Journal de Théorie des Nombres
de Bordeaux **15** (2003), 141–149

Representation of prime powers in arithmetical progressions by binary quadratic forms

par Franz HALTER-KOCH

Résumé. Soit Γ une famille de formes quadratiques à deux variables de même discriminant, Δ un ensemble de progressions arithmétiques et m un entier strictement positif. Nous nous intéressons au problème de la représentation des puissances de nombres premiers p^m appartenant à une progression de Δ par une forme quadratique de Γ.

Abstract. Let Γ be a set of binary quadratic forms of the same discriminant, Δ a set of arithmetical progressions and m a positive integer. We investigate the representability of prime powers p^m lying in some progression from Δ by some form from Γ.

1. Introduction and notations

By a *form* φ we always mean a primitive integral non-degenerated binary quadratic form, that is, $\varphi = aX^2 + bXY + cY^2 \in \mathbb{Z}[X,Y]$, where $\gcd(a,b,c) = 1$, $d = b^2 - 4ac$ is not a square, and $a > 0$ if $d < 0$. We call d the *discriminant* of φ. More generally, any non-square integer $d \in \mathbb{Z}$ with $d \equiv 0 \mod 4$ or $d \equiv 1 \mod 4$ will be called a *discriminant.* Two forms $\varphi, \psi \in \mathbb{Z}[X,Y]$ are called (properly) *equivalent* if $\varphi(X,Y) = \psi(\alpha X + \beta Y, \gamma X + \delta Y)$ for some $\alpha, \beta, \gamma, \delta \in \mathbb{Z}$ such that $\alpha\delta - \beta\gamma = 1$. For any discriminant d, we denote by $\mathcal{H}(d)$ the (finite) set of equivalence classes of forms with discriminant d. If $\varphi = aX^2 + bXY + cY^2$ is a form with discriminant d, we denote by $[\varphi] = [a,b,c] \in \mathcal{H}(d)$ the equivalence class of φ. For any discriminant d, we call

$$I = I_d = \begin{cases} [1, 0, -d/4]\,, & \text{if } d \equiv 0 \mod 4, \\ [1, 1, (1-d)/4]\,, & \text{if } d \equiv 0 \mod 4 \end{cases}$$

the *principal class* of $\mathcal{H}(d)$.

A form $\varphi \in \mathbb{Z}[X,Y]$ is said to *represent* (properly) an integer $q \in \mathbb{Z}$, if $q = \varphi(x,y)$ for some $x, y \in \mathbb{Z}$ such that $\gcd(x,y) = 1$. Equivalent forms

Manuscrit reçu le 11 octobre 2001.

represent the same integers, and we write $C \to q$ if $C = [\varphi]$ for some form φ representing q.

This paper is addressed to the representation of prime powers in arithmetical progressions. To be precise, we shall derive criteria for a form φ (or its class $[\varphi]$) to represent all prime powers (of fixed exponent) $p^m \in b + a\mathbb{Z}$ for given coprime positive integers a and b. If $m = 1$ and if genera are considered instead of individual forms or classes, the problem is solved by Gauss' genus theory. A first result for individual classes was proved by A. Meyer [9] using Dirichlet's theorem. A complete solution for $m = 1$ and fundamental discriminants was presented by T. Kusaba [8] (using class field theory). The case of arbitrary discriminants (for $m = 1$ and $p \neq 2$) was settled by P. Kaplan and K. S. Williams [7] (using elementary methods and Meyer's theorem).

In fact, in this paper we shall consider more generally a set $\Gamma \subset \mathcal{H}(d)$ (for some discriminant $d \in \mathbb{Z}$) and a set $\Delta \subset (\mathbb{Z}/a\mathbb{Z})^\times$ of arithmetical progressions (for some distance $a \geq 2$), and we shall deal with the problem whether every prime power p^m (with fixed exponent m) satisfying $p^m + a\mathbb{Z} \in \Delta$ is represented by some class $C \in \Gamma$. We shall throughout make use of class field theory, and in order to do so, we will also formulate Gauss' genus theory in a class field theoretic setting.

