Легко убедиться, что при $Y \geqslant Xt^{-4/11}$ $f(n, y)$ удовлетворяет условиям теоремы с

$$F = \frac{tY}{X}, \quad \Delta = \frac{Y}{X}, \quad k = 3, \quad N = \frac{tY^2}{X^2}, \quad N^\beta = \frac{N^4}{t} = \frac{t^3 Y^6}{X^8},$$

поэтому

$$S^2 \ll X^2/q = Xt^{\frac{346}{1067}} \ln^{\frac{331}{100}} t.$$

Значит,

$$\zeta(\tfrac{1}{2}+it) \ll t^{\frac{173}{1067}} \ln^{\frac{331}{200}} t.$$

Литература

[1] Хуа Ло-ген, *Метод тригонометрических сумм и его применения в теории чисел*, Москва 1964.

[2] Е. К. Титчмарш, *Теория дзета-функции Римана*, Москва 1953.

[3] W. Haneke, *Verschärfung der Abschätzung von* $\zeta(\frac{1}{2}+it)$, Acta Arith. 8 (1963), стр. 357–430.

[4] Чень Цзин-жунь, *On the order of* $\zeta(\frac{1}{2}+it)$, Acta Math. Sinica, 15 (2) (1965), стр. 159–173.

[5] Г. А. Колесник, *Улучшение остаточного члена в проблеме делителей*, Математические заметки 6 (5) (1969), стр. 549–558.

[6] S. H. Min, *On the order of* $\zeta(\frac{1}{2}+it)$, Trans. Amer. Math. Soc. 65 (3) (1949), стр. 448–472.

[7] Г. А. Колесник, *О распределении простых чисел в последовательностях вида* $[n^c]$, Математические заметки 2 (2) (1967), стр. 117–128.

Получено 5. 8. 1971 (203)

ACTA ARITHMETICA
XXV (1973)

On characters and polynomials

by

J. B. Friedlander (University Park, Penn.)

1. Introduction. In two recent papers ([4], [5]) results of Burgess [1] were generalized to obtain estimates for character sums in algebraic number fields. It is the purpose of this paper to discuss some further applications of these results.

Particular attention is paid to problems concerning quadratic non-residues and primitive roots occurring in the values of polynomials. One such problem is the following.

Let m be a rational integer (positive or negative) which is not a perfect square. Let $\varepsilon > 0$ be fixed. Let p denote an odd prime and let π denote the set of primes p such that $x^2 - m \equiv 0 \pmod p$ is irreducible. Let $g_2(m, p)$ be the smallest positive x such that $x^2 - m$ is a quadratic non-residue $(\mathrm{mod}\ p)$.

Burgess [3] obtained the following estimates.

A. $g_2(m, p) \ll p^{2/3\sqrt{e}+\varepsilon}$.

B. For $p \in \pi$, $g_2(m, p) \ll p^{1/2\sqrt{e}+\varepsilon}$

(The implied constants depend on m and ε.)

One of the results of this paper is the removal of the restriction $p \in \pi$ in B. This is accomplished by considering character sums of composite modulus in quadratic fields.

In [2], Burgess obtains estimates for various characters of composite modulus and uses these to derive estimates for L-series. Such a program seems quite feasible for algebraic number fields but, for our purposes, it suffices to consider a particularly simple case.

2. Lemma 1. *Let K be an algebraic number field of degree n. Let $\alpha \in \mathfrak{O}$, the ring of integers of K. Let p be a prime of the n-th degree in K and d a positive rational integer dividing $p-1$. Then,*

$$\alpha^{(p^n-1)/d} \equiv 1 \pmod p \Leftrightarrow (N\alpha)^{(p-1)/d} \equiv 1 \pmod p$$

where $N\alpha$ is the norm of α in K. In particular, if α is a primitive root $(\mathrm{mod}\ p)$ *in $\mathfrak{O}$, then $N\alpha$ is a primitive root* $(\mathrm{mod}\ p)$ *in Z (the rational integers). Also, α*

is a quadratic residue (mod p) *in* $\mathfrak{O}$ *if and only if* $N\alpha$ *is a quadratic residue* (mod p) *in* Z.

