On the Brocard-Ramanujan problem for homogeneous polynomials

Wataru Takeda

Abstract. This is a report of the author's talk in RIMS Workshop 2019 "Analytic Number Theory and Related Topics". We summarize the author's talk in the first half of this report and explain our recent results related to the Brocard-Ramanujan problem in the second half.

1. The Brocard-Ramanujan problem

Brocard and Ramanujan conjectured that the only solutions of the equation $x^2-1=l!$ are $(x,l)=(5,4),(11,5)$ and $(71,7)$ independently [Br76, Br85, Ra13]. More generally, it is proposed that there are only finitely many solutions of the polynomial-factorial Diophantine equation

$$P(x)=l!, \tag{1.1}$$

where $P(x)$ is a polynomial of degree 2 or more with integer coefficients.

This problem excludes the case $\deg P=1$. In this case, we can observe that if $a_1|a_0$ the equation $a_1x+a_0=l!$ has infinitely many solutions (x,l), and otherwise has only finitely many solutions easily.

Erdős and Obláth considered the equation $x^m\pm y^m=l!$ as one of the generalizations of the equation $x^2-1=l!$. They showed that for $m\geq 3$ the equation $x^m+y^m=l!$ has no solution with $\gcd(x,y)=1$ except for $(x,y,l)=(1,1,2)$ and $x^m-y^m=l!$ has no solution with $\gcd(x,y)=1$ except for $m=4$ [EO37]. For the remaining case, Pollack and Shapiro showed that $x^4-1=l!$ also has no solution [PS73].

Berend and Osgood dealt with all polynomial $P(x)\in\mathbf{Z}[x]$ and showed that for any polynomial P of degree 2 or more with integer coefficients, the equation $P(x)=l!$ has only a density 0 set of solutions l [BO92], that is,

$$\lim_{n\to\infty}\frac{\#\{l\leq n\mid \text{there exists } x\in\mathbf{Z} \text{ such that } P(x)=l!\}}{n}=0.$$

2010 *Mathematics Subject Classification.* 11D09,11D45,11D72, 11D85.

Key words and phrases. quadratic form, Diophantine equation, finiteness of solutions, generalized Brocard-Ramanujan problem.

In 2006, Berend and Harmse considered several related problems. They considered the equation $P(x) = H_l$, where H_l is a function resembling the factorial function $l!$. They showed that for any polynomial P which is an irreducible polynomial or satisfies some condition, there exist only finitely many solutions of $P(x) = H_l$ [BH06]. They chose the following four sequence as H_l,

- $H_l = l!$.
- $H_l = [1, 2, \ldots, l]$,
  where $[1, 2, \ldots, l]$ is the least common multiple of all positive integers less than or equal to l.
- $H_l = p_1 p_2 \cdots p_l$,
  where $2 = p_1 < p_2 < \cdots < p_l < \cdots$ is the sequence of all primes.
- For fixed integer a,

$$H_l = \binom{al}{l, \ldots, l} = \frac{(al)!}{(l!)^a}$$

In the author's talk, we focus on the equation

$$\sum_{i=0}^{n} a_i x^i y^{n-i} = \Pi_K(l), \tag{1.2}$$

where $a_i \in \mathbf{Z}$ and Π_K is generalized factorial function over number fields. Let K be a number field and $\mathcal{O}_K$ be its ring of integers. Then the function $\Pi_K(l)$ is defined by

$$\Pi_K(l) = \prod_{\substack{\mathfrak{a}:\text{ideal} \\ \mathfrak{N}\mathfrak{a} \leq l}} \mathfrak{N}\mathfrak{a},$$

where $\mathfrak{N}\mathfrak{a} = \#\mathcal{O}_K/\mathfrak{a}$.

We study the number of not (x, y, l) but l for which there exists a pair (x, y) such that $a_n x^n + \cdots + a_0 y^n = \Pi_K(l)$ by the following reasons. It is known that when d is not a square integer $x^2 - dy^2 = 1$ has infinitely many solutions from the theory of Pell's equation. Therefore, we can find $x^2 - dy^2 = l!$ has infinitely many solutions (x, y, l) easily. To consider the relation between integers represented as polynomial and those of factorial, we consider the number of l for which there exists a pair (x, y) such that $a_n x^n + \cdots + a_0 y^n = \Pi_K(l)$. In the case $K = \mathbf{Q}$ and $y = 1$, equation (1.2) is reduced to the generalized Brocard-Ramanujan's equation (1.1). Therefore, it is expected that our results give some improvement of the generalized Brocard-Ramanujan problem.

