QUADRATIC RESIDUES

By N. C. Ankeny

Introduction. Denote by $n(k)$ the least quadratic non-residue (mod k), k being a prime. In this present paper we shall prove that if $k \equiv 3 \pmod 4$, then for any $\epsilon > 0$, $k > k_0(\epsilon)$.

$$(1) \qquad n(k) < k^{\epsilon}.$$

Although (1) is probably true for all primes k the case when $k \equiv 1 \pmod 4$ seems quite a bit more difficult.

For all primes k Vinogradov [7] proved

$$(2) \qquad n(k) < k^{\frac{1}{2}e^{1/2}+\epsilon}.$$

Professor A. Brauer also developed various bounds for $n(k)$ by rather elegant use of the "Dirichlet Chest of Drawer Principle". Unfortunately these results are not quite as sharp as the deep result (2).

On the assumption of various, as yet, unsolved hypotheses concerning Dirichlet L series far more than (1) can be proved. On the assumption of the extended Reimann hypothesis [1], then for all primes k

$$3) \qquad n(k) = O((\log k)^2).$$

See [1] for a proof of (3). If one makes certain assumptions on the order of magnitude of $L(1, (n/k))$, (n/k) is the quadratic residue symbol, Chowla and Erdös made various improvements on (1). Assumptions on the magnitude of $L(1, (n/k))$ are, of course, weaker than the extended Reimann hypothesis. The methods of this paper also yield sharpenings of (1) on these various hypotheses but they are weaker than the results of Chowla and Erdös.

1. We shall make use of the following well-known facts about quadratic imaginary extensions of the rationals. See [4; Chapter VII] for complete proofs.

In the following k will denote a large prime $\equiv 3 \pmod 4$ such that $(i/k) = 1$ for all $1 \leq i \leq k^{1/m}$.

All integers of $F = R((-k)^{\frac{1}{2}})$, where R denotes the rational numbers, are of the form $u + v\omega$, $\omega = \frac{1}{2}(1 + (-k)^{\frac{1}{2}})$, where u, v vary over all rational integers. Let σ denote the non-trivial automorphism of F $[\sigma((-k)^{\frac{1}{2}}) = -(-k)^{\frac{1}{2}}]$.

If p is any odd rational prime and $(-k/p) = +1$, where $(-k/p)$ is the quadratic residue symbol, then in $(p) = PP^{\sigma}$, where P is a prime ideal in F and P^{σ} denotes the conjugate prime ideal. Also $P \neq P^{\sigma}$ and $N(P) = N(P^{\sigma}) = p$, where $N(P)$ denotes the norm of the ideal P in F with respect to R.

We say that two ideals A, B and F are equivalent, $A \sim B$, if there exist a principal ideal (γ) such that $A = (\gamma)B$.

Received March 3, 1953.