In section 2, we gather the necessary facts from genus theory and class field theory in a form which is suitable for our purposes. In section 3, we formulate and prove the main results of this paper.

2. Class field theory and genus theory

The main references for this section are [2] and [1], but see also [3] and [4]. For a discriminant d, we set

$$R_d = \begin{cases} \mathbb{Z}[(1+\sqrt{d})/2], & \text{if } d \equiv 1 \mod 4, \\ \mathbb{Z}[\sqrt{d}/2], & \text{if } d \equiv 0 \mod 4. \end{cases}$$

Let $\mathcal{C}^+(R_d)$ be the Picard group of R_d in the narrow sense (that is, the group of invertible fractional ideals modulo fractional principal ideals generated by totally positive elements). If $\varphi = aX^2 + bXY + cY^2 \in \mathbb{Z}[X, Y]$ is a form with discriminant d and $a > 0$, then

$$\mathfrak{c}_\varphi = (a, \frac{b + \sqrt{d}}{2}) \triangleleft R_d$$

is a primitive invertible ideal with norm $\mathcal{N}(\mathfrak{c}_\varphi) = (R_d : \mathfrak{c}_\varphi) = a$. Every class $C \in \mathcal{H}(d)$ contains a form $\varphi = aX^2 + bXY + cY^2$ with $a > 0$, and the assignment $\varphi \mapsto \mathfrak{c}_\varphi$ induces a bijective map

$$\theta_d : \mathcal{H}(d) \to \mathcal{C}^+(R_d)\,.$$

For an invertible ideal $\mathfrak{a}$ of R_d we denote by $[\mathfrak{a}] \in \mathcal{C}^+(R_d)$ its class (in the narrow sense). Gauss' composition is the group structure on $\mathcal{H}(d)$ for which θ_d is an isomorphism, and $I_d = \theta_d^{-1}(R_d)$ is the unit element of $\mathcal{H}(d)$.

For a class $C \in \mathcal{H}(d)$ and $q \in \mathbb{N}$, we have $C \to q$ if and only if $q = \mathcal{N}(\mathfrak{a})$ for some primitive ideal $\mathfrak{a} \in \theta_d(C)$. For a form $\varphi = aX^2 + bXY + cY^2 \in \mathbb{Z}[X, Y]$, we denote by $\bar{\varphi} = aX^2 - bXY + cY^2$ its conjugate (or opposite) form, and for a quadratic surd $\alpha = u + v\sqrt{d} \in \mathbb{Q}(\sqrt{d})$, we denote by $\bar{\alpha} = u - v\sqrt{d}$ its (algebraic) conjugate. Conjugation induces inversion, both on $\mathcal{H}(d)$ and $\mathcal{C}^+(R_d)$ (that means, $[\bar{\varphi}] = [\varphi]^{-1}$ for every form φ, and $[\bar{\mathfrak{a}}] = [\mathfrak{a}]^{-1}$ for every invertible ideal $\mathfrak{a}$).

For every class $C \in \mathcal{H}(d)$, C and C^{-1} represent the same integers. A prime power p^m with $p \nmid d$ is represented by some class $C \in \mathcal{H}(d)$ if and only if $\left(\frac{d}{p}\right) = 1$. In this case, $pR_d = \mathfrak{p}\bar{\mathfrak{p}}$ for some prime ideal $\mathfrak{p}$ of R_d such that $\mathfrak{p} \neq \bar{\mathfrak{p}}$, and if $C = \theta_d^{-1}([\mathfrak{p}^m])$, then C and C^{-1} are precisely the classes from $\mathcal{H}(d)$ representing p^m.