2. Integers represented as polynomial

First, we recall some basic definitions and some propositions of algebraic number theory. Let $P(x) = a_n x^n + \cdots + a_0 \in \mathbf{Z}[x]$ be an irreducible polynomial with $\deg P = n$ and the discriminant Δ_P. When $\alpha_1, \ldots, \alpha_n$ are roots of P, the splitting field K_P of P is $\mathbf{Q}(\alpha_1, \ldots, \alpha_n)$. It is known that $K_P/\mathbf{Q}$ is a Galois extension and the Galois closure of $\mathbf{Q}(\alpha_i)/\mathbf{Q}$ for all $i = 1, \ldots, n$. The Galois group G_P of $K_P/\mathbf{Q}$ plays a crucial role in splitting of primes in $\mathbf{Q}(\alpha_i)$ as follows.

We call a subgroup H of S_n transitive if the group orbit $H(i) = \{\sigma(i) \mid \sigma \in H\}$ is equal to $\{1, \ldots, n\}$ for $1 \leq i \leq n$. From Galois Theory, Galois group G_P can be identified with a transitive subgroup H of the symmetric group S_n of degree n. For $\sigma \in H$, the cycle type of σ is defined as the ascending ordered list $[f_1, \ldots, f_r]$ of the sizes of the cycles in the cycle decomposition of σ. For example, the cycle type of $(1\ 2)(3\ 4)(6\ 7\ 8) = (1\ 2)(3\ 4)(5)(6\ 7\ 8)(9) \in H \subset S_9$ is $[1, 1, 2, 2, 3]$. Since if two permutations are conjugate in H then they have the same cycle type, we can define the cycle type of conjugacy class $C = [\sigma]$ of H by the cycle type of a representative σ. We introduce a lemma for transitive subgroups of the symmetric group S_n.

Lemma 2.1. Let H be a transitive subgroup of the symmetric group S_n of degree $n \geq 2$. Then there exists an element $\sigma \in H$ such that $\sigma(i) \neq i$ for all $i = 1, \ldots, n$.

This lemma ensures that for any Galois group $G \neq \{1\}$ of splitting field of polynomial P, there exists an element such that it fixes no roots of P.

Next, we review the definitions and properties of the Frobenius map. Let p be a prime and $\mathfrak{P}$ prime ideal of $\mathcal{O}_{K_P}$ lying above p. For prime ideal $\mathfrak{P}$ in $\mathcal{O}_{K_P}$, we define the decomposition group $D_{\mathfrak{P}}$ of $\mathfrak{P}$ by $\{\sigma \in G_P \mid \sigma(\mathfrak{P}) = \mathfrak{P}\}$. Since $\sigma(\mathfrak{P}) = \mathfrak{P}$ and $\sigma(\mathcal{O}_{K_P}) = \mathcal{O}_{K_P}$ for $\sigma \in D_{\mathfrak{P}}$, σ induces an automorphism $\overline{\sigma}$ of $\mathcal{O}_{K_P}/\mathfrak{P}$ over $\mathbf{Z}/p\mathbf{Z}$. Now we consider the Galois group $\mathrm{Gal}((\mathcal{O}_{K_P}/\mathfrak{P})/(\mathbf{Z}/p\mathbf{Z}))$. It is known that this group is cyclic and there exists an unique automorphism $\sigma : x \to x^p$ which generates it. Then the Frobenius map $(p, K_P/\mathbf{Q})$ of p is the image of σ in Galois group G_P. If the Frobenius map $(p, K_P/\mathbf{Q})$ of p belongs to a conjugacy class C of G_P, then we say that p corresponds to C. We denote the set of primes corresponding to $C \in \mathcal{C}$ by $\mathbf{P}(\mathcal{C})$. The following theorem gives a relation between the cycle type of Frobenius map of p and the monic irreducible factorization of $P(x) \mod p$, where p does not divide $a_n \Delta_P$.

Theorem 2.2 (Frobenius)**.** Let p be a prime such that p does not divide $a_n\Delta_P$. We denote the cycle type of the Frobenius map $(p, K_P/\mathbf{Q})$ of p by $[f_1, \ldots, f_r]$. Then the monic irreducible factorization of $P(x)$ mod p is $P(x) \equiv a_n P_1(x) \cdots P_r(x) \mod p$, where $P_i(x)$ are distinct and $f_i = \deg P_i(x)$.

