[p]$, p belongs to $\phi(n)$ modulo n. Then p^2 belongs to $\phi(n)/2$ modulo n. But $(p^2, n) = 1$, so among the numbers $s \equiv p^2 \pmod{n}$ there is an infinite number of primes which belong to $\phi(n)/2$ modulo n by Dirichlet's theorem. Thus by theorem 1 there is an infinite number of q_i such that $g_n(x)$ factors into two irreducible factors of equal degree in $GF[q_i]$.

We may now prove the following theorem.

THEOREM 7. Let $g_n(x)$ be irreducible in GF[p] and let q_i ($i = 1, 2, \ldots$) be the set of primes such that $g_n(x)$ factors into two irreducible factors of equal degree in GF[q_i]. Then for almost all q_i, a coefficient different from 0 or ± 1 appears in at least one factor.

PROOF. By lemma 4 the set of primes q_i is infinite. Let q_k be one of the q_i's such that $q_k > 2 + \phi(n)/2$ and assume that all coefficients in the two irreducible factors of equal degree of $g_n(x)$ in GF[q_k] are 0 or ± 1. Let the two factors be:

$$f_1(x) = x^{\phi(n)/2} + c_1 x^{\phi(n)/2-1} + \ldots + c_{\phi(n)/2}$$

and

$$f_2(x) = x^{\phi(n)/2} + c_1' x^{\phi(n)/2-1} + \ldots + c_{\phi(n)/2}'.$$

Now by theorem 6, all coefficients in $g_n(x)$ are 0 or ± 1. Thus all the sums of products of the coefficients in $f_1(x)$ and $f_2(x)$ obtained by multiplying together these two factors and collecting the coefficients of each power of x, must be congruent to 0 or ± 1 modulo q_k. If every such sum were equal to 0 or ± 1 before reduction modulo q_k, this would give a factorization in the rational number field as well as in GF[q_k]. But as noted previously $g_n(x)$ is irreducible in the rational number field, and hence this is not possible. Thus at least one sum of products must equal rq_k or $rq_k \pm 1$, $r \neq 0$. The largest possible value for such a sum of products will be obtained when every coefficient is +1. In multiplying $f_1(x)$ $f_2(x)$, the coefficient of $x^{\phi(n)/2}$ in the product will be

$$c'_{\phi(n)/2} + c_1 c'_{\phi(n)2-1} + \cdots + c_{\phi(n)/2} = 1 + \phi(n)/2,$$

and this is the largest since any other contains fewer products. But $1 + \phi(n)/2$ cannot be of the form rq_k or $rq_k \pm 1$ $(r \neq 0)$, since q_k was chosen greater than $2 + \phi(n)/2$. Since all but a finite number of the q_i are greater than $2 + \phi(n)/2$, the theorem is proved.

The case for prime n will now be examined more closely. Corollary 1, regarding distribution of roots in factors suggests use of the quadratic period equation. The $(q-1)/2$ - nomial periods, η and η', of the cyclotomic polynomial $g_q(x)$, for q an odd prime, are defined as: $\eta = \sum_a \rho^a$, $\eta' = \sum_b \rho^b$, where ρ is a primitive qth root of unity and a ranges over the quadratic residues, b over the quadratic non-residues of q. Gauss showed that the $(q-1)/2$ - nomial periods of $g_q(x)$ are the roots of the quadratic equation $x^2 + x + (1 - (-1|q)q)/4 = 0$ (19, p.128).

According to the above-mentioned corollary, when $g_q(x)$ factors into two irreducible factors of equal degree, η is the sum of the roots of one factor, η' is the sum of the roots of the other. Thus if $g_q(x)$ factors into two irreducible factors of equal degree in GF[p], the relations between the roots and coefficients in a polynomial show that η and η' are also elements of GF[p]. The complete connection between the factorization of $g_n(x)$ and of the quadratic period equation is established in the following theorem which is a special case of a theorem proved by Pellet (14, pp.156-167).