Associated with a discriminant d, there is an abelian field extension $K_d/\mathbb{Q}(\sqrt{d})$, together with an isomorphism

$$\alpha_d : \mathcal{H}(d) \xrightarrow{\sim} \mathrm{Gal}\big(K_d/\mathbb{Q}(\sqrt{d})\big) ,$$

having the following properties:

1. $K_d/\mathbb{Q}$ is a Galois extension which is unramified at all primes $p \nmid d\infty$ and whose Galois group is given by the splitting group extension

$$1 \longrightarrow \mathcal{H}(d) \xrightarrow{\alpha_d} \mathrm{Gal}(K_d/\mathbb{Q}) \xrightarrow{\rho_d} \langle\tau\rangle \longrightarrow 1 ,$$

where $\langle\tau\rangle = \mathrm{Gal}\big(\mathbb{Q}(\sqrt{d})/\mathbb{Q}\big)$, $\rho_d(\sigma) = \sigma \mid \mathbb{Q}(\sqrt{d})$, and τ acts on $\mathcal{H}(d)$ by $C^\tau = C^{-1}$.

2. For a class $C \in \mathcal{H}(d)$ and a prime p with $p \nmid d$, we have $C \to p$ if and only if $\alpha_d(C)$ is the Frobenius automorphism of some prime divisor of p in K_d.

Let K_d^* be the maximal absolutely abelian subfield of K_d. Then $\mathrm{Gal}(K_d/K_d^*) = \alpha_d\big(\mathcal{H}(d)^2\big)$, and there is an isomorphism

$$\alpha_d^* : \begin{cases} \mathcal{H}(d)/\mathcal{H}(d)^2 & \xrightarrow{\sim} \ \mathrm{Gal}\big(K_d^*/\mathbb{Q}(\sqrt{d})\big) \\ \quad C\mathcal{H}(d)^2 & \longmapsto \ \alpha_d(C) \mid K_d^*. \end{cases}$$

The field K_d is called the *ring class field*, the field K_d^* is called the *genus field*, the cosets $C\mathcal{H}(d)^2 \subset \mathcal{H}(d)$ are called the *genera* and $\mathcal{H}(d)^2$ is called the *principal genus* of discriminant d.

An explicit generation of K_d^* was given in [5] as follows: Let $p_1, \dots, p_t$ be the distinct odd prime divisors of d, set

$$p_i^* = \Big(\frac{-1}{p_i}\Big) p_i \quad \text{for} \quad i \in \{1, \dots, t\} \qquad \text{and} \qquad K_d' = \mathbb{Q}(\sqrt{p_1^*}, \dots, \sqrt{p_t^*})\,.$$

Then we obtain

$$K_d^* = \begin{cases} K_d', & \text{if} \quad d \equiv 1 \mod 4 \quad \text{or} \quad d \equiv 4 \mod 16\,, \\ K_d'(\sqrt{-1}), & \text{if} \quad d \equiv 12 \mod 16 \quad \text{or} \quad d \equiv 16 \mod 32\,, \\ K_d'(\sqrt{\pm 2}), & \text{if} d \equiv \pm 8 \mod 32\,, \\ K_d'(\sqrt{-1}, \sqrt{2}), & \text{if } d \equiv 0 \mod 32\,. \end{cases}$$

we define the *reduced discriminant* d^* associated with d by

$$d^* = \begin{cases} p_1 \cdot \ldots \cdot p_t\,, & \text{if} \quad d \equiv 1 \mod 4\,, \\ 2p_1 \cdot \ldots \cdot p_t\,, & \text{if} \quad d \equiv 4 \mod 16\,, \\ 4p_1 \cdot \ldots \cdot p_t\,, & \text{if} \quad d \equiv 12 \mod 16 \quad \text{or} \quad d \equiv 16 \mod 32\,, \\ 8p_1 \cdot \ldots \cdot p_t\,, & \text{if} \quad d \equiv 0,\ 8 \text{ or } 24 \mod 32\,. \end{cases}$$

For $a \in \mathbb{N}$, we denote by $\mathbb{Q}^{(a)}$ the field of a-th roots of unity and by

$$\beta_a : (\mathbb{Z}/a\mathbb{Z})^\times \ \xrightarrow{\sim}\ \mathrm{Gal}(\mathbb{Q}^{(a)}/\mathbb{Q})$$

the Artin isomorphism for $\mathbb{Q}^{(a)}/\mathbb{Q}$, that is, for a prime $p \nmid a$, $\beta_a(p + a\mathbb{Z})$ is the Frobenius automorphism of the prime divisors of p in $\mathbb{Q}^{(a)}$.