Proof. It is sufficient to prove that

$$N\alpha \equiv \alpha^{(p^n-1)/(p-1)} \pmod{p}.$$

For $\alpha \equiv 0 \pmod{p}$, this is trivial.

Let γ be a primitive root (mod p) in $\mathfrak{O}$. Then, since γ is a generator of the finite field $\mathfrak{O}/(p)$, its minimal polynomial f over Z is of degree n and is irreducible (mod p). If a_0 is the constant coefficient of f, then $N\gamma = (-1)^n a_0$.

On the other hand, considering f as a polynomial over $Z/(p)$, its roots are $\gamma, \gamma^p, \ldots, \gamma^{p^{n-1}}$ and their product is $(-1)^n a_0$. Thus,

$$N\gamma \equiv \gamma^{1+p+\ldots+p^{n-1}} \pmod{p}.$$

Now, let $\alpha \equiv \gamma^j \pmod{p}$. Then

$$p \mid \alpha_{(i)} - \gamma_{(i)}^j \qquad (i = 1, \ldots, n)$$

where $\alpha_{(i)}, \gamma_{(i)}^j$ are the ith conjugates of α and γ^j respectively. Thus,

$$N\alpha \equiv N\gamma^j \equiv (N\gamma)^j \equiv (\gamma^{(p^n-1)/(p-1)})^j \equiv (\gamma^j)^{(p^n-1)/(p-1)} \equiv \alpha^{(p^n-1)/(p-1)} \pmod{p}.$$

Lemma 2. *Let* Q *denote the rationals and* $K = Q(\sqrt{m})$ *the quadratic field of discriminant* d. *Let* p *be an odd rational prime and* χ *a real proper character* (mod p) *in* $\mathfrak{O}$ (*i.e. a character of the multiplicative group of reduced residue classes* mod p). *Let* $G_2(m, p)$ *be the least positive integer in the set*

$$\{|N\alpha| \;\; \alpha \in \mathfrak{O}, \chi(\alpha) = -1\}.$$

Let $\varepsilon > 0$ *and* $M > 0$ *be fixed and assume* $|d| < (\log p)^M$. *Then,*

$$G_2(m, p) \ll p^{1/2\sqrt{e}+\varepsilon},$$

the implied constant depending on M *and* ε.

Proof. If p is prime in K, the result is to be found in [5]. If p splits in K, then the proof is a slight modification of which we give a brief outline.

As in [2], the character sum estimate follows quite easily from the crucial lemma (cf. Lemma 8 of [2] and Lemma 2.6 of [5]), the only essential difference being that the parameter $\mathfrak{Q}$ is forced to avoid the prime divisors of p. Unlike [2], the lemma itself follows easily if a minor assumption is made about h which ensures that the polynomials in question are squares if and only if they are squares (mod p). This restriction on h is easily seen to be satisfied by the choice of h used in proving the theorem (cf. 3.1 of [5]).

The derivation of the result from the character sum estimate follows the classical method, an error term being introduced to account for the integers not prime to p.

Lemma 3. *If* m *is any integer which is not a perfect square and*

$$a = x^2 - my^2 \qquad (a, x, y \in Z)$$

then there exists a representation

$$a = u^2 \prod_{i=1}^{r} (v_i^2 - m)^{\varrho_i}$$

for some non-negative $r \in Z$, *positive* $u, v_1, \ldots, v_r$ *all in* Z *and all* $\leqslant n$ *and* $\varrho_1, \ldots, \varrho_r$ *which are* ± 1.

Proof. See [3].

Theorem 1. *Let* $\varepsilon > 0$ *and* $M > 0$ *be fixed. Let* p *run through the odd primes other than those which are divisors of* m.

A.

$$g_2(m, p) \ll p^{1/2\sqrt{e}+\varepsilon},$$

the implied constant depending on m *and* ε.

B. *Assume that* m *is square-free and* $|m| < (\log p)^M$. *Then*

$$g_2(m, p) \ll p^{1/2\sqrt{e}+\varepsilon},$$

the implied constant depending on M *and* ε.