THEOREM 8. The cyclotomic polynomial $g_q(x)$ with q an odd prime, $q \neq p$, factors into two factors of equal degree in GF[p] if and only if the quadratic period equation $x^2 + x + (1 - (-1|q)q)/4 = 0$ is reducible in GF[p].

PROOF. Let p belong to e modulo q. Then $g_q(x)$ factors into two factors of equal degree if and only if $(q-1)/e$ is even, i.e., $(q-1)/e = 2k$. But $(q-1)/e = 2k$ if and only if $(p|q) = 1$.

On the other hand, a necessary and sufficient condition for reducibility of the period equation $x^2 + x + (1 - (-1|q)q)/4 = 0$ in GF[p] is that $(-1|q)q$ be a quadratic residue of p, since by hypothesis $q \not\equiv 0 \pmod{p}$. Now $((-1|q)q|p) = ((-1)^{(q-1)/2}\, q|p) = (-1)^{(q-1)/2\cdot(p-1)/2}(q|p)$. But by the quadratic reciprocity law, $(p|q) = (-1)^{(q-1)/2\cdot(p-1)/2}(q|p)$. Thus $(p|q) = ((-1|q)q|p)$ which establishes the theorem.

In the case $g_q(x) = f_1(x)f_2(x)$ in GF[p], where $f_1(x)$ and $f_2(x)$ are irreducible, it is possible to find the coefficients in the factors by using Newton's identities. Since q is prime, $g_q(x) = x^{q-1} + x^{q-2} + \ldots + x+1$, and we have in GF[p];

$$g_q(x) = (x^{(q-1)/2} + c_1x^{(q-1)/2-1} + \ldots + c_{(q-1)/2})$$
$$\cdot (x^{(q-1)/2} + c_1'x^{(q-1)/2-1} + \ldots + c_{(q-1)/2}').$$

Now if $f(x) = x^n + a_1x^{n-1} + a_2x^{n-2} + \ldots + a_{n-1}x + a_n$ in GF[p] and has roots $x_1, x_2, \ldots, x_n$, then Newton's identities are:

$$a_1 = -s_1$$
$$2a_2 = -(s_2 + s_1a_1)$$
$$3a_3 = -(s_3 + s_2a_1 + s_1a_2)$$
$$\cdots\cdots$$
$$ia_i = -(s_i + s_{i-1}a_1 + s_{i-2}a_2 + \cdots + s_1a_{i-1})$$

where $s_j = \sum_{k=1}^{n} x_k^j$ $(j = 1, 2, \ldots, n)$.

Thus in order to find the coefficients, it is necessary to find $s_1, s_2, \ldots, s_{(q-1)/2}$ for each factor. As noted above, η is the sum of the roots in one factor, while η' is the sum of the roots in the other. Thus $s_1 = \eta$ and $s_1' = \eta'$. Furthermore, by definition $s_j = \sum_a \rho^{ja}$, where ρ is a primitive qth root of unity and a ranges over the quadratic residues of q. But $\sum_a \rho^{ja} = \eta$ or η' according as $(j|q) = \pm 1$, since $(ja|q) = (j|q)(a|q) = (j|q)$. Similarly $s_j' = \eta'$ or η according as $(j|q) = \pm 1$. Solution of the quadratic period equation gives η and η', and therefore the sums of the powers of the roots for each factor. The values for these sums may then be substituted in the identities and the coefficients determined successively. An obvious defect of this method appears when $(q-1)/2 > p$, for the equation $pc_p = -(s_p + s_{p-1}c_1 + \cdots + s_1c_{p-1})$ cannot be solved in GF[p]. In a particular case it seems possible to leave this coefficient undetermined until restrictions placed on it in finding other coefficients or in multiplying the two factors together define it. However, at best the determining equations are complicated and the proof that c_p can always be found in this way

is not evident.