If d is a discriminant, then $d^* \mid d$, hence $\mathbb{Q}^{(d^*)} \subset \mathbb{Q}^{(d)}$, and d^* is the smallest positive integer divisible by all prime divisors of d and satisfying $K_d^* \subset Q^{(d^*)}$. If $m \in \mathbb{Z}$ and $\gcd(m, d) = 1$, we consider the Kronecker symbol, defined by

$$\Big(\frac{d}{m}\Big) = \mathrm{sign}(d)^\varepsilon\, (-1)^{\frac{d-1}{4}\beta} \Big(\frac{d}{m_1}\Big)\,,$$

if $m = (-1)^\varepsilon 2^\beta m_1$, where $\varepsilon \in \{0, 1\}$, $\beta \in \mathbb{N}_0$, m_1 is odd and $\big(\frac{d}{m_1}\big)$ is the Jacobi symbol (for details see [6], Ch. 5.5). The Kronecker symbol $\big(\frac{d}{m}\big)$ depends only on the residue class $m + d^*\mathbb{Z} \in (\mathbb{Z}/d^*\mathbb{Z})^\times$, and

$$\chi_d = \Big(\frac{d}{\cdot}\Big) : (\mathbb{Z}/d^*\mathbb{Z})^\times \ \to\ \{\pm 1\}$$

is a quadratic character with the following property:

If $C \in \mathcal{H}(d)$, $k \in \mathbb{Z}$, $\gcd(k, d) = 1$ and $C \to k$, then $\big(\frac{d}{k}\big) = 1$. Indeed, observe that $C \to k$ implies $C = [k, b, c]$ for some $b, c \in \mathbb{Z}$, and since $d = b^2 - 4kc$, it follows that $\big(\frac{d}{k}\big) = \big(\frac{d}{|k|}\big) = 1$.

We define

$$\varphi_1, \dots, \varphi_g : (\mathbb{Z}/d^*\mathbb{Z})^\times \ \to\ \{\pm 1\} \qquad \text{by} \qquad \varphi_i(m + d^*\mathbb{Z}) = \Big(\frac{m}{p_i}\Big)\,.$$

If $d^* \equiv 0 \mod 4$, we define

$$\varepsilon : (\mathbb{Z}/d^*\mathbb{Z})^\times \to \{\pm 1\} \qquad \text{by} \qquad \varepsilon(m + d^*\mathbb{Z}) = \Big(\frac{-1}{m}\Big),$$

and if $d^* \equiv 0 \mod 8$, we define

$$\delta : (\mathbb{Z}/d^*\mathbb{Z})^\times \to \{\pm 1\} \qquad \text{by} \qquad \delta(m + d^*\mathbb{Z}) = \Big(\frac{2}{m}\Big).$$

Then the vector of genus characters

$$\boldsymbol{\varphi}_d : (\mathbb{Z}/d^*\mathbb{Z}) \to \{\pm 1\}^{\mu(d)}$$

is defined by its components as follows.

$$\boldsymbol{\varphi}_d = \begin{cases} (\varphi_1, \dots, \varphi_t), & \text{if} \quad d \equiv 1 \mod 4 \quad \text{or} \quad d \equiv 4 \mod 16, \\ (\varphi_1, \dots, \varphi_t, \varepsilon), & \text{if} \quad d \equiv 12 \mod 16 \quad \text{or} \quad d \equiv 16 \mod 32, \\ (\varphi_1, \dots, \varphi_t, \delta), & \text{if} \quad d \equiv 8 \mod 32, \\ (\varphi_1, \dots, \varphi_t, \varepsilon\delta), & \text{if} \quad d \equiv 24 \mod 32, \\ (\varphi_1, \dots, \varphi_t, \varepsilon, \delta), & \text{if} \quad d \equiv 0 \mod 32. \end{cases}$$

