

Average Version of Artin's Conjecture in an Algebraic Number Field

Shigeki EGAMI

Keio University

(Communicated by T. Saito)

Artin's conjecture on primitive root was proved by Hooley [1] under the generalized Riemann hypothesis for certain family of Dedekind Zeta functions. Its generalization to arbitrary number fields was also obtained by Weinberger [2] and Lenstra [3]. In another direction, Goldfeld [4] obtained a "large sieve type" result for the rational case without Riemann hypothesis. In this paper we shall show that his method can be applied to obtain the similar result for the case treated in [2], [3].

Let K be an algebraic number field of degree n , and q be a fixed integral divisor which contains all the infinite primes of K . For $A > 0$ we define a set of non-zero integers of K by

$$B'(A) = \{\alpha; |\alpha^{(\nu)}| \leq A, (\nu = 1, \dots, n)\},$$

where $\alpha^{(\nu)}$ denotes a conjugate element of α . We write $\alpha \sim \beta$ for integers α, β of K if both α and β generate the same principal ideal. We denote by $B(A)$ a fixed collection of the representatives taken from each equivalence class of $B'(A)/\sim$. Let h be a ray class modulo q , and define

$$(1) \quad N_{\alpha, q, h}(x) = N_{\alpha}(x) \\ = \text{card} \{p; Np \leq x, p \in h, \alpha \text{ is a primitive root modulo } p\},$$

and

$$g(K) = \sup_{1 \leq x < \infty} \sum_{N\alpha \leq x} 1/x$$

where α denotes an integral ideal of K . We denote

$$(2) \quad \text{Li}(x) = \int_2^x \frac{dt}{\log t}.$$

In the following p always denotes a rational prime, and \mathfrak{p} , \mathfrak{p}_1 , \mathfrak{p}_2 prime ideals of K . We denote by K_q the ray class field modulo q over K , and by $Q(\zeta_k)$ the k th cyclotomic field. Then our result is:

Theorem. Let $1 \leq A^* \leq x$. Then for each $D \geq 1$

$$(3) \quad N_\alpha(x) = C(K, q, h) \operatorname{Li}(x) + O\left(\frac{x}{\log^D x}\right)$$

for all $\alpha \in B(A)$ with at most

$$(4) \quad c_1 A^{(9/10)\kappa} (g(K)(5 \log x + 1))^{(\log x)/(\kappa \log A) + D + 2}$$

exceptions, where c_1 and the constant represented by O -symbol are positive and depend at most on K , q , h and D . And

$$(5) \quad C(K, q, h) = \frac{1}{[K_q; K]} \prod_p \left(1 - \frac{F(p) \cdot [Q(\zeta_p) \cap K_q; Q]}{p(p-1)} \right),$$

where $F(\)$ is defined by

$$(6) \quad F(k) = \begin{cases} 1 & \text{if there exists an ideal } \mathfrak{b} \text{ of } K \text{ such} \\ & \text{that } N\mathfrak{b} \equiv 1 \pmod{k}, \mathfrak{b} \in h, \\ 0 & \text{otherwise.} \end{cases}$$

We note that $B(A)$ has at least $c_2 A^\kappa$ elements as will be proved in Lemma 1, so that (3) is satisfied actually for "almost all" $\alpha \in B(A)$. Further we note that, by putting $K = \mathbb{Q}$, $q = (p_\infty)$ our result coincides with Goldfeld's one since $g(K) = 1$, $K_q = \mathbb{Q}$, and $C(K, q, h) = \prod_p (1 - (1/p(p-1)))$ in this case.

In the followings c_2, c_3, \dots are positive constants depending only on K , O -symbol and \ll may contain constants depending on K , q , h and D .

§1. Lemmas.

LEMMA 1. *There exist positive constants c_2, c_3 , and c_4 depending only on K such that*

$$(7) \quad c_3 A^\kappa \leq |B(A)| \leq c_4 A^\kappa$$

for all $A \geq c_2$.

