Existence of the solutions to the Brocard-Ramanujan problem for norm forms[1]

Wataru Takeda

Tokyo University of Science, Japan

To appear in Proc. Amer. Math. Soc. Ser. B

[1]This work was supported by JSPS KAKENHI JP22K13900.

Brocard-Ramanujan problem

Find integer solutions (x, ℓ) to

$$x^2 - 1 = \ell!. \tag{1}$$

$$\begin{aligned} 5^2 - 1 &= 24 = 4!, \\ 11^2 - 1 &= 120 = 5!, \\ 71^2 - 1 &= 5040 = 7!. \\ &\vdots \end{aligned}$$

Brocard-Ramanujan problem(1885,1913)

Are there only finitely many solutions to $x^2 - 1 = \ell!$? Moreover, are all solutions $(x, \ell) = (5, 4), (11, 5)$ and $(71, 7)$?

Conditional results

Theorem (Overholt 1993($A = 1$), Dąbrowski 1996)

If the weak Szpiro conjecture holds, then for any square A,

$$\#\{(x, \ell) \mid x^2 - A = \ell!\} < \infty.$$

- The abc conjecture implies the weak Szpiro conjecture.

Theorem (Luca 2002)

Let $P(x) \in \mathbb{Z}[x]$ be a polynomial with $\deg P \geq 2$. If the abc conjecture holds, then

$$\#\{(x, \ell) \mid P(x) = \ell!\} < \infty.$$

Unconditional results(one variable)

Theorem (Berend-Harmse 2006)

If a polynomial $P(x) \in \mathbb{Z}[x]$ with $\deg P \geq 2$ is irreducible or satisfies some condition (Condition A), then

$$\#\{(x, \ell) \mid P(x) = \ell!\} < \infty.$$

Polynomials $P(x) = x(x^2+1), (x^2+x+1)(x^3-2), \ldots$ satisfy Condition A.

Unconditional results(multi-variable)

Theorem (Erdős-Obláth 1937)

- *For* $n \geq 2$,

$$\{(x, y, \ell) \mid x^n + y^n = \ell!, \gcd(x, y) = 1\} = \{(1, 1, 2)\}.$$

- *For* $n = 3, n \geq 5$,

$$\{(x, y, \ell) \mid x^n - y^n = \ell!, \gcd(x, y) = 1\} = \emptyset.$$

Theorem (Pollack-Shapiro 1973)

The equation $x^4 - 1 = \ell!$ *has no solution* (x, ℓ).

Previous results

Norm form

Let K be a number field. Then the norm form N_K is defined by

$$N_K(\boldsymbol{x}) = \prod_{\sigma : K \to \mathbb{C}} \sigma(\boldsymbol{x}).$$

- $N_{\mathbb{Q}(\sqrt{2})}(x_1 + \sqrt{2}x_2) = (x_1 + \sqrt{2}x_2)(x_1 - \sqrt{2}x_2) = x_1^2 - 2x_2^2$;
- $N_{\mathbb{Q}(\sqrt[3]{a})}(x_1 + x_2\sqrt[3]{a} + x_3\sqrt[3]{a^2}) = x_1^3 + ax_2^3 + a^2x_3^3 - 3ax_1x_2x_3$.

Theorem (T. 2021)

Let $K \neq \mathbb{Q}$ be a number field and let $\mathcal{O}_K$ be its ring of integers. Then

$$\#S(K) = \#\{\ell \geq 2 \mid \exists \boldsymbol{x} \in \mathcal{O}_K \text{ s.t. } N_K(\boldsymbol{x}) = \ell!\} < \infty.$$

The existence of solutions(Today's main topic)

Question

- How many $\#S(K) = \#\{\ell \geq 2 \mid \exists \boldsymbol{x} \in \mathcal{O}_K \text{ s.t. } N_K(\boldsymbol{x}) = \ell!\}$?

- $S(\mathbb{Q}) = \mathbb{Z}_{\geq 2}$.
- $S(\mathbb{Q}(\sqrt{-1})) = \{2, 6\}$. (Erdős-Obláth 1937).
- $S(\mathbb{Q}(\sqrt{-43})) = S(\mathbb{Q}(\sqrt{-67})) = S(\mathbb{Q}(\sqrt{-163})) = \emptyset$.

Observation

Infiniteness of K with $S(K) \neq \emptyset$

For fixed integer n, there exist infinitely many number fields K such that $[K : \mathbb{Q}] = n$ and $S(K) \neq \emptyset$.

- We consider $K = \mathbb{Q}(\sqrt[n]{-\ell!})$.
- Let $\ell! = m^n k$, where k is the n-th power-free part of $\ell!$.
- $m\sqrt[n]{-k} \in \mathcal{O}_K$.