In the following, we introduce auxiliary lemmas to show the main theorems. The following lemmas characterize the prime factorization of integers which can be written as a polynomial. Let $F(x, y) = a_n x^n + a_{n-1}x^{n-1}y + \cdots + a_0 y^n$ be an irreducible homogeneous polynomial and K_F the splitting field of $F(x, 1)$. Also, we define the modified discriminant $\Delta_{F,mod}$ by

$$\Delta_{F,mod} = \frac{\Delta_F}{\gcd(a_n, a_{n-1}, \ldots, a_0)^{2n-2}},$$

where Δ_F is the discriminant of $F(x, 1)$. Let $\mathcal{C}_F$ be the set of conjugacy classes C of the Galois group $G_F = \mathrm{Gal}(K_F/\mathbf{Q})$ whose cycle type $[f_1, \ldots, f_r]$ satisfies $f_i \geq 2$ for all $i = 1, \ldots, r$. This classification is very important to characterize integers represented as $F(x, y)$.

Lemma 2.3. Let $F(x, y) = a_n x^n + a_{n-1}x^{n-1}y + \cdots + a_0 y^n$ be a homogeneous polynomial whose irreducible factorization is

$$F(x, y) = \prod_{j=1}^{u} F_j(x, y)$$

and $g = \gcd(a_n, a_{n-1}, \ldots, a_0)$. Let N be an integer with

$$N = g p_1 \cdots p_s q_1^{l_1} \cdots q_t^{l_t},$$

where q_i are distinct primes corresponding to $C \in \mathcal{C}_{F_j}$ for all j with $\gcd(q_i, a_n\Delta_{F,mod}) = 1$ or $\gcd(q_i, a_0\Delta_{F,mod}) = 1$ and p_i are the other primes. If N is represented as $F(x, y)$ then $n|l_i$ for all i.

Next we change the assumption of Lemma 2.3 and give a necessary and sufficient condition for integers represented as $F(x, y)$. We call a discriminant $\Delta_{F,mod}$ fundamental, if one of the following statements holds;

- $\Delta_{F,mod} \equiv 1 \mod 4$ and is square-free,
- $\Delta_{F,mod} = 4m$, where $m \equiv 2$ or $3 \mod 4$ and m is square-free.

In the following, we assume that one of a and c is a prime number or 1 and the discriminant $\Delta_{F,mod}$ is fundamental. We characterize the prime factorization of integers which are expressed as $ax^2 + bxy + cy^2$.

Lemma 2.4. Let $F(x,y) = ax^2 + bxy + cy^2$ be a positive definite quadratic form with fundamental modified discriminant $\Delta_{F,mod}$ and $g = \gcd(a,b,c)$. We denote the corresponding order to $\frac{F(x,y)}{g}$ by $\mathcal{O}$ and the set of principal ideals of $\mathcal{O}$ by $P_{\mathcal{O}}$. Let N be an integer with

$$aN = gp_1 \cdots p_s q_1 \cdots q_t r_1^{l_1} \cdots r_u^{l_u},$$

where p_i ramifies in $\mathbf{Q}(\sqrt{\Delta_F})$, q_i splits completely in $\mathbf{Q}(\sqrt{\Delta_F})$ and r_i are distinct inert primes in $\mathbf{Q}(\sqrt{\Delta_F})$. If a is a prime number or 1, then N is represented as $F(x,y)$ if and only if

1. l_i are even numbers.
2. There exist prime ideals $\mathfrak{p}_1, \ldots, \mathfrak{p}_s, \mathfrak{q}_1, \ldots, \mathfrak{q}_t$ lying above $p_1, \ldots, p_s, q_1, \ldots, q_t$ respectively such that

$$\mathfrak{p}_1 \cdots \mathfrak{p}_s \mathfrak{q}_1 \cdots \mathfrak{q}_t (r_1)^{\frac{l_1}{2}} \cdots (r_u)^{\frac{l_u}{2}} \in P_{\mathcal{O}}.$$

Remark 2.5. By swapping x and y in the binary form $ax^2+bxy+cy^2$, we can replace a by c in Lemma 2.4

In the following, we consider a Bertrand type estimate for primes corresponding to a conjugacy class C of Galois group G by following the way of Hulse and Murty. They gave one of the generalizations of Bertrand's postulate, or Chebyshev's theorem, to number fields [HM17]. We can obtain the following theorem, which gives a Bertrand type estimate for prime ideals $\mathfrak{p}$ corresponding to a conjugacy class C such that their ideal norm is of the form p^f, by following the argument of Hulse and Murty [HM17].