PROOF. Note first that

$$|B(A)| \leq \sum_{N\mathfrak{a} \leq A^\kappa} 1 \leq c_4 A^\kappa.$$

Let r_1, r_2 be the numbers of the real or the imaginary infinite primes of K respectively. Let $\{\varepsilon_1, \dots, \varepsilon_{r_1+r_2-1}\}$ be a system of the fundamental units of K . We denote for $\alpha \in K$

$$l^{(i)}\alpha = \begin{cases} \log |\alpha^{(i)}|, & i=1, \dots, r_1 \\ 2 \log |\alpha^{(i)}|, & i=r_1+1, \dots, r_1+r_2 \end{cases}$$

where the indices i are chosen so that $\{1, \dots, r_1\}, \{r_1+1, \dots, r_1+r_2\}$ corresponds to the complete set of real or imaginary primes of K respectively. Set

$$c_2 = \exp\left(\frac{1}{n} \sum_{i=1}^r \sum_{j=1}^{r-1} |l^{(i)}\varepsilon_j|\right),$$

where $r=r_1+r_2$.

Let α be an integer of K satisfying $|N\alpha| \leq (c_2^{-1}A)^n$. Put

$$\begin{aligned} x_i &= l^{(i)}\alpha, \quad i=1, \dots, r, \\ y_i &= \begin{cases} \log A - \sum_{j=1}^{r-1} |l^{(i)}\varepsilon_j| & i=1, \dots, r_1, \\ 2 \log A - \sum_{j=1}^{r-1} |l^{(i)}\varepsilon_j| & i=r_1+1, \dots, r, \end{cases} \end{aligned}$$

and

$$u_{ij} = \begin{cases} l^{(i)}\varepsilon_j & i=1, \dots, r; j=1, \dots, r \\ 0 & i=1, \dots, r-1; j=r \\ 1 & i=r; j=r. \end{cases}$$

Since the matrix $U = \{u_{ij}\}$ is regular, there exist real numbers z_1, \dots, z_r satisfying

$$U \cdot \begin{bmatrix} z_1 \\ \vdots \\ z_r \end{bmatrix} = \begin{bmatrix} y_1 - x_1 \\ \vdots \\ y_r - x_r \end{bmatrix}.$$

By putting $n_j = [z_j]$ (the integer part) we have

$$y_i - x_i = \sum_{j=1}^{r-1} u_{ij} z_j \geq \sum_{j=1}^{r-1} u_{ij} n_j - \sum_{j=1}^{r-1} |u_{ij}|$$

for $i=1, \dots, r-1$. This inequality is also valid for $i=r$, since

$$y_r - x_r = \sum_{j=1}^{r-1} u_{rj} z_j + z_r$$

and

$$z_r = \sum_{i=1}^r y_i - x_i \geq 0.$$

Thus we have

$$x_i + \sum_{j=1}^{r-1} u_{ij} n_j \leq y_i + \sum_{j=1}^{r-1} |u_{ij}|$$

for $i=1, \dots, r$, which yields $\alpha \cdot \varepsilon_1^{n_1} \cdots \varepsilon_r^{n_r} \in B(A)$. Hence we have

$$|B(A)| \geq \sum_{\substack{N\alpha \leq (c_2^{-1}A)^n \\ \alpha \text{ principal}}} 1 \geq c_3 A^n$$

if $A \geq c_2$.

Let k be a positive integer and set $f=kq$. We denote by I_f the group of all the fractional ideals of K having no common divisor to f , and set

$$(8) \quad H_f = \{(\alpha) \in I_f; N(\alpha) \equiv 1 \pmod{k}, \alpha \equiv 1 \pmod{q}\},$$

where (α) denotes the principal ideal of K generated by α .

