Some Relations Between Number Theory and Group Theory.

BY G. A. MILLER.

The $\phi\left(\frac{m}{k}\right)$ numbers[*] which are less than m and have the same highest common factor (k) with m become an abelian group (G) when they are combined by multiplication modulo m, and G is the group of isomorphisms of the cyclic group of order $\frac{m}{k}$.[†] Every possible finite multiplication group in which the operators are represented by numbers is either such a group or it is contained in such a group.[‡] The group G may be made simply isomorphic with the group of isomorphisms of the cyclic group of order $\frac{m}{k}$ by associating with each operator of the latter, k into the index of the power into which this operator transforms every operator of the cyclic group of order $\frac{m}{k}$.

The identity of G is, therefore, its number which is congruent to unity modulo $\frac{m}{k}$. In fact, the numbers of G constitute the same multiplication group with respect to modulus $\frac{m}{k}$ as they constitute with respect to modulus m. The number of invariants[||] in G is therefore equal to the number of different odd primes which divide $\frac{m}{k}$ increased by β_0, where $\beta_0 = 2, 1,$ or 0 as $\frac{m}{k}$ is of the form $8n$, $8n+4$, or ∓ 0 mod 4 respectively. Each of these invariants is even since $\phi(l)$ is even whenever $l > 2$. That $\phi(l)$ is even

[*] Only positive integers are considered in this article.

[†] Annals of Mathematics, Vol. 2 (1901), p. 77.

[‡] Ibid., Vol. 6 (1905), p. 44.

[||] That is, the smallest possible number of independent generators of G.

follows from the fact that it represents the number of operators of highest order (the number of generators) in the cyclic group of order l. Since we may associate an operator with its inverse and this property is reciprocal, it follows that the number of operators of order r, $r > 2$, in any group is even. In particular, the number of generators of any cyclic group whose order exceeds 2 is even.

It may be observed that this proof of the elementary theorem that $\phi(l)$, $l > 2$, is even associates it with the fundamental theorem that the number of operators of order l in any group is even, and hence the number of operators of order 2 in any group of even order is odd. The main object of the present paper is to exhibit relations between fundamental theorems of the two subjects mentioned in the heading. Only one more will be noted here. Let $d_1, d_2, \ldots, d_\lambda$ be the orders of all the cyclic subgroups (including the identity) of any group of order g. Since the total number of operators of highest order contained in all of these subgroups is equal to the order of the group, it follows that

$$g = \phi(d_1) + \phi(d_2) + \cdots + \phi(d_\lambda)$$

when the group is cyclic the numbers $d_1, d_2, \ldots, d_\lambda$ are all distinct and represent all the divisors of g. In this special case the formula reduces to the well known theorem that the totient of a number is the sum of the totients of its divisors.

§1. *Quadratic Residues of Numbers.*

The necessary and sufficient condition that G is cyclic is that $\frac{m}{k}$ has primitive roots.* That is, G is cyclic only when $\frac{m}{k}$ has one of the following values: $4, p^\alpha, 2p^\alpha$, p being an odd prime. In each of these cases G involves only one operator of order 2 and hence just half of its operators have square roots under G. Each of these operators has just two square roots. These facts follow directly from the elementary theorem that the n^{th} powers of all the operators of any abelian group constitute a quotient group, which is the entire group whenever n is prime to the order of the group, and that *each operator of this quotient group may be made to correspond to all its n^{th} roots in an isomorphism between the*

* The number m' has primitive roots whenever the group of isomorphisms of the cyclic group of order m' is cyclic and vice versa.

group and the given quotient group. In particular, each operator that has n^{th} roots has the same number of such roots.

If β represents the smallest number of independent generators of G, the operators of order 2 in G generate a group of order 2^β. Hence it results from the given theorem that just $\frac{1}{2^\beta}$ of the numbers of G have square roots and that each number that has one square root has just 2^β square roots, modulo m or modulo $\frac{m}{k}$. The manner in which the value of β may be obtained from the number $\frac{m}{k}$ was noted above. In the language of number theory this result is generally stated as follows: The congruence

$$x^2 \equiv N \text{ mod. } \frac{m}{k}, \text{ or mod. } m$$

where N and $\frac{m}{k}$ are relatively prime, has either no solution or it has 2^β solutions, β being equal to the number of odd prime factors of $\frac{m}{k}$ increased by β_0.