Theorem 2.6 (cf. [HM17, Ta19])**.** Let L be the Galois closure of $K/\mathbf{Q}$ with $k = [L : \mathbf{Q}]$ and p a prime corresponding to a conjugacy class C of $\mathrm{Gal}(L/\mathbf{Q})$. For any $A > 1$ there exists an effectively computable constant $c(A) > 0$ such that for $p^{f_i} > \exp(c(A)k(\log D_L)^2)$ there exists a prime ideal $\mathfrak{q}$ with $\mathfrak{N}\mathfrak{q} = q^{f_i} \in (p^{f_i}, Ap^{f_i})$, where $q \in \mathbf{P}(C)$.

3. Main results

In this section, we explain the main theorems of the author's talk. First, we consider the equation $a_n x^n + \cdots + a_0 y^n = l!$.

Theorem 3.1. Let $F(x,y) = a_n x^n + a_{n-1} x^{n-1} y + \cdots + a_0 y^n$ be a homogeneous irreducible polynomial with $\deg F \geq 2$, then there exist only finitely many l such that $l!$ is represented as $F(x,y)$.

Proof. Lemma 2.1 provides that $\mathcal{C}_F \neq \emptyset$. Let $C \in \mathcal{C}_F$ be a fixed conjugacy class of G_F. The assumption $\deg F \geq 2$ and Lemma 2.3 lead that if N is represented as $F(x,y)$ and $p|N$ for prime p corresponding to C

with $\gcd(q_i, a_n\Delta_{F,mod}) = 1$ or $\gcd(q_i, a_0\Delta_{F,mod}) = 1$, then N is divided by p^2 at least. In particular, $F(x,y) = p!$ has no integer solution (x,y). Moreover, since the second smallest positive integer divided by p is $2p$, $l!$ is not of the form in Lemma 2.3 for $p \leq l < 2p$, that is, there exists no pair $(x,y) \in \mathbf{Z}^2$ such that $F(x,y) = l!$ for $p \leq l < 2p$.

Let α be a root of $F(x,1)$ and let k be the extension degree of $K_F/\mathbf{Q}$. We denote the ring of integers of $\mathbf{Q}(\alpha)$ by $\mathcal{O}_\alpha$. Theorem 2.6 states that there exists $c > 0$ such that for $x > \exp(ck(\log D_{K_F})^2)$ there is a prime ideal $\mathfrak{p}$ of $\mathcal{O}_\alpha$ corresponding to C with $\mathfrak{N}\mathfrak{p} = p^f \in (x, 2x)$. Let $\mathfrak{p}$ be a prime ideal of $\mathcal{O}_\alpha$ corresponding to C with $\mathfrak{N}\mathfrak{p} = p^f > \max\{\exp(ck(\log D_{K_F})^2), (a_n\Delta_{F,mod})^f,\ (a_0\Delta_{F,mod})^f\}$. Since we have $p^f > \exp(ck(\log D_{K_F})^2)$, there exists $\mathfrak{q}$ corresponding to C with $\mathfrak{N}\mathfrak{q} = q^f \in (p^f, 2p^f)$, that is, there exists a prime q corresponding to C with $q \in (p, 2p)$.

As well as the above, $l!$ is not of the form in Lemma 2.3 for $q \leq l < 2q$ and there exists a prime q_1 corresponding to C with $q_1 \in (q, 2q)$. By induction, $l!$ is not of the form in Lemma 2.3 for $p \leq l$. This shows the finiteness of l such that $l!$ is represented as $F(x,y)$. □

As a corollary of this theorem, we obtain the result of Berend and Harmse for irreducible polynomial.

Theorem 3.2 (Theorem 3.1. of [BH06])**.** For any irreducible polynomial $P(x) \in \mathbf{Z}[x]$ with $\deg P \geq 2$, the equation $P(x) = H_l$ has only finitely many solutions (x,l).

Next we consider the general case $F(x,y) = \Pi_K(l)$. For a prime p and its Frobenius map $(p, K_P/\mathbf{Q})$ with cycle type $[f_1, \ldots, f_r]$, we define $G_p(l;K)$ as the number of f_i such that $f_i = l$. If $K/\mathbf{Q}$ is a Galois extension with extension degree k, then $fG_p(f;K) = k$ for all primes p unramified in K, where f is the inertia degree of p in K. Therefore, we obtain the following theorem.