LEMMA 2.

$$(9) \quad [I_f: H_f] = [K_q: K] \cdot \frac{\varphi(k)}{[Q(\zeta_k) \cap K_q: Q]},$$

where $\varphi(k)$ is Euler function. If k is square free, we have

$$(10) \quad [I_f: H_f] = [K_q: K] \prod_{p|k} \frac{p-1}{[Q(\zeta_p) \cap K_q: Q]}.$$

PROOF. (10) is a simple consequence of (9) since $Q(\zeta_p) \cap Q(\zeta_{p'}) = Q$ for different primes p and p' . According to class field theory $[I_f: H_f] = [K_q(\zeta_k): K]$. Since $K_q(\zeta_k) = K_q \cdot Q(\zeta_k)$ we have

$$\begin{aligned} [K_q(\zeta_k): K] &= [K_q(\zeta_k): K_q] \cdot [K_q: K] \\ &= [Q(\zeta_k): Q(\zeta_k) \cap K_q] \cdot [K_q: K] = \frac{[Q(\zeta_k): Q]}{[Q(\zeta_k) \cap K_q: Q]} \cdot [K_q: K] \\ &= [K_q: K] \frac{\varphi(k)}{[Q(\zeta_k) \cap K_q: Q]}, \end{aligned}$$

which yields Lemma 2.

Set

$$\pi(x; k) = \sum_{\substack{Np \leq x, p \in h \\ Np \equiv 1 \pmod{k}}} 1.$$

The following lemma is an easy consequence of the theorem of Goldstein [6].

LEMMA 3. For arbitrary $D \geq 1$ we have

$$\pi(x; k) = \frac{F(k)}{[I_f; H_f]} \left(\text{Li}(x) + O\left(\frac{x}{\log^{D+1} x}\right) \right),$$

if $k \leq \log^D x$.

Next we quote a large sieve inequality of Huxley ([7]; Theorem 4) in a slightly modified form which is appropriate for our purpose. Let μ be a positive integer and set

$$B(A)^\mu = \{\alpha_1 \cdots \alpha_\mu; \alpha_i \in B(A) \ (i=1, \dots, \mu)\}.$$

LEMMA 4. Let $a(\alpha)$ be a complex valued function defined on $B(A)^\mu$, then for $x \geq 0$

$$\begin{aligned} \sum_{Na \leq x} \sum_{\chi \pmod a}^* \left| \sum_{\alpha \in B(A)^\mu} a(\alpha) \chi(\alpha) \right|^2 \\ \leq c_5 (A^{*\mu} + x^2) \sum_{\alpha \in B(A)^\mu} |a(\alpha)|^2, \end{aligned}$$

where the sum $\sum_{\chi \pmod a}^*$ is taken over all the primitive characters modulo a .

Let

$$\tau_\mu(a) = \sum_{\substack{(\alpha_1, \dots, \alpha_\mu) \\ a = \alpha_1 \cdots \alpha_\mu}} 1.$$

Similarly to the rational case (cf. Hua [8]), we get the following estimate.

LEMMA 5. For $y \geq 0$ and nonnegative integer l ,

$$\sum_{Na \geq y} \tau_\mu(a)^l \leq y \cdot g(K)^{\mu l} (\log y + 1)^{\mu l - 1}.$$

LEMMA 6. $F(k)$ is a multiplicative function.

PROOF. Let k and k' are relatively prime. If $F(kk')=1$, clearly $F(k)=1$ and $F(k')=1$ by the definition. Suppose $F(k)=F(k')=1$, then there exist integral ideals \mathfrak{b} , \mathfrak{b}' of K such that

$$(11) \quad Nb \equiv 1 \pmod{k}, \quad b \in h; \quad Nb' \equiv 1 \pmod{k'}, \quad b' \in h.$$

let c be an integral ideal in h^{-1} . Then there exist integers α, α' of K such that

$$(12) \quad bc = (\alpha), \quad \alpha \equiv 1 \pmod{q}; \quad b'c = (\alpha'), \quad \alpha' \equiv 1 \pmod{q}.$$

Since $\alpha \equiv \alpha' \pmod{q}$ and $(k, k') = 1$, there exists an integer β of K satisfying

$$\beta \equiv \alpha \pmod{qk}, \quad \beta \equiv \alpha' \pmod{qk'}.$$

Now set $b^* = (\beta)c^{-1}$, then clearly $b^* \in h$. Furthermore we have

$$(13) \quad N\beta \equiv N\alpha \pmod{k}, \quad N\beta \equiv N\alpha' \pmod{k'}.$$

But $N(\alpha) = N\alpha$ and $N(\beta) = N\beta$ since both α and β are totally real. Therefore we have $Nb^* \equiv 1 \pmod{kk'}$ from (11), (12), and (13), which proves Lemma 6.

