ELEMENTARY ESTIMATES FOR THE NUMBER OF PURE NUMBER FIELDS OF DEGREE p

Yusuke Fujisawa
Graduate School of Mathematics, Nagoya University, Furocho, Chikusa-ku, Nagoya, Japan
fujisawa.gifu@gmail.com

Received: 11/27/13, Revised: 11/9/14, Accepted: 12/13/14, Published: 1/19/15

Abstract

Let p be an odd prime number, and X a large real number. In this note, we consider the lower and upper bounds of the number of pure number fields of degree p with the absolute values of discriminants at most X by elementary methods.

1. Introduction

Let n be a positive integer, X a large positive number, and $N_n(X)$ the number of number fields F of degree n with $|d(F)| \le X$. Here $d(F)$ is the discriminant of a number field F. A well-known conjecture asserts that

$$N_n(X) \sim c_n X$$

for some c_n. This conjecture has been proved for $n = 2$, 3, 4, and 5 ([3], [1], [2]). However, this problem is very difficult and deep. In this paper, we consider the distribution of pure number fields of odd prime degree by elementary methods.

Let p be an odd prime number, and F a number field of degree p. If there exists a p-free positive integer $n > 1$ such that $F = \mathbb{Q}(\sqrt[p]{n})$, then we shall call F a pure number field of degree p. (If there is no prime number l such that $l^k | n$, then n is said to be k-free.) For $X > 0$, we denote the number of pure number fields F of degree p with $|d(F)| \le X$ by $P_p(X)$.

Theorem 1. *For an odd prime number p, we have*

$$\frac{B_p}{\zeta(2)} X^{\frac{1}{p-1}} \le P_p(X) \le \frac{A_p}{\zeta(p)} X$$

where $\zeta(s)$ is the Riemann zeta function,

$$A_p = \frac{p^{p+1} - p^{p-1} + p^{p-2} - 1}{(p^p - 1)p^p},$$

and

$$B_p = \frac{1}{(p+1)p^{\frac{p-2}{p-1}}} + \frac{p}{(p+1)p^{\frac{p}{p-1}}}.$$

For example, $P_3(X)$ is the number of pure cubic fields F with $|d(F)| \leq X$, and

$$\frac{1}{2\sqrt{3}\zeta(2)}\sqrt{X} \leq P_3(X) \leq \frac{37}{351\zeta(3)}X.$$

To show this theorem, we use two important lemmas.

First, we explain a result of Cohen and Robinson [4]. Let k, $q > 1$ be positive integers, $a \in \mathbb{Z}/q\mathbb{Z}$, and X a real positive large number. We set

$$Q_k(X; a, q) = \sharp\{n : k\text{-free} \leq X, n \equiv a\ (mod\ q)\}.$$

If there is a k-free positive integer n such that $n \equiv a\ (mod\ q)$, then $n = cq + a$ for some $c \in \mathbb{Z}$ and $gcd(a, q)$ must be k-free. Thus, since $Q_k(X; a, q) = 0$ when $gcd(a, q)$ is not k-free, we assume $gcd(a, q)$ is k-free.

A divisor $d > 0$ of q is called a unitary divisor when $gcd(d, q/d) = 1$. If d is a unitary divisor of q, we write $d|_*q$. The largest unitary divisor of q which is a divisor of a is denoted by $(a, q)_*$. Moreover, we denote the core of H by H_0. Namely, H_0 is the largest square-free divisor of H.

In [4], Cohen and Robinson proved the following result.

Lemma 1. *Let $H := (a, q)_*$. We have*

$$Q_k(X; a, q) = \frac{q^{k-1}}{J_k(q)} \frac{\varphi^*(H_0^k/H)}{H_0^k/H} \frac{1}{\zeta(k)} X + O(\sqrt[k]{X})$$

where

$$J_k(n) = n^k \prod_{\substack{l|n \\ l:prime}} \left(1 - \frac{1}{l^k}\right)$$

and

$$\varphi^*(n) = n \prod_{\substack{l^e|_*n \\ l:prime}} \left(1 - \frac{1}{l^e}\right).$$

For example, if $H = 1$, then

$$Q_k(X; a, q) = \frac{1}{q} \prod_{\substack{l|q \\ l:\mathrm{prime}}} \left(1 - \frac{1}{l^k}\right)^{-1} \frac{1}{\zeta(k)} X + O(\sqrt[k]{X}).$$

Next lemma computes the discriminants of pure number fields.