An identity due to Gauss, which is true in the rational number field R, makes it possible to circumvent this difficulty. The identity states that for q an odd prime, $4g_q(x) = \phi^2(x) - (-1|q)q\,\psi^2(x)$, where $\phi(x)$ and $\psi(x)$ are polynomials with integral coefficients. More useful for the present purposes is another relationship used by Mathews (13, pp.215-219) in proving the above. That is, if $g_q(x) = f_1(x)\, f_2(x)$ in $R(\rho)$, where $f_1(x)$ has roots $\rho^{a_1}, \rho^{a_2}, \ldots, \rho^{a(q-1)/2}$, $f_2(x)$ has roots $\rho^{b_1}, \rho^{b_2}, \ldots, \rho^{b(q-1)/2}$, with $(a_i|q) = 1 = -(b_i|q)$, then

$$f_1(x) = \phi_1(x) + \eta\,\phi_2(x), \quad f_2(x) = \phi_1(x) + \eta'\,\phi_2(x),$$

where $\phi_1(x)$ and $\phi_2(x)$ are polynomials with integral coefficients. That is, the coefficients of f_1 and f_2 can be found by Newton's identities as polynomials in η and η' with integral coefficients independent of p. Then solving the period equation modulo p, substituting these values, and reducing the coefficients modulo p gives the coefficients of the factors in GF[p] without the necessity for finding inverses which caused difficulty in the first method. An example may help to clarify these two methods.

Consider $g_{11}(x) \equiv 0 \pmod 5$. Since 5 belongs to (11-1)/2 = 5 modulo 5, $g_{11}(x)$ factors in GF[5] into two irreducible factors each of degree 5. The quadratic period equation is $x^2 + x + (1 - (-1|11)11)/4 = 0$ which reduces to $x^2 + x + 3 = 0$. Solving this equation modulo 5 gives $\eta \equiv 1$, $\eta' \equiv 3 \pmod 5$. The numbers 1, 3, 4, 5 are quadratic residues of 11 and 2 is a non-residue.

Following the procedure of the first method:

$s_1 \equiv 1 \quad c_1 \equiv -1 \quad s_1' \equiv 3 \quad c_1' \equiv 2$

$s_2 \equiv 3 \quad c_2 \equiv -1 \quad s_2' \equiv 1 \quad c_2' \equiv -1$

$s_3 \equiv 1 \quad c_3 \equiv 1 \quad s_3' \equiv 3 \quad c_3' \equiv 1$

$s_4 \equiv 1 \quad c_4 \equiv -2 \quad s_4' \equiv 3 \quad c_4' \equiv 1$

$s_5 \equiv 1 \quad c_5 \equiv c_5 \quad s_5' \equiv 3 \quad c_5' \equiv c_5' \pmod 5$

where the values for the coefficients are determined successively from Newton's identities. Since $g_{11}(x) = x^{10} + x^9 + \ldots + x+1$, the two factors $x^5 - x^4 - x^3 + x^2 - 2x + c_5$ and $x^5 + 2x^4 - x^3 + x^2 + x + c_5'$ can be multiplied together and the undetermined coefficients defined. The equations which result are $c_5 + c_5' \equiv 3$ and $c_5 c_5' \equiv 1 \pmod 5$. Solving these gives $c_5 \equiv c_5' \equiv -1 \pmod 5$. Therefore $g_{11}(x) \equiv (x^5 - x^4 - x^3 + x^2 - 2x - 1)(x^5 + 2x^4 - x^3 + x^2 + x - 1) \pmod 5$.

Following the procedure of the second method, substitution for η and η' will not be made immediately. Use will be made of the fact that η and η' are the two roots of the equation $x^2 + x + 3 = 0$, thus that $\eta + \eta' = -1$ and $\eta\eta' = 3$.