Theorem 3.3. Let K be a Galois extension of $\mathbf{Q}$ and $F(x,y)$ a polynomial in $\mathbf{Z}[x,y]$ whose irreducible factorization is

$$F(x,y) = \prod_{j=1}^{u} F_j(x,y).$$

Assume that there exist a conjugacy class C of $\mathrm{Gal}(K/\mathbf{Q})$, positive integers a and $b > 1$ such that $\mathbf{P}(C) \cap \bigcap_i \mathbf{P}(\mathcal{C}_{F_i}) \supset \{p : \text{prime} \mid p \equiv a \mod b\}$. If $\deg F$ does not divide $[K : \mathbf{Q}]$ then there exist only finitely many l such that $\Pi_K(l)$ is represented as $F(x,y)$.

Since the p-factor of the above H_l appears with regularity, we can replace $\Pi_K(l)$ with H_l in Theorem 3.3. When $K = \mathbf{Q}$, the conjugacy class C in Theorem 3.3 is equal to $\{1\}$ and $\deg F$ does not divide $[K : \mathbf{Q}]$. Therefore, we obtain the following corollary.

Corollary 3.4. Let $F(x, y)$ a polynomial in $\mathbf{Z}[x, y]$ whose irreducible factorization is

$$F(x, y) = \prod_{j=1}^{u} F_j(x, y).$$

Assume that there exist positive integers a and $b > 1$ such that

$$\bigcap_i \mathbf{P}(\mathcal{C}_{F_i}) \supset \{p : \text{prime} \mid p \equiv a \mod b\}.$$

Then there exist only finitely many l such that H_l is represented as $F(x, y)$.

Taking $y = 1$ in Corollary 3.4, we get the result of Berend and Harmse for reducible polynomials partially. To explain their result, we introduce the natural density $d(S)$ for a subset S of the set of all primes defined by

$$d(S) = \lim_{x \to \infty} \frac{\pi(x, S)}{\pi(x)},$$

where $\pi(x)$ is the number of primes $p \leq x$ and $\pi(x, S)$ is the number of those belonging to S.

Theorem 3.5 (Theorem 4.1. of [BH06])**.** Consider the equation

$$P(x) = H_l. \tag{3.6}$$

Let $Q(x) \in \mathbf{Z}[x]$ be any factor (irreducible or not) of P. Denote by $S(Q) \subset P$ the set of all primes p for which the congruence $Q(x) \equiv 0 \mod p$ has a solution. If $d(S(Q)) < \frac{\deg Q}{\deg P}$, then (3.6) has only finitely many solutions.

The assumption $\bigcap_i \mathbf{P}(\mathcal{C}_{F_i}) \supset \{p : \text{prime} \mid p \equiv a \mod b\}$ in Corollary 3.4 leads to $d(S(F(x, 1))) < 1$. Thus, Theorem 3.5 implies Corollary 3.4 with $y = 1$.

For special quadratic forms, we give a sufficient condition for the existence of infinitely many solutions. We denote the set of primes which is inert in $\mathbf{Q}(\sqrt{\Delta})$ by P_Δ.

Theorem 3.7. Let K be a number field with $n = [K : \mathbf{Q}]$ and D_K its discriminant. Let $F(x, y) = ax^2 + bxy + cy^2$ be a positive definite quadratic form with fundamental modified discriminant $\Delta_{F,mod}$, where one of a and c is a prime number or 1. We denote $P_{\Delta_F, D_K} = P_{\Delta_F} \setminus$

$\{p|D_K\}$. We assume that the class number of $\mathbf{Q}(\sqrt{\Delta_F})$ equals 1. If for all $p \in P_{\Delta_F,D_K}$ and for odd i, $G_p(i;K)$ is even, then there exist infinitely many l such that $\Pi_K(l)$ is represented as $F(x,y)$.

Proof. We assume for all $p \in P_{\Delta_F,D_K}$ and odd i, $G_p(i;K)$ is even. It suffices to show that the prime factorization of $\Pi_K(l)$ contains no prime $p \in P_{\Delta_F,D_K}$ raised to an odd power for infinitely many l. Let $a(n)$ be the number of ideals of $\mathcal{O}_K$ with $\mathfrak{N}\mathfrak{a} = n$ It follows from the Chinese Remainder Theorem that the function $a(n)$ satisfies the multiplicative property

$$a(mn) = a(m)a(n) \qquad \text{if } \gcd(m,n) = 1.$$

From this multiplicative property of $a(n)$, it suffices to show $a(p^m)$ is even for all primes $p \in P_{\Delta_F,D_K}$ and odd m. The ideals $\mathfrak{a}$ such that $\mathfrak{N}\mathfrak{a} = p^m$ is expressed by product of prime ideals $\mathfrak{p}$ with $\mathfrak{N}\mathfrak{p} = p^k (k \leq m)$. If $\mathfrak{a}$ is expressed as $\mathfrak{p}_1 \cdots \mathfrak{p}_s$ and the number of $\mathfrak{p}_t$ with $\mathfrak{N}\mathfrak{p}_t = p^i$ equals a_i, then we have $a_1 + \cdots + ma_m = m$. By considering the number of combinations with reputation, we get

$$a(p^m) = \sum_{\substack{a_1+\cdots+ma_m=m \\ a_i \geq 0}} \prod_{i=1}^{m} \binom{G_p(i;K) + a_i - 1}{a_i}.$$

