HYPERELLIPTIC CURVES

MATHEMATICS

1966

SovietRxiv

Abstract

Full Text

UDC 511

MATHEMATICS

A. I. VINOGRADOV, Academician Yu. V. LINNIK

HYPERELLIPTIC CURVES

AND THE LEAST PRIME QUADRATIC RESIDUE

Andre Weil's proof of the Riemann hypothesis for zeta-functions and L-functions ([1]) of curves over a finite field led to certain profound results also in analytic number theory. One of the most remarkable applications of Andre Weil' s theorem to the analytic theory of Dirichlet characters was given in the works of D. Burgess ([2, 3]). Applying the proved Riemann hypothesis for hyperelliptic curves $y^2 = p(x)$ ($p(x)$ a polynomial of high degree) over a prime finite field, he obtained a new estimate for the least quadratic nonresidue, which constituted a notable advance in the known "first hypothesis of I. M. Vinogradov" on the least quadratic nonresidue.

In the present note we combine the estimates obtained by Burgess with the well-known theorem of C. L. Siegel on quadratic fields. In this way we obtain an advance in the direction of the second hypothesis of I. M. Vinogradov (on the least prime quadratic residue).

The second hypothesis of I. M. Vinogradov asserts that the least prime quadratic residue modulo a prime modulus D—the least prime number $p = P_{\min}(D)$ for which $\chi(p) = 1$—has the estimate $P_{\min}(D) = O(D^{\varepsilon})$ as $D \to \infty$ and for any $\varepsilon > 0$. Until now it was known that $P_{\min}(D) = O(D^{1/2})$ (a consequence of the indicated theorem of Siegel). We prove the theorems:

Theorem 1. *The least prime quadratic residue modulo a prime modulus D has the estimate*

$$P_{\min}(D) = O\left(D^{1/4+\varepsilon}\right) \tag{1}$$

for any $\varepsilon > 0$.

Connected with Theorem 1 is a theorem on ideals of small norm in quadratic fields. Let $D \geq 0$ be a fundamental discriminant. Consider the nonprincipal real character $\chi(n)$ modulo D, the corresponding L-series $L(s, \chi)$, and the ζ-function of the corresponding quadratic field $k(\sqrt{D})$:

$$\zeta_k(s) = \zeta(s)L(s,\chi) = \sum_{n=1}^{\infty} \frac{a_n}{n^s} \quad (\text{for } s = \sigma + it,\ \sigma > 1);$$

here the numbers a_n run through the norms of ideals of the field.

Theorem 2. *For any x satisfying*

$$|D|^{1/4+\varepsilon} \le x \le |D|^{1/2} \tag{2}$$

we have

$$\sum_{n\le x} a_n = xL(1,\chi)\left[1 + O\left(x^{-\eta_0}\right)\right]. \tag{3}$$

Here $\varepsilon > 0$ is an arbitrarily small constant; $|D| > D_0(\varepsilon)$; $\eta_0 = \eta_0(\varepsilon)$ is a constant connected with Burgess' s constant ([3]).

Proof of Theorem 2. We note that

$$a_n = \sum_{d|n} \chi(d).$$

Consider the sum

$$\sum_{n\le x}\left(1-\frac{n}{x}\right)a_n = \sum_{n\le x}\left(1-\frac{n}{x}\right)\cdot\sum_{d|n}\mu(d) = \sum_{d\le x}\chi(d)\cdot\sum_{m\le\frac{x}{d}}\left(1-\frac{md}{x}\right) =$$

$$= \frac{1}{2\pi i}\int_{2-iT}^{2+iT}\frac{x^s}{s(s+1)}\,\zeta(s)\left(\sum_{d\le x}\frac{\chi(d)}{d^s}\right)ds + O(1).$$

By shifting the contour to the left to $\operatorname{Re} s = -1/2$, we obtain

$$\sum_{n\le x}\left(1-\frac{n}{x}\right)a_n = \frac{x}{2}\sum_{d\le x}\frac{\chi(d)}{d} + \frac{1}{2\pi i}\int_{\frac12-iT}^{\frac12+iT}\frac{x^s}{s(s+1)}\zeta(s)\left(\sum_{d\le x}\frac{\chi(d)}{d^s}\right) + O(1). \tag{4}$$

Let us estimate the sum under the integral. We represent it in the form

$$\sum_{d\le|D|^{1/4}}\frac{\chi(d)}{d^s} + \sum_{Q_i}\sum_{Q_i<d\le 2Q_i}\frac{\chi(d)}{d^s}, \qquad Q_0 = |D|^{1/4}.$$