$s_1 = \eta \quad c_1 = -\eta$

$s_2 = \eta' \quad c_2 = -(1/2)(\eta' - \eta^2) = -1$

$s_3 = \eta \quad c_3 = -(1/3)(\eta - \eta\eta' - \eta) = 1$

$s_4 = \eta \quad c_4 = -(1/4)(\eta - \eta^2 - \eta' + \eta) = -(\eta + 1)$

$s_5 = \eta \quad c_5 = -(1/5)(\eta - \eta^2 - \eta + \eta' - \eta^2 - \eta) = -1.$

Substituting η' for η throughout gives values for the coefficients in the other factor immediately.

$$s_1' = \eta' \qquad c_1' = -\eta'$$
$$s_2' = \eta \qquad c_2' = -1$$
$$s_3' = \eta' \qquad c_3' = 1$$
$$s_4' = \eta' \qquad c_4' = -(\eta' + 1)$$
$$s_5' = \eta' \qquad c_5' = -1$$

Now substituting for η and η' their values modulo 5, and reducing the coefficients gives the following factors:

$g_{11}(x) \equiv (x^5 - x^4 - x^3 + x^2 - 2x - 1)(x^5 + 2x^4 - x^3 + x^2 + x - 1) \pmod 5$.

These are exactly the same as those obtained by the first method.

The following theorem shortens considerably the work involved in finding the coefficients.

THEOREM 9. Let

$$g_q(x) = (x^{(q-1)/2} + c_1 x^{(q-1)/2-1} + \ldots + c_{(q-1)/2}) \cdot (x^{(q-1)/2} + c_1' x^{(q-1)/2-1} + \ldots + c_{(q-1)/2}')$$

where the roots of one factor are $\rho^{a_1}, \ldots, \rho^{a_{(q-1)/2}}$, and the roots of the other are $\rho^{b_1}, \ldots, \rho^{b_{(q-1)/2}}$ with $(a_i | q) = 1 = -(b_i | q)$, $(i = 1, 2, \ldots, (q-1)/2)$. Then if $q = 4k + 1$, $c_{(q-1)/2} = c'_{(q-1)/2} = 1$, $c_r = c_{(q-1)/2-r}$, and $c_r' = c'_{(q-1)/2-r}$, $(r = 1, 2, \ldots, (q-3)/2)$. If $q = 4k - 1$, $c_{(q-1)/2} = c'_{(q-1)/2} = -1$, and $c_r = -c'_{(q-1)/2-r}$, $(r = 1, 2, \ldots, (q-3)/2)$.

PROOF. (a) Let $q = 4k + 1$. By the relations between roots and coefficients in a polynomial,

$$c_s = (-1)^s \sum \rho^{a_{i_1}} \rho^{a_{i_2}} \ldots \rho^{a_{i_s}} = (-1)^s \sum \rho^{a_{i_1} + \ldots + a_{i_s}},$$

where $i_1, i_2, \ldots, i_s$ range over all possible combinations of the

integers 1, 2, ..., (q-1)/2 taken s at a time. Similarly

$$c'_s = (-1)^s \sum \rho^{b_{i_1}+\ldots+b_{i_s}}.$$

Thus

$$c_{(q-1)/2} = (-1)^{(q-1)/2} \sum \rho^{a_1+a_2+\ldots+a_{(q-1)/2}} = \rho^{a_1+a_2+\ldots+a_{(q-1)/2}}$$

since (q-1)/2 is even and the sum contains just one term. But

$$\sum_{i=1}^{(q-1)/2} a_i \equiv \sum_{i=1}^{(q-1)/2} b_i \equiv 0 \pmod{q}.$$

Therefore $c_{(q-1)/2} = \rho^0 = 1$. In the same manner $c'_{(q-1)/2} = 1$.

