CYCLOTOMIES AND DIFFERENCE SETS MODULO A PRODUCT OF TWO DISTINCT ODD PRIMES

Thomas Storer

1. INTRODUCTION

A theory of cyclotomy modulo a product of two distinct odd primes was developed in [5], where it was used in the construction of a family $\{W_e\}$ of difference sets. Necessary and sufficient conditions for the existence of W_e-difference sets were given, with a detailed analysis of the cases $e = 2, 4$. In [1] it was shown that W_6- and W_8-difference sets do not exist, and it has been conjectured that those of type W_{2n} exist for no $n > 2$.

The purpose of the present paper is to investigate some other cyclotomies modulo a product of two distinct odd primes, and to determine necessary and sufficient conditions that certain subsets of the above residue systems constitute difference sets.

2. CYCLOTOMY MODULO A PRODUCT OF PRIMES

Throughout the paper, p and q denote distinct odd primes, ζ and η divisors of $p - 1$ and $q - 1$, respectively, and g an integer modulo pq that belongs to the exponents $\frac{p-1}{\zeta}$ modulo p and $\frac{q-1}{\eta}$ modulo q. Further, we define

$$e = \text{g.c.d.}\,(p-1,\, q-1), \quad \varepsilon = \text{g.c.d.}\left(\frac{p-1}{\zeta}, \frac{q-1}{\eta}\right), \quad f = \frac{p-1}{e}, \quad f' = \frac{q-1}{e}, \quad d = eff'.$$

If g has d distinct powers modulo pq, we call g a *generator* (or, alternately, a *quasi-primitive root*) of pq; when $\zeta = \eta = 1$, g is called a *primitive root* of pq. We shall be concerned with the special case $\zeta = 1$.

LEMMA 1. *If* g' *is a primitive root of* q, *and if* g *is a generator of* pq *and*

$$x \equiv 1 \pmod p \qquad \textit{and} \qquad x \equiv g' \pmod q,$$

then the de *integers*

$$g^s x^i \qquad (s = 0, 1, \cdots, d-1;\ i = 0, 1, \cdots, e-1)$$

constitute a reduced residue system modulo pq.

This lemma (as well as further lemmas whose proofs we suppress) can be proved by techniques developed in [5]. We remark that, if η is odd, then g is a nonsquare modulo q. Also, $\alpha = \text{g.c.d.}\,(\eta, f') = 1$, since otherwise $g^{d/\alpha} \equiv 1 \pmod{pq}$.

COROLLARY 1. *There is an integer* μ: $0 \le \mu \le d - 1$ *such that* $x^e \equiv g^\mu \pmod{pq}$.

Received June 2, 1966.
Supported by a National Science Foundation Post-doctoral Research Grant.