By its very definition, for a prime $p \nmid d$ the Frobenius automorphism $\beta_{d^*}(p + d^*\mathbb{Z}) \mid K_d^*$ is uniquely determined by its genus character values $\boldsymbol{\varphi}_d(p + d^*\mathbb{Z}) \in \{\pm 1\}^{\mu(d)}$. We have

$$(\mathbb{Z}/d^*\mathbb{Z})^{\times 2} \subset \operatorname{Ker}(\boldsymbol{\varphi}_d) \subset \operatorname{Ker}(\chi_d) \subset (\mathbb{Z}/d^*\mathbb{Z})^\times,$$

and

$$\big(\operatorname{Ker}(\boldsymbol{\varphi}_d) : (\mathbb{Z}/d^*\mathbb{Z})^{\times 2}\big) = \begin{cases} 2, & \text{if} \quad d \equiv \pm 8 \mod 32, \\ 1 & \text{otherwise.} \end{cases}$$

From the class field theoretic description of K_d, K_d^* and $\mathbb{Q}^{(d^*)}$ we derive immediately the following two assertions **3.** and **4.** which are usually quoted as the main theorems of Gauss' genus theory.

3. The group

$$X_d = \operatorname{Ker}(\chi_d) = \beta_{d^*}^{-1}\Big[\operatorname{Gal}\big(\mathbb{Q}^{(d^*)}/\mathbb{Q}(\sqrt{d})\big)\Big] \subset (\mathbb{Z}/d^*\mathbb{Z})^\times$$

consists of all residue classes $p + d^*\mathbb{Z} \in (\mathbb{Z}/d^*\mathbb{Z})^\times$ generated by primes p such that $p \nmid d$ and $C \to p$ for some $C \in \mathcal{H}(d)$.

4. The map $\omega_d : (\mathbb{Z}/d^*\mathbb{Z})^\times \to \mathcal{H}(d)/\mathcal{H}(d)^2$, defined by

$$\omega_d(x) = \alpha_d^{*-1}\Big[\beta_{d^*}(x) \mid K_d^*\Big]$$

is a group epimorphism, and $\operatorname{Ker}(\omega_d) = \operatorname{Ker}(\boldsymbol{\varphi}_d)$. In particular,

$$\big(\mathcal{H}(d) : \mathcal{H}(d)^2\big) = [K_d^* : \mathbb{Q}(\sqrt{d})] = 2^{\mu(d)-1}.$$

If p is a prime, $p \nmid d$ and $C \in \mathcal{H}(d)$ with $C \to p$, then $\omega_d(p+d^*\mathbb{Z}) = C\mathcal{H}(d)^2$. Consequently, the genus representing p depends only on the residue class $p + d^*\mathbb{Z}$.

Meyer [9] proved that if a class $C \in \mathcal{H}(d)$ represents some prime $p \nmid d$ in a coprime arithmetical progression, then it represents infinitely many primes from this progression. We shall need the following refinement of this result.

Proposition 1. *Let d be a discriminant, $a, b \in \mathbb{N}$ and $\gcd(a, b) = 1$. Let $C_0 \in \mathcal{H}(d)$ be a class representing some prime $p_0 \in b + a\mathbb{Z}$ with $p_0 \nmid d$.*

1. *The set of all primes $p \in b+a\mathbb{Z}$ represented by C_0 has positive Dirichlet density.*
2. *Let $\Omega \subset \mathcal{H}(d)$ be the set of all classes representing primes $p \in b + a\mathbb{Z}$ with $p \nmid d$. Then $\Omega\mathcal{H}(d)^2 = \Omega$ (that means, Ω consists of full genera).*

Proof. We may assume that $d^* \mid a$, $\gcd(d, b) = 1$ and $\left(\frac{d}{b}\right) = 1$ (otherwise we replace a by ad^* and consider all residue classes $b' + ad^*\mathbb{Z}$, where $\left(\frac{d}{b'}\right) = 1$ and $b' \equiv b \mod a$). Since $C_0 \to p_0$, we have

$$\beta^{(a)}(b + a\mathbb{Z}) \mid K_d^* = \alpha_d(C_0) \mid K_d^* .$$

For a prime $p \in b+a\mathbb{Z}$, we have $C_0 \to p$ if and only if $\left(\alpha_d(C_0)|K_d^*\right)^{\pm 1}$ is the Frobenius automorphism for a prime divisor of p in K_d^*. By Čebotarev's theorem, this set has positive Dirichlet density.