§2. Proof of Theorem.

Let α be an integer of K . For a prime ideal $\mathfrak{p} \nmid \alpha$ we denote by $e_\alpha(\mathfrak{p})$ the least positive integer m satisfying $\alpha^m \equiv 1 \pmod{\mathfrak{p}}$, and put $f_\alpha(\mathfrak{p}) = (N\mathfrak{p} - 1)/e_\alpha(\mathfrak{p})$. Then we have

$$N_\alpha(x) = \sum_{k \leq x} \mu(k) \cdot P_\alpha(x, k),$$

where

$$P_\alpha(x, k) = \sum_{\substack{N\mathfrak{p} \leq x, \mathfrak{p} \in h \\ k \mid f_\alpha(\mathfrak{p})}} 1,$$

and $\mu(k)$ is the Mobius function.

We show first

$$(14) \quad \sum_{k > x^{3/4}} P_\alpha(x, k) = O(x^{1/2} \log x),$$

for $\alpha \in B(A)$. Since

$$\prod_{k > x^{3/4}} \prod_{\substack{N\mathfrak{p} \leq x \\ k \mid f_\alpha(\mathfrak{p})}} \mathfrak{p} \mid \prod_{m \leq x^{1/4}} (\alpha^m - 1)$$

and $N\mathfrak{p} \geq 2$, we have

$$(15) \quad \left(\sum_{k > x^{3/4}} P_\alpha(x, k) \right) \log 2 \leq \sum_{m < x^{1/4}} \log |N(\alpha^m - 1)|.$$

But by $A^n \leq x$,

$$\begin{aligned}
 (16) \quad \log |N(\alpha^m - 1)| &= \sum_{\nu=1}^n \log |\alpha^{(\nu)m} - 1| \\
 &\leq \sum_{\nu=1}^n \log (1 + |\alpha^{(\nu)m}|) \\
 &\leq c_b m \log x .
 \end{aligned}$$

Therefore we obtain (14) from (15) and (16). We have thus proved

$$(17) \quad N_\alpha(x) = \sum_{k \leq x^{3/4}} \mu(k) P_\alpha(x, k) + O(x^{1/2} \log x) .$$

Let $\chi_{\nu, k}$ be a character modulo p of order k . Since

$$\sum_{\nu=1}^k \chi_{\nu, k}(\alpha) = \begin{cases} k & \text{if } \alpha \text{ is a } k\text{th power residue modulo } p, \\ 0 & \text{otherwise,} \end{cases}$$

we obtain

$$\begin{aligned}
 (18) \quad P_\alpha(x, k) &= \sum_{\substack{N_p \leq x, p \in h \\ N_p \equiv 1 \pmod{k}}} \frac{1}{k} \sum_{\nu=1}^k \chi_{\nu, k}(\alpha) \\
 &= \frac{1}{k} \{ \pi(x; k) + S_\alpha(x, k) + O(\log |N\alpha|) \} ,
 \end{aligned}$$

where

$$S_\alpha(x, k) = \sum_{\substack{N_p \leq x, p \in h \\ N_p \equiv 1 \pmod{k}}} \sum_{\nu=1}^{k-1} \chi_{\nu, k}(\alpha) .$$

Thus we have from (17) and (18) that

$$\begin{aligned}
 N_\alpha(x) &= \sum_{k \leq x^{3/4}} \frac{\mu(k)}{k} \pi(x; k) + \sum_{k \leq x^{3/4}} \frac{\mu(k)}{k} S_\alpha(x, k) \\
 &\quad + O(x^{1/2} \log x) .
 \end{aligned}$$