Using partial summation, we find

$$\sum_{Q_i<d\le 2Q_i} \frac{\chi(d)}{d^s} = s\int_{Q_i}^{2Q_i} \frac{s(x)}{x^{s+1}}\,dx + \frac{s(2Q_i)}{(2Q_i)^s} - \frac{s(Q_i)}{Q_i^s}.$$

But for the interval $(Q_i, 2Q_i)$ the Burgess estimate is valid,

$$|s(x)| \ll Q_i^{1-\eta}.$$

Consequently,

$$\left|\sum_{Q_i<d\le 2Q_i} \frac{\chi(d)}{d^s}\right| \ll |s|\, Q_i^{1/2-\eta}.$$

Combining all the estimates, we obtain:

$$\left|\sum_{d\le x} \frac{\chi(d)}{d^s}\right| \ll |s|\, x^{1/2-\eta},$$

where $\eta > 0$ is a constant from the Burgess estimate. Consequently, the integral on the right-hand side of (4) has order of magnitude

$$x^{1-\eta}\ln^2 x.$$

Moreover, from the Burgess estimate it follows that

$$\sum_{d\le x} \frac{\chi(d)}{d} = L(1,\chi) + O\left(x^{1-\eta}\ln x\right).$$

Thus

$$\sum_{n\le x}\left(1-\frac{n}{x}\right)a_n = \frac{x}{2}L(1,\chi) + O\left(x^{1-\eta}\ln^2 x\right). \tag{5}$$

The transition from equality (5) to (3) is carried out according to the classical scheme. In Theorem 2 and its proof, by a real character we understood the Kronecker symbol $\left(\frac{D}{n}\right)$. In Theorem 1, as the real character $\chi(n)$, we must take the Legendre symbol $\left(\frac{n}{D}\right)$, where D is a prime number.

In this case

$$a_n = \prod_{p/n} \left[1 + \chi(p) + \cdots + \chi(p^{\alpha_p})\right], \tag{6}$$

where $n = p_1^{\alpha_1} p_2^{\alpha_2} \cdots p_n^{\alpha_n}$. In the canonical decomposition of n we group together all prime factors that are quadratic residues mod (D), and denote this part of the number by n_0; in exactly the same way we group the nonresidues and denote their product by n_1.

Consequently,

$$n = n_0 n_1.$$

We note that $a_n \geq 1$ in two cases: if $n_1 = 1$ and if $n_1 = m^2$ $(m > 1)$. In order to prove Theorem 1, we have to prove the existence of such n that $n_1 = 1$. To establish this, we apply the sieve:

$$a_n \sum_{\delta^2/n_1} \mu(\delta) = \begin{cases} a_n, & \text{if } n_1 = 1, \\ 0, & \text{if } n_1 > 1, \end{cases}$$

where $\delta \mid m$, $n_1 = m^2$, $n = n_0 m^2$.

Consequently, if for the sum

$$\sum_{n \leq x} \left(1 - \frac{n}{x}\right) a_n \cdot \sum_{\delta^2/n_1} \mu(\delta) \tag{7}$$

one establishes an equality analogous to (5), then Theorem 1 will be proved. Such an equality for (7) can indeed be established by the same method that was set forth in the proof of Theorem 2. It is true that the sieve introduces additional arithmetic for the indices of summation, but this plays no essential role, since the sieve over the squares of divisors is trivial and may be cut off at $\delta > x^{\varepsilon}$.

In conclusion we note that Theorem 2 has important applications in the theory of ternary quadratic forms and in the ergodic theory of algebraic fields ([4]).

Leningrad Branch of the V. A. Steklov Mathematical Institute Academy of Sciences of the USSR

Received 28 I 1966

REFERENCES

[1] A. Weil, Proc. Nat. Acad. Sci. U.S.A., **34**, No. 5, 204 (1948).
[2] D. A. Burgess, Proc. London Math. Soc., **13**, No. 51, 524 (1963).
[3] D. A. Burgess, J. London Math. Soc., **39**, No. 1, 103 (1964).
[4] Yu. V. Linnik, *Ergodic properties of algebraic fields*, L., 1966.

Note: Figure translations are in progress. See original paper for figures.

Source: Math-Net.Ru and CyberLeninka. Machine translation. Verify with the original.