Lemma 2 (Fujisaki [5], p.133). *Let p be an odd prime number, n a p-free positive integer, and n_0 the core of n. Put $F = \mathbb{Q}(\sqrt[p]{n})$. We have*

$$d(F) = \begin{cases} (-1)^{\frac{p-1}{2}} p^{p-2} (n_0)^{p-1} & \text{if } n^{p-1} \equiv 1 \mod p^2, \\ (-1)^{\frac{p-1}{2}} p^{p} (n_0)^{p-1} & \text{if } n^{p-1} \not\equiv 1 \mod p^2. \end{cases}$$

Since the author doesn't find the proof of this lemma in the literature, and the original proof was published in Japanese, we shall sketch the proof here. Every p-free positive integer n can be put uniquely into the form $n = \prod_{i=1}^{p-1} a_i^i$ where $a_i \in \mathbb{Z}_{>0}$ and $n_0 = \prod_{i=1}^{p-1} a_i$. Put

$$\alpha_j = \left(\prod_{i=1}^{p-1} a_i^{ij - [\frac{ij}{p}]p} \right)^{\frac{1}{p}}$$

for $j = 0, 1, \cdots, p-1$. Let $\mathfrak{n}$ be the $\mathbb{Z}$-module generated by $\alpha_0, \cdots, \alpha_{p-1}$. We can check $d(\mathfrak{n}) = (O_F : \mathfrak{n})^2 d(F)$ where O_F is the ring of integers of F, and $d(\mathfrak{n})$ is the discriminant of $\mathfrak{n}$ as $\mathbb{Z}$-module. By algebraic argument, we obtain

$$d(\mathfrak{n}) = (-1)^{\frac{p-1}{2}} p^p (n_0)^{p-1}$$

and

$$(O_F : \mathfrak{n}) = \begin{cases} p & \text{if } n^{p-1} \equiv 1 \mod p^2, \\ 1 & \text{if } n^{p-1} \not\equiv 1 \mod p^2. \end{cases}$$

For more details, refer to [5].

2. Proof

First, we consider the upper bound. It is obvious that

$$\begin{aligned} P_p(X) &\leq \sharp\{n : p\text{-free} > 1, |d(\mathbb{Q}(\sqrt[p]{n}))| \leq X\} \\ &= \sum_{a=1}^{p^2} \sharp\{n : p\text{-free} > 1, n \equiv a (\text{mod } p^2), |d(\mathbb{Q}(\sqrt[p]{n}))| \leq X\} \\ &=: \sum_{a=1}^{p^2} P_{p,a}(X). \end{aligned}$$

If $a^{p-1} \equiv 1 (\text{mod } p^2)$, we have

$$P_{p,a}(X) = \sharp\{n : p\text{-free} > 1, n \equiv a (\text{mod } p^2), p^{p-2} n_0^{p-1} \leq X\}$$

by Lemma 2. Since $n \le n_0^{p-1}$ for p-free number n, we see

$$P_{p,a}(X) \le Q_p\left(\frac{X}{p^{p-2}}; a, p^2\right)$$

in this case. Similarly, if $a^{p-1} \not\equiv 1 (\text{mod } p^2)$, we obtain

$$P_{p,a}(X) \le Q_p\left(\frac{X}{p^{p}}; a, p^2\right)$$

by Lemma 2.

We can estimate $Q_p(X; a, p^2)$ for $a = 1, 2, \cdots, p^2$ by using Lemma 1. Note that $(a, p^2)_* = p^2$ if $a = p^2$ and $(a, p^2)_* = 1$ otherwise. Thus, we have

$$Q_p(X; a, p^2) \sim \frac{p^{p-2}}{p^p - 1}\frac{1}{\zeta(p)}X,$$

when $a = 1, \cdots, p^2 - 1$, and

$$Q_p(X; p^2, p^2) \sim \frac{p^{p-2} - 1}{p^p - 1}\frac{1}{\zeta(p)}X.$$

Therefore, for a large number X, we obtain that

$$\begin{aligned}
P_p(X) &= \sum_{a^{p-1} \equiv 1 (\text{mod } p^2)} P_{p,a}(X) + \sum_{a^{p-1} \not\equiv 1 (\text{mod } p^2)} P_{p,a}(X) \\
&\le \sum_{a^{p-1} \equiv 1 (\text{mod } p^2)} Q_p\left(\frac{X}{p^{p-2}}; a, p^2\right) + \sum_{a^{p-1} \not\equiv 1 (\text{mod } p^2)} Q_p\left(\frac{X}{p^{p}}; a, p^2\right) \\
&\sim \sum_{a^{p-1} \equiv 1 (\text{mod } p^2)} \frac{p^{p-2}}{p^p - 1}\frac{1}{\zeta(p)}\frac{X}{p^{p-2}} + \sum_{\substack{a^{p-1} \not\equiv 1 (\text{mod } p^2) \\ a \ne p^2}} \frac{p^{p-2}}{p^p - 1}\frac{1}{\zeta(p)}\frac{X}{p^{p}} \\
&+ \frac{p^{p-2} - 1}{p^p - 1}\frac{1}{\zeta(p)}\frac{X}{p^p} \\
&= \left((p-1)\frac{p^{p-2}}{(p^p - 1)p^{p-2}} + (p^2 - p)\frac{p^{p-2}}{(p^p - 1)p^p} + \frac{p^{p-2} - 1}{(p^p - 1)p^p}\right)\frac{X}{\zeta(p)} \\
&= \left(\frac{p^{p+1} - p^{p-1} + p^{p-2} - 1}{(p^p - 1)p^p}\right)\frac{X}{\zeta(p)}.
\end{aligned}$$

Thus, we have proved that $P_p(X) \le A_p X/\zeta(p)$.