Proof. Case I. $x^2 - m \equiv 0 \pmod{p}$ irreducible. By Lemma 2, there exist x and y with

$$x^2 - y^2 m \ll p^{1/2\sqrt{e}+\varepsilon}$$

such that $\alpha = x + y\sqrt{m}$ is a quadratic non-residue (mod p) in $Q(\sqrt{m})$.

Letting a^2 be the largest square divisor of m (in case B, $a^2 = 1$), we may, by considering $4a^2\alpha$, assume that x and y are rational integers.

By Lemma 1, $x^2 - y^2 m$ is a quadratic non-residue (mod p) in Z. Applying Lemma 3, the result follows.

Case II. $x^2 - m \equiv 0 \pmod{p}$ reducible. Let $(p) = \mathfrak{p}\mathfrak{p}'$ be the prime decomposition of p in $Q(\sqrt{m})$, and let $(\alpha/\mathfrak{p})$ denote the Legendre symbol in $Q(\sqrt{m})$. Define

$$\chi(\alpha) = \left(\frac{\alpha}{\mathfrak{p}}\right)\left(\frac{\alpha}{\mathfrak{p}'}\right).$$

It is clear that χ is a real character (mod p) in $Q(\sqrt{m})$. Furthermore, χ is proper, for if not we can write $\chi(\alpha) = \chi_1(\alpha)\chi_2(\alpha)$ where χ_1 is a character (mod $\mathfrak{p}$), χ_2 is a character (mod $\mathfrak{p}'$) and at least one of the χ_i, say χ_2, is

principal. Choosing β and γ prime to p and noting that $\mathfrak{p} \neq \mathfrak{p}'$, we may write $\beta-\gamma = \sigma-\sigma'$ where $\sigma \equiv 0 \pmod{\mathfrak{p}}$ and $\sigma' \equiv 0 \pmod{\mathfrak{p}'}$. Now, $\beta+\sigma' \not\equiv 0 \pmod{\mathfrak{p}'}$ and, since $\beta+\sigma' = \gamma+\sigma$, $\beta+\sigma' \not\equiv 0 \pmod{\mathfrak{p}}$. Hence

$$\left(\frac{\beta}{\mathfrak{p}'}\right) = \left(\frac{\beta+\sigma'}{\mathfrak{p}'}\right) = \chi_1(\beta+\sigma')\left(\frac{\beta+\sigma'}{\mathfrak{p}}\right) = \chi_1(\gamma+\sigma)\left(\frac{\gamma+\sigma}{\mathfrak{p}}\right)$$

$$= \chi_1(\gamma)\left(\frac{\gamma}{\mathfrak{p}}\right) = \left(\frac{\gamma}{\mathfrak{p}'}\right).$$

Since every reduced residue class $(\mathrm{mod}\ \mathfrak{p}')$ contains an integer prime to $\mathfrak{p}$, this means that $(\beta/\mathfrak{p}')$ is principal, which, for p odd, is a contradiction.

Furthermore, if α' is the conjugate of α, then $(\alpha/\mathfrak{p}') = (\alpha'/\mathfrak{p})$ so that

$$\chi(\alpha) = \left(\frac{N\alpha}{\mathfrak{p}}\right).$$

Since $(N\alpha/\mathfrak{p}) \equiv (N\alpha)^{(N\mathfrak{p}-1)/2} \equiv (N\alpha)^{(p-1)/2} \pmod{\mathfrak{p}}$ and since both $(N\alpha/\mathfrak{p})$ and $(N\alpha)^{(p-1)/2}$ are rational integers, therefore

$$\chi(\alpha) = \left(\frac{N\alpha}{\mathfrak{p}}\right) \equiv (N\alpha)^{(p-1)/2} \pmod{p}.$$

Hence, if $\chi(\alpha) = -1$, $N\alpha$ is a quadratic non-residue $(\mathrm{mod}\ p)$ in Z. Using Lemma 2 to pick such an α and applying Lemma 3 to $N\alpha$, we get the result.

Remark. Analogues to Lemma 2 go through for complex characters and these together with Lemma 1 give results for kth power non-residues. Unfortunately, Lemma 3 seems to have no natural counterpart. Thus, the best we can do is get "small" kth power non-residues of the form x^2-my^2 not necessarily of the form x^2-m.