The group of isomorphisms (I) of the cyclic group of order 2^n is the direct product of a cyclic group of order 2^{n-2}, which is composed of all the operators of I which are commutative with operators of order 4 in the cyclic group of order 2^n, and the group of order 2 generated by the operator of I which transforms each operator of this cyclic group into its inverse.* The square of every operator of I is therefore also the square of an operator in the given cyclic subgroup of order 2^{n-2}. Since all the operators of the latter are commutative with the operators of order 4 in the cyclic group of order 2^n their squares must be commutative with the operators of order 8 in this cyclic group. Hence these squares must transform each operator into a power which is congruent to unity modulo 8. Since the operators of I transform the operators of the cyclic group of order 2^n into every odd power, it follows that *the square of every odd number is congruent to unity modulo* 8.

Since the squares of the operators of the given cyclic subgroup of order 2^{n-2} give all the operators of I which are commutative with the operators of order 8 in the cyclic group of order 2^n, it follows that every odd number which

* Bulletin of the American Mathematical Society, Vol. 7 (1901), p. 351.

is congruent to unity modulo 8 is the square of some other odd number modulo 2^n. That is, every such odd number is a quadratic residue modulo 2^n. Since the identity of I is its own square it follows that every odd number is a quadratic residue of 2 and every odd number congruent to unity modulo 4 is a quadratic residue of 4.

In general, the 2^δ, $\delta > 0$, power of every operator of I is the 2^δ power of an operator in the given cyclic subgroup of order 2^{n-2} and these powers constitute all the operators of I which are commutative with each operator of the subgroup of order $2^{\delta+2}$ in the given cyclic group of order 2^n. That is, *every number which is congruent to unity modulo* $2^{\delta+2}$ *is the* 2^δ *power of some number modulo* 2^n, *where* n *is arbitrary.* Conversely, the 2^δ power of every odd number is congruent to unity modulo $2^{\delta+2}$. If a number has one 2^δ root it has just $2^{\delta+1}$ such roots modulo p^α, $\alpha > \delta + 1$, since I is the direct product of a cyclic group of even order and an operator of order 2.

The preceding results apply directly to the odd multiples of any odd number (k). The first 2^{n-1} of these multiples constitute a group which is simply isomorphic with I if the products are taken modulo 2^nk. Hence each of these numbers which is congruent to unity modulo $2^{\delta+2}$ is the 2^δ power of some number modulo 2^nk where n is arbitrary. That is, any number which is congruent to unity modulo $2^{\delta+2}$ is the 2^δ power of some number modulo 2^nk, where k is any factor of the first number and n is arbitrary.

The group of isomorphisms I of the cyclic group (C) of order p^α (p being an odd prime) is the direct product of two cyclic groups of order $p^{\alpha-1}$ and $p - 1$ respectively. The former is composed of all the operators of I which transform the operators of C into powers whose indices are congruent to unity modulo p.[*] In other words, when I is represented as a number group modulo p^α the numbers which correspond to this subgroup of order $p^{\alpha-1}$ are composed of all the numbers less than p^α which are congruent to unity modulo p. The p^δ powers of these numbers are congruent to unity modulo $p^{\delta+1}$ and are composed of all the numbers modulo p^α which have this property. Any number which is congruent to unity modulo $p^{\delta+1}$ is, therefore, the p^δ power of some other number modulo p^α, where α is arbitrary.

If an operator of I corresponds to a number which is incongruent to unity

[*] Bulletin of the American Mathematical Society, Vol. 7 (1901), p. 351.

modulo p it must transform every operator of C besides the identity. In particular, all the operators of the given cyclic subgroup of order $p-1$ transform every operator of C besides the identity. If any power of such an operator is commutative with an operator of order p in C it must be commutative with every operator of C; i.e. it must be the identity. In other words, the numbers which correspond to the operators of this cyclic group of order $p-1$ belong to the same exponent with respect to each of the moduli p, and p^{a}. If such a number is an r^{th} root modulo p it must also be an r^{th} root modulo p^{a}, and it must have just r such roots with respect to each modulus since I is cyclic. From this it follows directly that when r is prime to p *every number which is an r^{th} root modulo p is also an r^{th} root modulo p^{a}, α being arbitrary.* In particular, a quadratic residue of p is also a quadratic residue of p^{a}, and it is the square of just two numbers with respect to each modulus.