Finally, we consider the lower bound. Since $\mathbb{Q}(\sqrt[p]{n}) \ne \mathbb{Q}(\sqrt[p]{m})$ for distinct square-free numbers m and n, it is obvious that

$$\begin{aligned} P_p(X) &\geq \sharp\{n : \text{square-free} > 1, d(\mathbb{Q}(\sqrt[p]{n})) \leq X\} \\ &= \sum_{a=1}^{p^2} \sharp\{n : \text{square-free} > 1, n \equiv a (\text{mod } p^2), d(\mathbb{Q}(\sqrt[p]{n})) \leq X\} \\ &=: \sum_{a=1}^{p^2} P'_{p,a}(X). \end{aligned}$$

If $a^{p-1} \equiv 1 (\text{mod } p^2)$, we have

$$P'_{p,a}(X) = \sharp\{n : \text{square-free} > 1, n \equiv a (\text{mod } p^2), p^{p-2} n_0^{p-1} \leq X\}$$

by Lemma 2. Since $n^{p-1} \geq n_0^{p-1}$, we see

$$P'_{p,a}(X) \geq Q_2 \left(\left(\frac{X}{p^{p-2}} \right)^{\frac{1}{p-1}} ; a, p^2 \right)$$

in this case. Similarly, if $a^{p-1} \not\equiv 1 (\text{mod } p^2)$, we obtain

$$P'_{p,a}(X) \geq Q_2 \left(\left(\frac{X}{p^{p}} \right)^{\frac{1}{p-1}} ; a, p^2 \right)$$

by Lemma 2.

Since $gcd(p^2, p^2) = p^2$ is not square-free, we see that

$$Q_2(X; p^2, p^2) = 0.$$

By Lemma 1, we have

$$Q_2(X; a, p^2) \sim \frac{1}{(p^2-1)\zeta(2)} X$$

for $a = 1, 2, \cdots, p^2 - 1$.

Therefore, for a large number X, we obtain that

$$\begin{aligned} P_p(X) &\geq \sum_{a^{p-1} \equiv 1 (\text{mod } p^2)} Q_2 \left(\left(\frac{X}{p^{p-2}} \right)^{\frac{1}{p-1}} ; a, p^2 \right) + \sum_{\substack{a^{p-1} \not\equiv 1 (\text{mod } p^2) \\ a \neq p^2}} Q_2 \left(\left(\frac{X}{p^{p}} \right)^{\frac{1}{p-1}} ; a, p^2 \right) \\ &\sim (p-1) \frac{1}{(p^2-1)\zeta(2)} \left(\frac{X}{p^{p-2}} \right)^{\frac{1}{p-1}} + (p^2 - p) \frac{1}{(p^2-1)\zeta(2)} \left(\frac{X}{p^{p}} \right)^{\frac{1}{p-1}} \\ &= \left(\frac{1}{(p+1) p^{\frac{p-2}{p-1}}} + \frac{p}{(p+1) p^{\frac{p}{p-1}}} \right) \frac{X^{\frac{1}{p-1}}}{\zeta(2)}. \end{aligned}$$

Thus, it holds that $P_p(X) \geq B_p X^{\frac{1}{p-1}}/\zeta(2)$. This completes the proof of the assertion.

Acknowledgements. The author would like to thank the anonymous referee and Professor Hiroshi Suzuki for carefully reading the first version of this paper and for making helpful comments and suggestions.

References

[1] M. Bhargava, *The density of discriminants of quartic rings and fields*, Ann. of Math. **162** (2005), 1031–1063.

[2] M. Bhargava, *The density of discriminants of quintic rings and fields*, Ann. of Math. **172** (2010), 1559–1591.

[3] H. Davenport and H. Heilbronn, *On the density of discriminants of cubic fields. II*, Proc. Royal Soc. London Ser. A **322** (1971), 405–420.

[4] E. Cohen and R. L. Robinson, *On the distribution of the k-free integers in residue classes*, Acta Arith. **8** (1962/1963), 283–293. errata, ibid. **10** (1964/1965), 443.

[5] G. Fujisaki, *daisuteki seisuron nyumon ge*, (in Japanese) shokabo, 1975.