A class $C \in \mathcal{H}(d)$ represents some prime $p \in b + a\mathbb{Z}$ if and only if $\alpha_d(C)|K_d^* = \alpha_d(C_0)|K_d^*$, and since $\mathrm{Gal}(K_d/K_d^*) = \alpha_d(\mathcal{H}(d)^2)$, this is equivalent to $C \in C_0\mathcal{H}(d)^2$. Hence we obtain $\Omega = C_0\mathcal{H}(d)^2 = \Omega\mathcal{H}(d)^2$. $\square$

3. The main results

For a discriminant d, we denote by $\mathcal{H}_2(d)$ the 2-Sylow subgroup and by $\mathcal{H}'(d)$ the odd part of $\mathcal{H}(d)$, so that $\mathcal{H}(d) = \mathcal{H}_2(d) \times \mathcal{H}'(d)$.

Theorem 1. *Let d be a discriminant, m an odd positive integer and $\Omega \subset \mathcal{H}(d)^m$ a set of classes satisfying $\Omega\mathcal{H}(d)^{2m} = \Omega$. Then there is a subset $\Delta \subset X_d$ such that, for every prime $p \nmid d$, if $p^m + d^*\mathbb{Z} \in \Delta$ then $C \to p^m$ for some $C \in \Omega$.*

Proof. Suppose $\Omega = \Omega_0^m$, where $\Omega_0 \subset \mathcal{H}(d)$, and set $\Delta = \omega_d^{-1}\left(\Omega_0\mathcal{H}(d)^2\right) \subset X_d$. Let p be a prime such that $p \nmid d$ and $p^m + d^*\mathbb{Z} \in \Delta$. Since m is odd, we obtain $p + d^*\mathbb{Z} \in X_d$ and $\omega_d(p + d^*\mathbb{Z}) = \omega_d(p^m + d^*\mathbb{Z}) = C_0\mathcal{H}(d)^2$ for some class $C_0 \in \Omega_0$. Hence there exists some $A \in \mathcal{H}(d)$ such that $C_0A^2 \to p$, and if $C = (C_0A^2)^m$, then $C \to p^m$ and $C \in \Omega_0^m\mathcal{H}(d)^{2m} = \Omega$. $\square$

The assumption $\Omega\mathcal{H}(d)^{2m} = \Omega$ made in Theorem 1 is very restrictive. But as we shall see in Theorem 2, it is necessary. We investigate its effect in the special case $\Omega = \{C, C^{-1}\}$ for some $C \in \mathcal{H}(d)$. Note that the following (simple) Proposition 2 remains true if we replace $\mathcal{H}(d)$ by any finite abelian group.

Proposition 2. *Let d be a discriminant, m an odd positive integer and $C \in \mathcal{H}(d)$ a class satisfying $\{C, C^{-1}\}\mathcal{H}(d)^{2m} = \{C, C^{-1}\}$. Then we have $\mathcal{H}'(d)^m = \{1\}$, and either $\mathcal{H}_2(d)^2 = \{1\}$ or $C^4 = I$ and $\mathcal{H}_2(d) = \langle C \rangle \times \mathcal{H}_2^*(d)$, where $\mathcal{H}_2^*(d)^2 = \{1\}$.*

Proof. By assumption,

$$|\mathcal{H}(d)^{2m}| \leq |\{C, C^{-1}\}\mathcal{H}(d)^{2m}| \leq 2\,,$$

and since $\mathcal{H}(d)^{2m} = \mathcal{H}_2(d)^2 \times \mathcal{H}'(d)^m$, we obtain $\mathcal{H}'(d)^m = \{1\}$ and $|\mathcal{H}_2(d)^2| \leq 2$. Suppose that $\mathcal{H}_2(d)^2 = \langle A^2 \rangle$ for some $A \in \mathcal{H}_2(d)$ with $A^4 = I$, $A^2 \neq I$. Then $CA^2 = CA^{2m} \in \{C, C^{-1}\}$, hence $CA^2 = C^{-1}$ and therefore $C^4 = I$. $\square$

Now we formulate our main results (Theorems 2, 3 and 4) which will be proved in a uniform way later on.