$\rightarrow$ $N_K((-1)^n m\sqrt[n]{-k}) = \ell!$.

Main Theorems(1/2)

Theorem 1 (T. 2023)

Let $K = \mathbb{Q}(\sqrt[n]{2})$.

1. *If* $\gcd(n, 6) = 1$, *then* $\{\ell \mid 2 \leq \ell \leq 10\} \subset S(K)$;
2. *if* $\gcd(n, 30) = 1$, *then* $\{\ell \mid 2 \leq \ell \leq 22\} \subset S(K)$.

This implies that there are infinitely many number fields K *with* $\#S(K) \geq 21$.

Main Theorems(2/2)

Theorem 2 (T. 2023)

Let a, n be integers. If the class number of $K = \mathbb{Q}(\sqrt[n]{a})$ is 1, then

$$\{\ell \mid 2 \leq \ell \leq M - 1\} \subset S(K),$$

where $M = M(n, a)$ is the minimum of $S_1(n, a) \cup S_2(n, a) \cup S_3(n, a)$, in which

$$S_1(n, a) = \{p : \textit{prime} \mid \gcd(p - 1, n) > 1\};$$
$$S_2(n, a) = \{p : \textit{prime} \mid p^2 | a\};$$
$$S_3(n, a) = \{p : \textit{prime} \mid p | n, a^{p-1} \equiv 1 \mod p^2\}.$$

Integers represented as $N_K(1/2)$

Prime ideal factorization

Any ideal $\boldsymbol{a}$ can be decomposed into a product of prime ideals as

$$\boldsymbol{a} = \prod_{i=1}^{g} \mathcal{P}_i^{e_i}.$$

Let $f_i = [\mathcal{O}_K/\mathcal{P}_i : \mathbb{Z}/p\mathbb{Z}]$ be the inertia degree.

$$N = x^2 + y^2 \ (\leftrightarrow K = \mathbb{Q}(\sqrt{-1}))$$
$$\iff N = 2^{\alpha} \prod_{p \equiv 1 \mod 4} p^{\beta_p} \prod_{q \equiv 3 \mod 4} q^{2\gamma_q} \ (\alpha, \beta_p, \gamma_q \in \mathbb{Z}_{\geq 0}).$$

$p \equiv 1 \mod 4 \iff p\mathcal{O}_K = \mathcal{P}_1\mathcal{P}_2$ and $f_i = 1$,
$p \equiv 3 \mod 4 \iff p\mathcal{O}_K$ is prime and $f_1 = 2$.

Integers represented as $N_K(2/2)$

Lemma 3

Let p be a prime with $f_i \geq 2$ for any $\mathcal{P}_i | p\mathcal{O}_K$. Then, for $\ell \in [p, 2p)$, there are no $\boldsymbol{x} \in \mathcal{O}_K$ such that $N_K(\boldsymbol{x}) = \ell!$.

We define

$$\mathrm{P}_K = \{p \mid \exists \mathcal{P}_i | p\mathcal{O}_K \text{ s.t. } f_i = 1\}.$$

- Let $K = \mathbb{Q}(\sqrt{-1})$. Then, $\mathrm{P}_K = \{p \mid p \equiv 1 \mod 4\}$.
- When $K = \mathbb{Q}(\sqrt[3]{2})$, the set P_K has density $\frac{2}{3}$ in primes.

Chebotarev's density theorem

Chebotarev's density theorem($\mathbb{Q}$ ver.)

Let $C \subset G$ be a stable subset under conjugation. Then

$$\frac{\#\{p \leq x \mid [(p, K/\mathbb{Q})] = C\}}{\#\{p \leq x\}} = \frac{\#C}{\#G}.$$

If $K/\mathbb{Q}$ is a Galois extension, then

$$p \in \mathrm{P}_K \Longleftrightarrow (p, K/\mathbb{Q}) = \mathrm{id}.$$

Radical fields vs Galois fields

In this slide, n is odd integer.

Radical fields $\mathbb{Q}(\sqrt[n]{a})$

inertia degree	Density
$m \geq 2, *, *$	$\frac{n-1}{n\varphi(n)}$
$1, *, *$	$\frac{\varphi(n)-1}{\varphi(n)}$
$1, \ldots, 1$	$\frac{1}{n\varphi(n)}$

} P_k

Galois extension with extension degree n

inertia degree	Density
$m, \ldots, m \geq 2$	$\frac{n-1}{n}$
$1, \ldots, 1$	$\frac{1}{n}$

} P_k

Proof of Theorem 1

Theorem (Theorem 1)

Let $K = \mathbb{Q}(\sqrt[n]{2})$. For all positive odd integers relatively prime to 30,

$$\{\ell \mid 2 \leq \ell \leq 22\} \subset S(K).$$

We have

$$N_K(\sqrt[n]{2}) = 2, \qquad N_K(1+\sqrt[n]{2}) = 3,$$
$$N_K(1+\sqrt[n]{4}) = 5, \qquad N_K(-1+\sqrt[n]{8}) = 7,$$
$$N_K(1-\sqrt[n]{2}+\sqrt[n]{4}-\sqrt[n]{8}+\sqrt[n]{16}) = 11, \qquad N_K(1-\sqrt[n]{4}+\sqrt[n]{16}) = 13,$$
$$N_K(1+\sqrt[n]{16}) = 17, \qquad N_K(1-\sqrt[n]{8}+\sqrt[n]{64}) = 57 = 3 \cdot 19$$

By the multiplicity of norms, we conclude the assertion.