Now we assume $G_p(i;K)$ is even for all odd i. Since m is odd, there exists an odd i such that a_i is odd in each product. For this odd i

$$\binom{G_p(i;K) + a_i - 1}{a_i}$$

is even, since binomial coefficients $\binom{e}{o}$, where e is an even number and o is an odd number, are always even. Accordingly, $a(p^m)$ is a sum of even numbers, $a(p^m)$ is also even for all odd m.

If $G_p(i;K)$ is odd for some $p \in P_{\Delta_F} \setminus P_{\Delta_F,D_K}$ and some odd i, we denote $m = \min\{i : \text{odd} \mid G_p(i,K) \text{ is odd}\}$. As we mentioned above, $a(p^m)$ is odd. Chebotarev's density theorem says that for any number fields K there exist infinitely many primes splitting completely in K. Let q be a prime splitting completely in K. Then we have $a(q^k) = \binom{n+k-1}{n-1}$. One can see easily that $\binom{n+k-1}{n-1}$ takes odd values infinitely many times and $a(p^m q^k)$ does. Since $P_{\Delta_F} \setminus P_{\Delta_F,D_K}$ is a finite set, $\Pi_K(l)$ satisfies the first condition in Theorem 2.4 infinitely many times. By assumption, the second condition in Theorem 2.4 is trivial. This shows the theorem. □

4. Generalizations

In the previous sections, we deal with two variables homogeneous polynomial. Naturally, we have an interest in the Brocard-Ramanujan problem for multi-variable homogeneous polynomial. In this section, we consider many more variables polynomials.

Since all positive integers n are expressed as the sum of four squares of integers, there are infinitely many l such that $l!$ is represented as $x^2+y^2+z^2+w^2$. Therefore, irreducibility of polynomials $f(x_1,\dots,x_n)$ is not important for the finiteness of the solutions of $f(x_1,\dots,x_n)=l!$.

In this report, we consider the equation $N_A(x)=H_l$, where N_A is a norm form constructed from the field norm of a field extension $K/\mathbf{Q}$. Let $\mathcal{O}$ be an order of number field K and $\{\alpha_1,\dots,\alpha_n\}$ be their basis over $\mathbf{Z}$. Then the norm form $N_{\alpha_1,\dots,\alpha_n}$ is defined by

$$N_{\alpha_1,\dots,\alpha_n}(x_1,\dots,x_n)=\prod_{\sigma\in\mathrm{Aut}(K/\mathbf{Q})}\sigma\left(\sum_{i=1}^{n}\alpha_i x_i\right).$$

There exists the matrix A converting from the basis $\{\alpha_1,\dots,\alpha_n\}$ to the basis $\{1,\alpha_2',\dots,\alpha_n'\}$ of $\mathcal{O}$. Also, since $A\in\mathrm{SL}_n(\mathbf{Z})$, an integer N is represented as $N_{\alpha_1,\dots,\alpha_n}$ if and only if N is also represented as $N_{1,\alpha_2',\dots,\alpha_n'}$. Therefore, it suffices to consider the case $\alpha_1=1$.

Since all norm form is irreducible, we have considered the norm form of quadratic fields in previous sections. As one of corollary of Theorem 3.1 we have

Corollary 4.1. For any norm form N_{α_1,α_2} of quadratic fields, there exists only finitely many l such that H_l is represented as $N_{\alpha_1,\alpha_2}(x_1,x_2)$.

We generalize this corollary to all norm forms by following the proof of Theorem 3.1 as follows.

Theorem 4.2. For any order $\mathcal{O}\neq\mathbf{Z}$ of a number field and their basis $\{\alpha_1,\dots,\alpha_n\}$ over $\mathbf{Z}$, there exists only finitely many l such that H_l is represented as $N_{\alpha_1,\dots,\alpha_n}(x_1,\dots,x_n)$.