Theorem 2. *Let d be a discriminant, let a and m be positive integers, and let $\Gamma \subset \mathcal{H}(d)$ and $\Delta \subset (\mathbb{Z}/a\mathbb{Z})^\times$ be any subsets. Suppose that for every prime p (except possibly a set of Dirichlet density zero) the following holds: If $\left(\frac{d}{p}\right) = 1$ and $p^m + a\mathbb{Z} \in \Delta$, then $C \to p^m$ for some $C \in \Gamma$.*

Let Ω be the set of all classes $C \in \mathcal{H}(d)$ representing some prime power p^m such that $p \nmid d$ and $p^m + a\mathbb{Z} \in \Delta$, and assume that $\Gamma \subset \Omega$. Then

$$\Omega = \Omega\mathcal{H}(d)^{2m} = \Gamma \cup \Gamma^{-1} \subset \mathcal{H}(d)^m,$$

where $\Gamma^{-1} = \{C \in \mathcal{H}(d) \mid C^{-1} \in \Gamma\}$. In particular, Ω consists of full cosets modulo $\mathcal{H}(d)^{2m}$.

From a qualitative point of view, Theorem 2 asserts that either Γ is large or $\mathcal{H}(d)^{2m}$ is small. This will become plain in Theorem 4, when we will consider the case $|\Gamma| = 1$. The subsequent Theorem 3 generalizes [7], Theorem 1.

Theorem 3. *Let assumptions be as in Theorem 2. Let $K \in \mathcal{H}(d)$ and $k \in \mathbb{Z}$ be such that $K \to k$ and $\gcd(k, ad) = 1$.*

Then for every prime p satisfying $\left(\frac{d}{p}\right) = 1$ and $p^m + a\mathbb{Z} \in k^m\Delta$, there exists some $C \in \Omega$ such that $K^mC \to p^m$.

Theorem 4. *Let assumptions be as in Theorem 2, and suppose in addition that $\Gamma = \{C\}$ consists of a single class. Then the following holds.*

1. $|\Omega| = |\mathcal{H}(d)^{2m}| \leq 2$.
2. *Suppose that $m = 2^tm'$, where $t \geq 0$ and $m' \in \mathbb{N}$ is odd, and let $\mathcal{H}_2(d)$ be of type $(2^{t_1}, 2^{t_2}, \ldots, 2^{t_s})$, where $s \geq 0$ and $t_1 \geq t_2 \geq \ldots \geq t_s \geq 1$.*

Then $\mathcal{H}'(d)^{m'} = \{1\}$, $t_2 \le t+1$ *and*

$$t_1 \le \begin{cases} t+2, & \text{if} \quad C \ne C^{-1}, \\ t+1, & \text{if} \quad C = C^{-1}. \end{cases}$$

3. *Suppose in addition that* $m = 1$, *and let* Δ' *be the set of all residue classes* $p + d^*\mathbb{Z} \in X_d$ *of primes* p *such that* $p + a\mathbb{Z} \in \Delta$. *Then we have* $|\omega_d(\Delta')| = 1$ *and* $\mathbb{Q}^{(d^*)} \subset \mathbb{Q}^{(a)}(\sqrt{d})$.

Remark. Kaplan and Williams [7] considered the case $m = 1$, $\Gamma = \{C\}$ and $\Delta = \{b + a\mathbb{Z}\}$ for some $b \in \mathbb{Z}$ such that $\gcd(a,b) = 1$. They assumed moreover that a is even and that every prime $p \in b + a\mathbb{Z}$ with $p \nmid d$ is represented by C. Then every prime $p \in b + a\mathbb{Z}$ with $p \nmid d$ satisfies $\left(\frac{d}{p}\right) = 1$. Therefore it follows that $\mathbb{Q}(\sqrt{d}) \subset \mathbb{Q}^{(a)}$, hence $\mathbb{Q}^{(d^*)} \subset \mathbb{Q}^{(a)}$ and $d^* \mid a$, since a is even.