Now consider

$$c_r - c_{(q-1)/2-r} = (-1)^r \sum \rho^{a_{i_1}+\ldots+a_{i_r}} - (-1)^{(q-1)/2-r} \cdot \sum \rho^{a_{i_1}+\ldots+a_{i_{(q-1)/2-r}}}.$$

Since (q-1)/2 is even, $(-1)^r = (-1)^{(q-1)/2-r}$, and therefore

$$c_r - c_{(q-1)/2-r} = (-1)^r \left(\sum \rho^{a_{i_1}+\ldots+a_{i_r}} - \sum \rho^{a_{i_1}+\ldots+a_{i_{(q-1)/2-r}}}\right).$$

From the fact that $\sum_{i=1}^{(q-1)/2} a_i \equiv 0 \pmod{q}$, each exponent

$a_{i_1} + \ldots + a_{i_{(q-1)/2-r}}$ in the second sum may be replaced by the negative of the remaining r a's. Thus

$$c_r - c_{(q-1)/2-r} = (-1)^r \left(\sum \rho^{a_{i_1}+\ldots+a_{i_r}} - \sum \rho^{-(a_{i_1}+\ldots+a_{i_r})}\right).$$

Since $(-1|q) = +1$ for $q = 4k + 1$,

$$\rho^{-(a_{i_1}+\ldots+a_{i_r})} = \rho^{a_{i_1}+\ldots+a_{i_r}}.$$

Hence

$$c_r - c_{(q-1)/2-r} = (-1)^r \left(\sum \rho^{a_{i_1}+\ldots+a_{i_r}} - \sum \rho^{a_{i_1}+\ldots+a_{i_r}}\right) = 0.$$

The proof that $c'_r = c'_{(q-1)/2-r}$ follows directly from the above if b's

are everywhere substituted for a's.

(b) Let $q = 4k - 1$. As before

$$c_{(q-1)/2} = (-1)^{(q-1)/2} \sum \rho^{a_1+a_2+\ldots+a_{(q-1)/2}}.$$

But now $(q-1)/2$ is odd, so $(-1)^{(q-1)/2} = -1$. Hence

$$c_{(q-1)/2} = c'_{(q-1)/2} = -1.$$

Consider

$$c_r + c'_{(q-1)/2-r} = (-1)^r \sum \rho^{a_{i_1}+\ldots+a_{i_r}} + (-1)^{(q-1)/2-r} \sum \rho^{b_{i_1}+\ldots+b_{i_{(q-1)/2-r}}}.$$

Since $(q-1)/2$ is odd, $(-1)^r = -(-1)^{(q-1)/2-r}$, so that

$$c_r + c'_{(q-1)/2-r} = (-1)^r \left(\sum \rho^{a_{i_1}+\ldots+a_{i_r}} - \sum \rho^{b_{i_1}+\ldots+b_{i_{(q-1)/2-r}}} \right).$$

Using the fact that $\sum_{i=1}^{(q-1)/2} b_i \equiv 0 \pmod{q}$ as in part (a),

$$c_r + c'_{(q-1)/2-r} = (-1)^r \left(\sum \rho^{a_{i_1}+\ldots+a_{i_r}} - \sum \rho^{-(b_{i_1}+\ldots+b_{i_r})} \right).$$

Then since $(-1|q) = -1$, $\rho^{-(b_{i_1}+\ldots+b_{i_r})} = \rho^{a_{i_1}+\ldots+a_{i_r}}$. Thus

$$c_r + c'_{(q-1)/2-r} = (-1)^r \left(\sum \rho^{a_{i_1}+\ldots+a_{i_r}} - \sum \rho^{a_{i_1}+\ldots+a_{i_r}} \right) = 0.$$

With the results thus far established it is possible to prove several theorems about the coefficients in the two irreducible factors. Since the object is to find coefficients different from 0 or ± 1, p and q will be taken greater than 3 in what follows.

THEOREM 10. Let q be a prime of the form $4k \pm 1$ where $p \nmid k$. If the cyclotomic polynomial $g_q(x)$ factors in $GF[p]$ $(p > 3)$ into

two irreducible factors of equal degree, then a coefficient different from 0 or ± 1 appears in at least one of the factors.