More generally, we deal with the equation $N_{\alpha_1,\dots,\alpha_n}(x_1,\dots,x_n)=l!_S$, where $l!_S$ is the Bhargava factorial for $S\subset\mathbf{Z}$. Bhargava introduced a generalization of the factorial function to generalize classical results in $\mathbf{Z}$ to Dedekind domains and unify them [Bh97, Bh00]. Since the ordinary factorial $l!$ is one of the examples of the Bhargava factorial, we regard this equation as one of the generalizations of the Brocard-Ramanujan problem. The Bhargava factorial is defined as follows.

Let S be an infinite subset of $\mathbf{Z}$. First, we define p-ordering of S. A p-ordering of S is any sequence $\{a_n\}$ of elements of S that is formed as follows:

- Choose any element $a_0 \in S$;
- For $k \geq 1$ choose an element $a_n \in S$ such that
$$v_p\left(\prod_{k=0}^{n-1}(a_n - a_k)\right) = \inf_{x \in S} v_p\left(\prod_{k=0}^{n-1}(x - a_k)\right),$$
where v_p is the p-adic valuation defined by $v_p(p^v a) = v$ with an integer a relatively prime to p.

For a p-ordering of S, we construct the p-sequence $\{v_p(n; S)\}$ as
$$v_p(n; S) = v_p\left(\prod_{k=0}^{n-1}(a_n - a_k)\right).$$
It is known that the associated p-sequence of S is independent of the choice of p-ordering of S [Bh00].

With these settings, we define the Bhargava factorial $l!_S$ by
$$l!_S = \prod_{p:\text{prime}} p^{v_S(l;p)}.$$
We give some examples of the Bhargava factorial. When $S = \mathbf{Z}$, we can choose the natural ordering $0, 1, 2, 3, \ldots$ as a p-ordering of $l!_S$ for all primes p and find $l!_{\mathbf{Z}}$ is the ordinary factorial $l!$. This is why we can regard the equation $P(x) = l!_S$ as one of the generalizations of the Brocard-Ramanujan problem $x^2 - 1 = l!$. Also, when $S(a, b) = \{an + b \mid n \in \mathbf{Z}\}$ for some $a, b \in \mathbf{Z}$ then $l!_{S(a,b)} = a^l l!$. Since we can apply the same way as the proof of Theorem 3.1 for the equation $P(x) = l!_{S(a,b)}$, we obtain the finiteness of solutions (x, l) for the equation $P(x) = l!_{S(a,b)}$.

We point out that we can generalize Luca's result to the Bhargava factorial by following his proof. Luca showed that the Oesterlé-Masser conjecture implies that the equation $P(x) = l!$ has only finitely many solutions (x, l) [Lu02]. In the proof of this result, Luca used the facts that $\mathrm{rad}(l!) < 4^l$ and the Stirling formula $\log l! \sim l \log l$ as $l \to \infty$ to estimate $\mathrm{rad}(l!)$ and $l!$. Hence, if we estimate $l!_S$ and $\mathrm{rad}(l!_S)$, we can judge whether or not we can apply the same argument with the proof of Luca's result. Since $l!|l!_S$, for all primes p, the p-adic valuation $v_p(l!_S)$ tends to infinity as $l \to \infty$. Therefore, we find that $\mathrm{rad}(l!_S) = o(l!_S)$ as $l \to \infty$ and obtain the following theorem.

Theorem 4.3 (cf. [Lu02])**.** Let $P(x) \in \mathbf{Z}[x]$ be a polynomial of $\deg P \geq 2$ and S be an infinite subset of $\mathbf{Z}$. Then the Oesterlé-Masser conjecture implies that the equation $P(x) = l!_S$ has only finitely many solutions (x, l).

For some special case, we can show the finiteness of solutions for the equation $P(x) = l!_S$ unconditionally. Let $f(x) = ax^2+bx+c \in \mathbf{Z}[x]$ be a polynomial. Then we consider the Bhargava factorial for $S = f(\mathbf{Z})$. Since we consider the case $a = 0$ above, it suffices to consider the case $a \neq 0$. Let p be an odd prime not dividing a. Then we have

$$\#\{f(n) \mid n \in \mathbf{Z}\} = \frac{p+1}{2}$$

and we can choose an ordering $f(n_0), \ldots, f(n_{p-1}), \ldots$ satisfying the following three conditions:

(1) $\{n_0, \ldots, n_{p-1}\} = [0, p-1] \cap \mathbf{Z}$;
(2) $f'(n_0) \equiv 0 \mod p$;
(3) For $0 \leq i < j \leq \frac{p-1}{2}$, $f(n_i) \not\equiv f(n_j) \mod p$.