This result may also be seen as follows: If a number is an r^{th} root modulo p it must correspond to an operator of I whose $\frac{p-1}{r}$ power is a power of p. If this condition is satisfied it is clearly also an r^{th} root of p^{a}. In other words, the operators of I which are r^{th} powers have for their constituent whose order is prime to p an operator whose order divides $\frac{p-1}{r}$, and vice versa. As this condition is independent of the value of α it furnishes a direct proof of the theorem in question.

We shall next consider the quadratic character of -1 with respect to modulus m. This number corresponds to the operator of I which transforms every operator of the cyclic group of order m into its inverse. This operator is clearly of order 2 and hence can only be the square of an operator of order 4. Moreover, when I is cyclic and involves an operator of order 4, its square must be the operator of order 2 contained in I. Hence, when m is either p^{a} or $2\ p^{a}$ the necessary and sufficient condition that -1 is a quadratic residue is that $p^{a-1}\ (p-1)$ is divisible by 4; i.e. $p-1$ must be divisible by 4.

It has been observed above that the operator of I which transforms each operator of the cyclic group of order 2^{n} into its inverse may be used as an independent generator of I and hence cannot be a power of any operator of higher order contained in I. In particular, -1 is a non-quadratic residue of 2^{n}, $n>1$, when $n=1$, $-1\equiv 1$ and hence may be regarded as a quadratic residue of every odd number. In general, I is the direct product of the Sylow subgroups of the cyclic group of order m. Hence -1 is a quadratic residue of m only when it is a quadratic residue of the orders of these Sylow subgroups. That is, *the necessary and sufficient condition that -1 is a quadratic residue of m is that all the odd prime factors of m are of the form $4l + 1$ and that* m *is not divisible by* 4. When this condition is satisfied the operator of order 2 in I which transforms each operator of the cyclic group of order m into its inverse is the square of an operator of order 4 and vice versa.

Since -1 corresponds to an operator of order 2 in I it is very easy to determine its general root character modulo m. When I is cyclic this operator has r^{th} root whenever the order of I is divisible by $2r$; i.e. whenever $p^{\alpha-1}(p-1)$ is divisible by $2r$. In general, the necessary and sufficient condition that -1 has r^{th} roots modulo $m = 2^{\alpha_0}, p_1^{\alpha_1}, p_2^{\alpha_2} \dots p_\lambda^{\alpha_\lambda}$ is that $2r$ divides each of the numbers $p_\alpha^{\alpha_\alpha - 1}(p_\alpha - 1)(\alpha = 1, 2, \dots, \lambda)$ and that $\alpha_0 = 1$ or 0 whenever r is even. Since -1 is any odd root of itself this condition has little meaning unless r is even.

§2. *Proof of several other fundamental theorems from the standpoint of group theory.*

From the introductory remarks it follows that the numbers (elements) of a number group G are either all odd or all even whenever the modulus m is even. When m is odd the $\phi\left(\frac{m}{k}\right)$ elements of G include just as many even numbers as odd numbers. In the subgroups of G the number of the even elements need not be the same as that of the odd elements unless the subgroup involves -1 modulo $\frac{m}{k}$. These theorems follow directly from the fact that the product of -1 into an even element is odd and vice versa. As illustration of subgroups of G in which the number of even elements is not equal to the number of odd elements, we give the following four groups:

1, 2, 4, 8 mod. 15; 1, 4, 7, 13 mod. 15; 7, 28, 49, 91 mod. 105; 1, 2, 4, 8, 11, 16 mod. 21.

From the fact that -1 is of order 2 it follows that each number which has a square root with respect to an odd modulus must have an equal number of odd and even numbers as square roots. If the modulus is even all the square roots of odd numbers are odd and those of even numbers are even since the elements of such a group are either all even or all odd.

Some of the formulas relating to the totient of m can be readily obtained by means of group concepts. Whenever m is not a power of a prime it can be resolved into two factors m_1, m_2 which are relatively prime. In this case the cyclic group of order m is the direct product of the two cyclic groups of orders m_1, m_2 respectively. The operators of highest order in the cyclic group of order m are obtained by multiplying the operators of highest order in the cyclic group of order m_1, into those of highest order in the cyclic group of order m_2. This furnishes a direct proof of the formula

$$\phi(m) = \phi(m_1)\,\phi(m_2)$$

whenever m_1, m_2 are relatively prime and $m = m_1 m_2$. Moreover, all the subgroups of the cyclic group of order p^a are contained in its subgroup of order p^{a-1}. That is, $\phi(p^a) = p^a - p^{a-1} = p^a\left(1 - \frac{1}{p}\right)$. Euler's ϕ-function of m is a direct consequence of these two results.