We denote the first sum by \sum_1 and the second by \sum_2 . It follows from Lemma 3 that

$$\begin{aligned}
 (19) \quad \sum_1 &= \sum_{k \leq \log^D x} \frac{\mu(k) \cdot F(k)}{k [I_f; H_f]} \text{Li}(x) + O\left(\frac{x}{\log^{D+1} x} \sum_{k \leq \log^D x} \frac{1}{k}\right) \\
 &\quad + \sum_{\log^D x < k \leq x^{3/4}} \frac{\mu(k)}{k} \cdot \pi(x; k) \\
 &= \text{Li}(x) \sum_{k \leq \log^D x} \frac{\mu(k) F(k)}{k [I_f; H_f]} + O\left(\frac{x}{\log^D x}\right)
 \end{aligned}$$

using

$$\pi(x; k) \ll \sum_{m \leq x, m \equiv 1 \pmod{k}} 1 \ll \frac{x}{k}$$

for $k > \log^D x$. Furthermore, since

$$[I_f: H_f] \gg \varphi(k) \geq c_0 \frac{k}{\log \log k}$$

we have for any $\varepsilon > 0$

$$\sum_{k=1}^{\infty} \frac{\mu(k)F(k)}{k[I_f: H_f]} = \sum_{k \leq \log^D x} \frac{\mu(k)F(k)}{k[I_f: H_f]} + O\left(\frac{x}{(\log^D x)^{1-\varepsilon}}\right).$$

Combining this with (19) we obtain,

$$\begin{aligned} \Sigma_1 &= \text{Li}(x) \sum_{k=1}^{\infty} \frac{\mu(k)F(k)}{k[I_f: H_f]} + O\left(\frac{x}{\log^D x}\right) \\ &= C(K, q, h) \text{Li}(x) + O\left(\frac{x}{\log^D x}\right) \end{aligned}$$

using Lemma 2 and Lemma 6.

To complete the proof it is sufficient to show

$$\Sigma_2 = O\left(\frac{x}{\log^D x}\right)$$

except some $\alpha \in B(A)$ indicated in (4). The number of α 's such that $\Sigma_2 \geq x/\log^D x$ does not exceed

$$(20) \quad \sum_{\substack{\alpha \in B(A) \\ S_\alpha(x) \geq x/\log^D x}} 1 \leq \frac{\log^D x}{x} \sum_{\alpha \in B(A)} S_\alpha(x),$$

where

$$(21) \quad S_\alpha(x) = \sum_{k \leq x^{3/4}} \frac{1}{k} |S_\alpha(x, k)|.$$

It follows from Cauchy-Schwarz's inequality that

$$\sum_{\alpha \in B(A)} |S_\alpha(x, k)| \leq |B(A)|^{1/2} \left(\sum_{\alpha \in B(A)} |S_\alpha(x, k)|^2 \right)^{1/2}.$$

Since $\chi_{\mathfrak{p}_1, k}^{\nu_1} \cdot \chi_{\mathfrak{p}_2, k}^{-\nu_2}$ is principal only if $\mathfrak{p}_1 = \mathfrak{p}_2$, we get using Lemma 1,

$$(22) \quad \begin{aligned} \sum_{\alpha \in B(A)} |S_\alpha(x, k)| &\ll A^n (xk)^{1/2} \\ &+ A^{n/2} \left| \sum_{\substack{N_{\mathfrak{p}_1} \leq x, \mathfrak{p}_1 \in \mathfrak{h} \\ N_{\mathfrak{p}_1} \equiv 1 \pmod{k}}} \sum_{\substack{N_{\mathfrak{p}_2} \leq x, \mathfrak{p}_2 \in \mathfrak{h} \\ N_{\mathfrak{p}_2} \equiv 1 \pmod{k} \\ \mathfrak{p}_1 \neq \mathfrak{p}_2}} \sum'_{\alpha \in B(A)} \chi(\alpha) \right|^{1/2}, \end{aligned}$$

where the sum \sum'_χ is taken over all the primitive characters modulo $p_1 p_2$ of order k . Let

$$T = \left| \sum_{\substack{Np_1 \leq x, p_1 \in h \\ Np_1 \equiv 1 \pmod{k} \\ p_1 \neq p_2}} \sum_{\substack{Np_2 \leq x, p_2 \in h \\ Np_2 \equiv 1 \pmod{k}}} \sum'_\chi \sum_{\alpha \in B(A)} \chi(\alpha) \right|.$$