Theorem 2

We review Theorem 2 again.

Theorem (T. 2023)

Let a, n be integers. If the class number of $K = \mathbb{Q}(\sqrt[n]{a})$ is 1, then

$$\{\ell \mid 2 \leq \ell \leq M - 1\} \subset S(K),$$

where $M = M(n, a)$ is the minimum of $S_1(n, a) \cup S_2(n, a) \cup S_3(n, a)$, in which

$$S_1(n, a) = \{p : \textit{prime} \mid \gcd(p - 1, n) > 1\};$$
$$S_2(n, a) = \{p : \textit{prime} \mid p^2 | a\};$$
$$S_3(n, a) = \{p : \textit{prime} \mid p | n, a^{p-1} \equiv 1 \mod p^2\}.$$

Proof of Theorem 2(1/2)

We will show that for any primes $p \notin S_1(n,a) \cup S_2(n,a) \cup S_3(n,a)$, there exists a prime ideal $x\mathcal{O}_K$ lying above p with $N_K(x) = p$, that is, the inertia degree of $x\mathcal{O}_K$ is 1.

We assume that $p \notin S_1(n,a) = \{p : \text{prime} \mid \gcd(p-1,n) > 1\}$.

- For any prime p with $\gcd(p-1,n) = 1$ or $\gcd(p,a) = 1$, there exists $b \in \mathbb{Z}$ such that $b^n - a \equiv 0 \mod p$.

$\rightarrow$ There exists a prime ideal $x\mathcal{O}_K$ lying above p with $N_K(x) = p$.

Proof of Theorem 2(2/2)

We assume that $p \notin S_2(n,a) = \{p : \text{prime} \mid p^2|a\}$.

- If $p||a$, then $x^n - a$ is an Eisenstein polynomial at p.

$\rightarrow$ The prime p ramifies totally in $K = \mathbb{Q}(\sqrt[n]{a})$.

$\rightarrow$ We have $p\mathcal{O}_K = \mathcal{P}_1^n$ and $f_1 = 1$.

$\rightarrow$ There exists a prime ideal $x\mathcal{O}_K$ lying above p with $N_K(x) = p$.

We assume that $p \notin S_3(n,a) = \{p : \text{prime} \mid p|n, a^{p-1} \equiv 1 \mod p^2\}$.

- If $p^r||n$ and $a^{p-1} \equiv 1 \mod p^2$, then $a^{p^r} \not\equiv a \mod p^2$.

$\rightarrow$ The polynomial $(x+a)^{p^r} - a = x^n + \cdots + a^{p^r} - a$ is an Eisenstein polynomial at p.

$\rightarrow$ The prime p ramifies totally in $K = \mathbb{Q}(\sqrt[p^r]{a})$.

Further examples

$K = \mathbb{Q}(\sqrt[p]{2})$

If $p = 7$, then

$$\{\ell \mid 2 \leq \ell \leq 28\} \subset S(K).$$

If $p = 17$, then

$$\{\ell \mid 2 \leq \ell \leq 102\} \subset S(K).$$

If $p = 19$, then

$$\{\ell \mid 2 \leq \ell \leq 190\} \subset S(K).$$

Finteness of solution

We define

$$\mathrm{NP}_K = \{\text{primes}\} \setminus \mathrm{P}_K = \{p \mid f_i \geq 2 \text{ for any } \mathcal{P}_i | p\mathcal{O}_K\}.$$

Lemma 4 (T. 2021 cf. T. 2019, 2023)

There exists an effectively computable constant $c(K) > 0$ such that for $x > c(K)$, there is a prime $p \in \mathrm{NP}_K \cap (x, 2x)$.

Combining Lemma 3 and Lemma 4, we obtain the finiteness of solutions.

Theorem (T. 2021)

Let $K \neq \mathbb{Q}$ be a number field and let $\mathcal{O}_K$ be its ring of integers. Then

$$\#S(K) = \#\{\ell \geq 2 \mid \exists \boldsymbol{x} \in \mathcal{O}_K \text{ s.t. } N_K(\boldsymbol{x}) = \ell!\} < \infty.$$