3. In this section we consider the analogous problem for primitive roots.

Lemma 4. *Let $\varepsilon > 0$ be fixed and $n = 2$ or $n = 3$. Let L be the finite field of p^n elements. There exists $p_0(\varepsilon)$ such that if $p > p_0$ and if θ is any element of L not in $Z/(p)$ then L has a primitive root of the form $\theta+r$ where $r \in Z$ and*

$$1 \leqslant r \leqslant p^{n/4+\varepsilon}.$$

Proof. See Theorem 2 of [6].

Theorem 2. A. *Let $K = Q(\sqrt{m})$. Let $\varepsilon > 0$ be fixed and let π denote the set of primes p of second degree in K which are not divisors of m.*

There exists p_0 depending only on ε such that, for each $p > p_0$ in π there exists a primitive root $(\mathrm{mod}\ p)$ in K of the form $x+\sqrt{m}$, for some $x \in Z$ with

$$0 < x < p^{1/2+\varepsilon}.$$

B. *Let $K' = Q(m^{1/3})$ be a pure cubic field. Let $\varepsilon > 0$ be fixed and let π' denote the set of primes of third degree in K' which are not divisors of m. There exists p_0' depending only on ε, such that for each $p > p_0'$ in π' there exists a primitive root $(\mathrm{mod}\ p)$ in K' of the form $x+m^{1/3}$ for some $x \in Z$ with*

$$0 < x < p^{3/4+\varepsilon}.$$

Proof. For $p \in \pi$, the residue classes $(\mathrm{mod}\ p)$ in K form a field of p^2 elements and $\sqrt{m}$ does not belong to its prime subfield. Thus, A follows immediately from Lemma 4. The proof of B is similar.

Applying Lemma 1, we get immediately

Corollary. A. *Assume that m is not a perfect square and let Π denote the set of rational primes for which $x^2-m \equiv 0 \pmod{p}$ is irreducible. Each $p > p_0(\varepsilon)$ in Π has a primitive root in Z of the form x^2-m with*

$$0 < x < p^{1/2+\varepsilon}.$$

B. *Assume that m is not a perfect cube and let Π' denote the set of rational primes for which $x^3-m \equiv 0 \pmod{p}$ is irreducible. Each $p > p_0'(\varepsilon)$ in Π' has a primitive root in Z of the form x^3-m with*

$$0 < x < p^{3/4+\varepsilon}.$$

Theorem 3. *Let $f(a)$ be real-valued function defined as follows:*

$$f(a) = \begin{cases} \frac{1}{4}+\frac{1}{2}\sqrt{a}+\frac{7}{4}a & \text{for} \quad 0 < a < \frac{1}{25}, \\ \frac{3}{10}+3a & \text{for} \quad \frac{1}{25} \leqslant a < \frac{1}{15}, \\ \frac{1}{2} & \text{for} \quad \frac{1}{15} \leqslant a < \frac{1}{2}, \\ a & \text{for} \quad \frac{1}{2} \leqslant a. \end{cases}$$

Let $K = Q(\sqrt{m})$ have discriminant d. Let $\mathfrak{p}$ be a prime ideal in K and $g(\mathfrak{p})$ the smallest positive integer in the set

$$\{|N\alpha| \mid \alpha \text{ a primitive root } (\mathrm{mod}\ \mathfrak{p}) \text{ in } K\}.$$

Let $\varepsilon > 0$ and $a > 0$ be fixed and assume $|d| < (N\mathfrak{p})^a$. Then,

$$g(\mathfrak{p}) \ll (N\mathfrak{p})^{f(a)+\varepsilon},$$

where the implied constant depends on a and ε.

Proof. If $\mathfrak{p}$ is a prime of the second degree, the bound

$$g(\mathfrak{p}) \ll |d| + (N\mathfrak{p})^{1/2+\varepsilon}$$

follows from A of Theorem 2. If $\mathfrak{p}$ is a prime of the first degree with norm p, then, for $d \mid p-1$ and β a rational integer,

$$\beta^d \equiv 1 \pmod{\mathfrak{p}} \Leftrightarrow \beta^d \equiv 1 \pmod{p}.$$

Since we can choose a primitive root $\beta_0 \pmod p$ in Z with $\beta_0 \ll p^{1/4+\varepsilon/2}$, β_0 will be a primitive root (mod p) in K with

$$N\beta_0 = \beta_0^2 \ll p^{1/2+\varepsilon}.$$

This completes the proof for $a \geqslant 1/15$.