Applying Hölder's inequality we have for each positive integer μ .

$$T^{1/2} \ll x^{1-1/2\mu} \left(\sum_{\substack{Np_1 \leq x, p_1 \in h \\ Np_1 \equiv 1 \pmod{k} \\ p_1 \neq p_2}} \sum_{\substack{Np_2 \leq x, p_2 \in h \\ Np_2 \equiv 1 \pmod{k}}} \sum'_\chi \left| \sum_{\alpha \in B(A)} \chi(\alpha) \right|^{2\mu} \right)^{1/4\mu}.$$

Let $a_\mu(\alpha)$ denote the number of ways α can be written as a product of μ elements of $B(A)$. Then we have

$$\left(\sum_{\alpha \in B(A)} \chi(\alpha) \right)^\mu = \sum_{\alpha \in B(A)^\mu} a_\mu(\alpha) \chi(\alpha).$$

By Lemma 4 we obtain

$$T^{1/2} \ll x^{1-1/2\mu} \left((A^{n\mu} + x^4) \sum_{\alpha \in B(A)^\mu} a_\mu(\alpha)^2 \right)^{1/4\mu}.$$

Note that $a_\mu(\alpha) \leq \tau_\mu((\alpha))$ and $N((\alpha)) \leq A^{n\mu}$ for $\alpha \in B(A)^\mu$. Therefore we obtain

$$(23) \quad T^{1/2} \ll x^{1-1/2\mu} \left\{ (A^{n\mu} + x^4) A^{n\mu} (\log A^{n\mu} + 1) g(K) \right\}^{\mu^2/4\mu}.$$

Now we take μ as an integer satisfying

$$(24) \quad \frac{4 \log x}{n \log A} \leq \mu < \frac{4 \log x}{n \log A} + 1.$$

It follows from (22), (23), and (24) that

$$\sum_{\alpha \in B(A)} |S_\alpha(x, k)| \ll A^n (xk)^{1/2} + A^{(9/10)n} x (g(K)(5 \log x + 1)) \frac{\log x}{n \log A} + 1.$$

Combining this with (20) and (21), we see that

$$\sum_{\substack{\alpha \in B(A) \\ \Sigma_2 > x/10^D x}} 1 \ll A^{(9/10)n} (g(K)(5 \log x + 1))^{(\log x/n \log A) + D + 2},$$

which completes the proof of Theorem.

ACKNOWLEDGMENT. The auther wishes to thank Prof. R. Kaneiwa who read the manuscript and made valuable suggestions. He also thanks

Prof. M. Hikari for many kind advices, particularly for simplification of the proof of Lemma 1.

References

- [1] C. HOOLEY, On Artin's conjecture, *J. Reine Angew. Math.*, **225** (1967), 209-220.
- [2] P. J. WEINBERGER, On Euclidean rings of algebraic integers, *Proc. Symp. Pure Math.*, Amer. Math. Soc., Providence, **24**, 321-332.
- [3] H. W. LENSTRA, JR, On Artin's conjecture and Euclid's algorithm in global fields, *Invent. Math.*, **42** (1977), 201-224.
- [4] M. GOLDFELD, Artin's conjecture on the average, *Matematika*, **15** (1968), 223-226.
- [5] T. TAKAGI, *Algebraic Number Theory*, Iwanami, Tokyo, 1971 (in Japanese).
- [6] L. J. GOLDSTEIN, A generalization of the Siegel-Walfisz's theorem, *Trans. Amer. Math. Soc.*, **149** (1970), 417-428.
- [7] M. N. HUXLEY, The large sieve inequality for algebraic number fields, *Matematika*, **15** (1968), 178-187.
- [8] L. K. HUA, *Additive theory of prime numbers*, *Transtations of Mathematical Monographs* 13, Amer. Math. Soc., 1965.

Present Address:
DEPARTMENT OF MATHEMATICS
KEIO UNIVERSITY
HIYOSHI-CHO, KOHOKU-KU
YOKOHAMA 223