PROOF. By hypothesis, $g_q(x) = f_1(x)\, f_2(x)$ in GF[p] where $f_1(x)$ and $f_2(x)$ are irreducible and of the same degree. By theorem 8, the quadratic period equation of $g_q(x)$ has roots η and η' in GF[p], and by definition and corollary 1, these are the sums of the roots of $f_1(x)$ and $f_2(x)$ respectively. If either η or η' is different from 0 or ± 1 the theorem is true since $c_1 = -\eta$, $c_1' = -\eta'$ by Newton's identities as shown previously. Suppose then that both η and η' are 0 or ± 1. The condition $\eta + \eta' = -1$ imposed by the fact that η and η' are roots of the equation $x^2 + x + (1 - (-1|q)q)/4 = 0$ restricts these values to $\eta = -1$, $\eta' = 0$ (or vice-versa). However, this implies that $\eta\eta' = (1 - (-1|q)q)/4 = 0$ in GF[p]. But since $q = 4k \pm 1$, $(1 - (-1|q)q)/4 = k$, this means that $k \equiv 0 \pmod{p}$ contrary to hypothesis. Therefore in every case a coefficient different from 0 or ± 1 appears in at least one factor.

COROLLARY 3. Let q be a Fermat prime greater than 3. If the cyclotomic polynomial $g_q(x)$ factors in GF[p] $(p > 3)$ into two irreducible factors of equal degree then a coefficient different from 0 or ± 1 appears in at least one factor.

PROOF. This is an immediate consequence of theorem 10 since a Fermat prime is a prime of the form $2^n + 1$ and no prime greater than 3 divides 2^n.

A slightly stronger result can be obtained for primes of the form $4k - 1$.

COROLLARY 4. Let q be a prime of the form $4k - 1$ where $p \nmid k$. If the cyclotomic polynomial $g_q(x)$ factors in $GF[p]$ $(p > 3)$ into two irreducible factors of equal degree, then a coefficient different from 0 or ± 1 appears in each factor.

PROOF. By theorem 10, a coefficient c_r different from 0 or ± 1 appears in at least one factor. But by theorem 9, $c_r = -c'_{(q-1)/2-r}$, for q of the type $4k - 1$. Thus a coefficient different from 0 or ± 1 appears in both factors.

Results for two other special types of primes follow immediately.

COROLLARY 5. Let q be a Mersenne prime or a prime of the form $2^s 3^t - 1$ $(s \geq 2)$. If the cyclotomic polynomial $g_q(x)$ factors in $GF[p]$ $(p > 3)$ into two irreducible factors of equal degree then a coefficient different from 0 or ± 1 appears in each factor.

PROOF. This follows immediately from corollary 4, since a Mersenne prime is a prime of the form $2^n - 1$ and no prime greater than 3 divides 2^n or $2^s 3^t$.

THEOREM 11. Let q be a prime of the form $8k \pm 3$. If the cyclotomic polynomial $g_q(x)$ factors in $GF[p]$ $(p > 3)$ into two irreducible factors of equal degree, a coefficient different from 0 or ± 1 appears in each factor.

PROOF. By hypothesis, $g_q(x) = f_1(x)\, f_2(x)$ in $GF[p]$, where $f_1(x)$ and $f_2(x)$ are irreducible and of the same degree. The quadratic

period equation has roots η and η' in GF[p] which are the sums of the roots of $f_1(x)$ and $f_2(x)$ respectively. These are three cases to consider.

Case 1. η and η' both different from 0 or ± 1. As before c_1 and c_1' are the desired coefficients.