For $a < 1/15$, the result follows by applying the classical argument of Vinogradov (cf. Theorem 3 of [1]) to the character sum estimates in Theorems 3.3 and 5.1 of [5]. In these theorems we let $\gamma = 3/2$. For $a \geqslant 1/25$, we choose $b = 3/10$, while, for $a < 1/25$, we choose $b = (1+\sqrt{a})/4$.

Remark. Applying Lemma 1 to Theorem 3 gives "small" primitive roots of the form $x^2 - y^2 m$ as p runs through the primes for which $x^2 - m \equiv 0 \pmod p$ is irreducible.

4. Let a and m be relatively prime positive integers and consider the arithmetic progression $a + mx$ ($x = 0, 1, 2, \ldots$). For p an odd prime, define $h(a, m, p)$ to be the smallest prime in this progression which is a quadratic non-residue (mod p).

The problem of obtaining upper bounds for $h(a, m, p)$ seems in general to be quite difficult and I cannot recall seeing any mention of it in the literature. It follows of course from the famous theorem of Linnik on the least prime in an arithmetic progression that there exists an absolute constant C such that

$$h(a, m, p) \ll (mp)^C,$$

where the implied constant is absolute.

We also have as consequences of the above results:

THEOREM 4.

A. $$h(1, 4, p) \ll p^{1/2\sqrt{e}+\varepsilon},$$

B. $$h(1, 3, p) \ll p^{1/2\sqrt{e}+\varepsilon}$$

the implied constant depending only on ε.

Proof. A. We consider character sums over the Gaussian field $Q(i)$. Let χ be a real proper character (mod p) in $\mathfrak{O}$. For $H \geqslant p^{1/2+\delta}$,

$$\sum_{\substack{\alpha \in \mathfrak{O} \\ N\alpha \leqslant H}} \chi(\alpha) = o(H).$$

As α runs through the integers of $\mathfrak{O}$ having norm $\leqslant H/2$, $(1+i)\alpha$ runs through the integers of $\mathfrak{O}$ having even norm $\leqslant H$. Thus,

$$\sum_{\substack{\beta \in \mathfrak{O} \\ N\beta \leqslant H \\ (1+i) \mid \beta}} \chi(\beta) = o(H),$$

and so

$$\sum_{\substack{\beta \in \mathfrak{O} \\ N\beta \leqslant H \\ (1+i)\nmid \beta}} \chi(\beta) = o(H).$$

Applying the usual argument to this last estimate, we get an $\alpha \in \mathfrak{O}$ with $\chi(\alpha) = -1$, $N\alpha \ll p^{1/2\sqrt{e}+\varepsilon}$, and $N\alpha$ odd. Now, $N\alpha = x^2 + y^2$ is a quadratic non-residue (mod p) in Z and is divisible only by primes which are $\equiv 1 \,(4)$. Hence the result.

B follows by applying a similar argument to the field $Q(\sqrt{-3})$.

References

[1] D. A. Burgess, *On character sums and primitive roots*, Proc. London Math. Soc. (3) 12 (1962), pp. 179–192.

[2] — *On character sums and L-series*, Proc. London Math. Soc. (3) 12 (1962), pp. 193–206.

[3] — *On the quadratic character of a polynomial*, J. London Math. Soc. 42 (1967), pp. 73–80.

[4] J. B. Friedlander, *On the least k-th power non-residue in an algebraic number field*, Proc. London Math. Soc. (3) 26 (1973), pp. 19–34.

[5] — *Character sums in quadratic fields* (to appear in Proc. London Math. Soc.).

[6] — *A note on primitive roots in finite fields*, Mathematika 19 (1972), pp. 112–114.

THE PENNSYLVANIA STATE UNIVERSITY
THE INSTITUTE FOR ADVANCED STUDY
Princeton, N. J.

Received on 8. 5. 1972 (287)