The total number of different sets of k numbers such that none of these numbers exceeds m and that the greatest common divisor of m and all the numbers of any set is unity has been denoted by $\phi_k(m)$ and is called the totient of order k with respect to m.* When $k = 1$ it reduces to the ordinary totient and the subscript is generally omitted. The value of $\phi_k(m)$ may be determined as follows:

Suppose that an abelian group G has k independent generators $(s_1, s_2, \ldots, s_k)$ each being of order m. It is well known that every operator of G can be written in the form

$$s = s_1^{a_1},\, s_2^{a_2} \ldots s_k^{a_k};\ \alpha_1, \alpha_2, \ldots, \alpha_k = 1, 2, \ldots, m.$$

The order of s is m whenever the greatest common divisor of the numbers $m, \alpha_1, \alpha_2, \ldots, \alpha_k$ is unity and vice versa. Hence, $\phi(m)$ is the number of operators of order m in G. As methods are known to find the total number of operators of any order in an abelian group† the determination of $\phi_k(m)$ becomes a very special case of these general methods.

If m is not a power of a prime an independent generator of order m may always be replaced by two independent generators of orders m_1, m_2 respectively,

*Jordan, Traite des substitutions, 1870, p. 96; cf. Cahan, Théorie des nombres, 1900, p. 36.

†Zsigmondy, Monatshefte für Mathematik und Physik, Vol. 7 (1896), p. 227; cf. Annals of Mathematics, Vol. 6 (1904), p. 3.

where $m_1\ m_2 = m$ and m_1, m_2 are relatively prime. Resolving each of the independent generators of G into two such factors, it is evident that G is the direct product of two subgroups having m independent generators of orders m_1, m_2 respectively. Moreover, the number of operators of highest order in G is equal to the product of the numbers of operators of highest order in each of these subgroups. In other words,

$$\phi_k\,(m) = \phi_k\,(m_1)\ \phi_k\,(m_2)$$

whenever $m = m_1\ m_2$ and m_1, m_2 are relatively prime.

When $m = p^a$ the number of operators of order p^a in G is equal to the total number of its operators (p^{ak}) diminished by $p^{(a-1)k}$, the number of its operators whose orders divide p^{a-1}. That is, $\phi_k\ (p^a) = p^{ak} - p^{(a-1)k} = p^{ak}\left(1 - \frac{1}{p^k}\right)$. From this and the preceding formula the value of the function $\phi_k\,(m)$ can be directly obtained. Hence,

$$\phi_k\,(m) = m^k\left(1-\frac{1}{p_1^k}\right)\left(1-\frac{1}{p_2^k}\right)\ \cdots\cdots\ \left(1-\frac{1}{p_\lambda^k}\right)$$

p_1, p_2 .... p_λ being the distinct prime factors of m.

One of the earliest developments in number theory relates to perfect numbers. The order (m) of a cyclic group (M) is said to be perfect whenever M is such that the sum of the orders of all its subgroups is equal to m. It is easy to see that such a cyclic group cannot contain a subgroup whose order (d) is perfect. Since M would contain a subgroup of order $\frac{m}{d}$ into every divisor of d (excluding d itself) and since the sum of these orders would be md, M could contain no other subgroup if m and d were both perfect. As this set of subgroups does not include the identity, it follows that the order of a cyclic group is redundant whenever the order of one of its subgroups is perfect.

It should be added that the developments of this article have close contact with those of Zsigmondy, "Beiträge zur Theorie Abel'scher Gruppen und ihrer Anwendung auf die Zahlentheorie," Monatshefte für Mathematik und Physik, Vol. 7 (1896), pp. 185-289, and the note on "Holomorphisms and primitive roots," Bulletin of the American Mathematical Society, Vol. 7 (1901), pp. 350-354. The object of the present article is to exhibit certain additional developments where the group concept seems especially useful in the study of number theory.

STANFORD UNIVERSITY, *March* 1905.