This ordering forms a p-ordering of S and we can estimate $v_p(l!_S)$ as

$$v_p(l!_S) = \begin{cases} 0 & \text{if } 0 \leq l \leq \frac{p-1}{2}, \\ 1 & \text{if } \frac{p+1}{2} \leq l \leq p-1, \\ 2 & \text{if } l = p. \end{cases} \tag{4.4}$$

Therefore, the same way with the proof of Theorem 3.1 also works for the equation $P(x) = l!_S$.

Theorem 4.5. Let $N_{\alpha_1,\ldots,\alpha_n}(x_1, \ldots, x_n)$ be a norm form of number field $K \neq \mathbf{Q}$. For a polynomial $f(x) = ax^2 + bx + c$ with $(a, b, c) \in \mathbf{Z}^3 - \{(0, 0, c) \mid c \in \mathbf{Z}\}$ we denote $S = f(\mathbf{Z})$. Then there exist only finitely many l such that $l!_S$ is represented as $N_{\alpha_1,\ldots,\alpha_n}(x_1, \ldots, x_n)$.

The case $\deg f \geq 3$, it depends on the base field K. For example, when $f(x) = x^3$ then we find

$$\#\{n^3 \mod p \mid n \in \mathbf{Z}\} = \begin{cases} \frac{p+2}{3} & \text{if } p \equiv 1 \mod 3, \\ p & \text{otherwise.} \end{cases} \tag{4.6}$$

If $K/\mathbf{Q}$ is an abel extension, then the exists a positive integer D which characterizes the set of primes corresponding to a conjugacy class $C \subset \mathrm{Gal}(K/\mathbf{Q})$. Therefore, for any norm form N_A of K and we can show the finiteness of solutions for $N_A(x) = l!_S$. On the other hand, if $K/\mathbf{Q}$ is not an abel extension, then we cannot characterize the set of primes corresponding to a conjugacy class $C \subset \mathrm{Gal}(K/\mathbf{Q})$ by any modulus and it is difficult to show the finiteness of solutions in general.

ACKNOWLEDGEMENT

I would like to express my gratitude to Professor Masatoshi Suzuki and Professor Takashi Nakamura for this opportunity to give a talk in RIMS Workshop 2019 "Analytic Number Theory and Related Topics". This work was supported by Grant-in-Aid for JSPS Research Fellow (Grant Number: 19J10705).

References

[BH06] D. Berend and J. E. Harmse. On polynomial–factorial Diophantine equations. *Trans. Amer. Math. Soc.* **358**(4), 1741–1779. 2006.

[BO92] D. Berend and C. F. Osgood. On the equation $P(x) = n!$ and a question of Erdős. *Journal of Number Theory.* **42**, 189–193. 1992.

[Bh97] M. Bhargava. P-orderings and polynomial functions on arbitrary subsets of Dedekind rings. *J. Reine Angew. Math.* **490**, 101–127. 1997.

[Bh00] M. Bhargava. The factorial function and generalizations. *Amer. Math. Monthly*, **107**, no. **9**, 783–799. 2000.

[Br76] H. Brocard. Question 166, *Nouv. Corres. Math.* **2**, 287. 1876.

[Br85] H. Brocard, Question 1532, *Nouv. Ann. Math.* (3)**4**, 391. 1885.

[EO37] P. Erdős. and R. Obláth. Über diophantische Gleichungen der Form $n! = x^p \pm y^p$ und $n! \pm m! = x^p$. *Acta Szeged*, **8**, 241–255. 1937

[HM17] T. A. Hulse and M. Ram Murty. Bertrand's postulate for number fields. *Colloquium Mathematicum*, **147**, 165–180. 2017.

[Lu02] F. Luca, The Diophantine equation $P(x) = n!$ and a result of M. Overholt, *Glasnik Matematički Ser. III* **37**(57). 269–273. 2002.

[PS73] R. M. Pollack and H. N. Shapiro. The next to last case of a factorial diophantine equation. *Communications on pure and applied mathematics*, **26**(3), 313–325. 1973.

[Ra13] S. Ramanujan. Question 469. *Journal of the Indian Mathematical Society.* **5**, 59. 1913.

[Ta19] Wataru Takeda. Finiteness of trivial solutions of factorial products yielding a factorial over number fields. *Acta arithmetica*, **190**(4), 395–401. 2019.

Department of Mathematics, Nagoya University, Chikusa-ku, Nagoya 464-8602, Japan.

Email address: d18002r@math.nagoya-u.ac.jp