Case 2. One and only one of η and η' different from 0 or ± 1. The condition $\eta + \eta' = -1$ here restricts η and η' to $\eta = 1$, $\eta' = -2$. Since $c_1' = -\eta'$, a coefficient different from 0 or ± 1 appears in one factor. In the other factor $s_1 = 1$, $s_2 = -2$ since $q = 8k \pm 3$ implies that $(2|q) = -1$. Applying Newton's identities we see that $c_1 = -1$, $c_2 = 2^{-1} + 1 = 1 + (p + 1)/2$. For $p > 5$, $1 + (p+1)/2 \neq 0$ or ± 1. In case $p = 5$, there are two possibilities, $(3|q) = \pm 1$. Solving Newton's identities for c_3 and c_4 in the case $(3|q) = +1$ gives $c_3 = 1$, $c_4 = 2$. Solving these identities when $(3|q) = -1$ gives $c_3 = 2$. Thus in every case a coefficient different from 0 or ± 1 appears among the first four coefficients in both factors.

Case 3. Both η and η' equal to 0 or ± 1. As in theorem 10 the only possibility is $\eta = 0$, $\eta' = -1$. Then $s_1 = 0$, $s_2 = -1$, $s_1' = -1$ and $s_2' = 0$, since $(2|q) = -1$. By Newton's identities $c_1 = c_1' = 2^{-1} = (p+1)/2$. But $(p+1)/2 \neq 0$ or ± 1 for $p > 3$. Hence the theorem is true in all three cases.

BIBLIOGRAPHY

1. Bateman, P. T. Note on the coefficients of the cyclotomic polynomial. American mathematical society bulletin 55: 1180-1181. 1949.

2. Dickson, Leonard Eugene. History of the theory of numbers, volume 1. Washington, Carnegie institution of Washington, 1919. 486p.

3. _____. Linear groups with an exposition of the Galois field theory. Leipzig, B. G. Teubner, 1901. 312p.

4. _____. Modern elementary theory of numbers. Chicago, University of Chicago press, 1939. 309p.

5. Erdös, Paul. On the coefficients of the cyclotomic polynomial. American mathematical society bulletin 52: 179-184. 1946.

6. Gauss, Karl Friedrich. Disquisitiones Arithmeticae. Leipzig, Fleischer, 1801. 464p.

7. Hasse, Helmut. Höhere Algebra II. Zweite, verbesserte Auflage. Berlin, Walter de Gruyter and Co., 1927. 158p.

8. Kronecker, Leopold. Leopold Kronecker's Werke I. Leipzig, G. B. Teubner, 1895.

9. Landau, Edmund. Elementare Zahlentheorie. Reprint. New York, Chelsea, 1946. 180p.

10. Lehmer, Derrick Henry. Guide to tables in the theory of numbers. Bulletin of the national research council, number 105, Feb., 1941. 177p.

11. Lehmer, Emma. On the magnitude of the coefficients of the cyclotomic polynomial. American mathematical society bulletin 42: 389-392. 1936.

12. MacDuffee, Cyrus Colton. An introduction to abstract algebra. New York, Wiley, 1940. 303p.

13. Mathews, G. B. Theory of numbers, part I. Reprint. New York, Stechert, 1927. 323p.

14. Pellet, A. E. Sur les fonctions réduites suivant un module premier. Bulletin de la Société Mathématik de France 17: 156-167. 1889.

15. Rauter, Herbert. Höhere Kreiskörper. Journal für die reine und angewandte Mathematik 159: 220-227. 1928.

16. Schönemann, Theodor. Grundzüge einer allgemeiner Theorie der höhern Congruenzen, deren Modul eine reelle Primzahl ist. Journal für die reine und angewandte Mathematik 31: 269-325. 1846.

17. Steinitz, Ernst. Algebraische Theorie der Körper. Neu herausgegeben, mit Erläuterungen und einem Anhang: Abriss der Galoisschen Theorie versehen von Reinhold Baer und Helmut Hasse. New York, Chelsea, 1950. 176p.

18. Waerden, Bartel Leendert van der. Moderne Algebra, erster Teil. Zweite, verbesserte Auflage. Berlin, Julius Springer, 1937. 272p.

19. Weyl, Hermann. Algebraic theory of numbers. Princeton, Princeton university press, 1940. 223p.