ROCKY MOUNTAIN
JOURNAL OF MATHEMATICS
Volume 19, Number 4, Fall 1989

RESIDUACITY OF PRIMES

RONALD EVANS

ABSTRACT. Let q, p be distinct primes with $p = ef + 1$. A variant of the Kummer-Dedekind theorem is proved for Gaussian periods, which shows in particular that q is an e-th power (mod p) if and only if the Gaussian period polynomial of degree e has e (not necessarily distinct) linear factors (mod q). This is applied to give a simple criterion in terms of the parameters in the partitions $p = 8f+1 = \mathbf{X}^2+\mathbf{Y}^2 = \mathbf{C}^2+2\mathbf{D}^2$ for an odd prime q to be an octic residue (mod p). Some consequences and a generalization of an analogous quartic residuacity law (proved by E. Lehmer in 1958) are also given.

1. Introduction. Throughout, let p and q be distinct primes with $p = ef + 1$. In [8], E. Lehmer gave elegant criteria for an odd prime q to be an e-th power residue (mod p), for $e = 3, 4$. The result given for $e = 4$ was essentially the following theorem.

THEOREM 1.1. *Let p be a prime $\equiv 1 (\mathrm{mod}\, 4)$ and write*

$$p = \mathbf{X}^2 + \mathbf{Y}^2, \quad \mathbf{X} \equiv 1 \ (\mathrm{mod}\, 4). \tag{1.1}$$

Then an odd prime $q \neq p$ is quartic (mod p) if and only if

$$\left(\frac{(2/p)}{q}\right) = 1, q|\mathbf{Y}, \text{ or } \left(\frac{2(2/p)(p + \mathbf{X}s)}{q}\right) = 1, \quad q \nmid \mathbf{Y}, \tag{1.2}$$

where s is any integer satisfying $p \equiv s^2 (\mathrm{mod}\, q)$, and $(2/p)$ is the Legendre symbol.

In view of the congruence $(p+\mathbf{Y}s)(2p+2\mathbf{X}s) \equiv (p+\mathbf{X}s+\mathbf{Y}s)^2 (\mathrm{mod}\, q)$, one can replace (1.2) by the equivalent condition

$$\left(\frac{2(2/p)}{q}\right) = 1, q|\mathbf{X}, \text{ or } \left(\frac{(2/p)(p + \mathbf{Y}s)}{q}\right) = 1, q \nmid \mathbf{X}. \tag{1.3}$$

AMS *Subject classification*: Primary 11A15, 11T21; Secondary 11T06.
Received by the editors on January 22, 1987.