Proof of the Theorems. Let $\Delta_0 \subset (\mathbb{Z}/a\mathbb{Z})^\times$ be the set of all residue classes $p + a\mathbb{Z}$ of primes p such that $\left(\frac{d}{p}\right) = 1$ and $p^m + a\mathbb{Z} \in \Delta$. We may assume that $\Delta = \Delta_0^m \subset (\mathbb{Z}/a\mathbb{Z})^\times$ (the other residue classes of Δ are of no interest). Let Γ_0 be the set of all classes $C \in \mathcal{H}(d)$ such that $C^m \in \Gamma$. Since $\Gamma \subset \mathcal{H}(d)^m$ by assumption, we have $\Gamma = \Gamma_0^m$. For the same reason, $\Omega = \Omega_0^m$, where Ω_0 is the set of all classes $C \in \mathcal{H}(d)$ representing some prime p satisfying $p \nmid d$ and $p + a\mathbb{Z} \in \Delta_0$. Now $\Omega_0 = \Omega_0\mathcal{H}(d)^2$ consists of full genera by Proposition 1, and therefore $\Omega = \Omega_0^m = \Omega_0^m\mathcal{H}(d)^{2m} = \Omega\mathcal{H}(d)^{2m}$.

If $C \in \Omega$, then $C = C_0^m$ for some $C_0 \in \Omega_0$ and (by Proposition 1) the set of all primes p such that $p + a\mathbb{Z} \in \Delta_0$ and $C_0 \to p$ has positive Dirichlet density. Hence the set of all primes p such that $p^m + a\mathbb{Z} \in \Delta$ and $C \to p$ has positive Dirichlet density, too. Therefore there exists some $C' \in \Gamma$ representing a prime power which is also represented by C, hence $C \in \{C', {C'}^{-1}\} \subset \Gamma \cup \Gamma^{-1}$, and $\Omega \subset \Gamma \cup \Gamma^{-1}$ follows. The other inclusion is obvious, since Γ and Γ^{-1} represent the same prime powers. This argument completes the proof of Theorem 2.

For the proof of Theorem 3, let p be a prime satisfying $\left(\frac{d}{p}\right) = 1$ and $p^m + a\mathbb{Z} \in k^m\Delta$. Let p_0 be a prime satisfying $p \equiv kp_0 \bmod ad$. Then

$$1 = \left(\frac{d}{p}\right) = \left(\frac{d}{k}\right)\left(\frac{d}{p_0}\right) = \left(\frac{d}{p_0}\right),$$

and $p^m \equiv k^m p_0^m \bmod a$ implies $p_0 + a\mathbb{Z} \in \Delta_0$, whence $C_0 \to p_0$ for some $C_0 \in \Gamma_0$. Let $C_1 \in \mathcal{H}(d)$ be such that $C_1 \to p$. Then $C_1^m \to p^m$,

$$C_1\mathcal{H}(d)^2 = \omega_d(p + d^*\mathbb{Z}) = \omega_d(k + d^*\mathbb{Z})\,\omega_d(p_0 + d^*\mathbb{Z}) = KC_0\mathcal{H}(d)^2,$$

and therefore $C_1 = KC_0A^2$ for some $A \in \mathcal{H}(d)^2$, which implies $C_1^m = K^mC$, where $C = C_0^mA^{2m} \in \Omega$.

It remains to prove Theorem 4. Suppose that $\Gamma = \{C\}$ and $C = C_1^m$. Then

$$\Omega = \Omega\mathcal{H}(d)^{2m} = \{C, C^{-1}\} = C_1^m\mathcal{H}(d)^{2m} ,$$

and therefore

$$|\Omega| = |\mathcal{H}(d)^{2m}| = \begin{cases} 2, & \text{if} \quad C \neq C^{-1} , \\ 1, & \text{if} \quad C = C^{-1} . \end{cases}$$

Since $\mathcal{H}(d)^{2m} = \mathcal{H}'(d)^{m'} \times \mathcal{H}_2(d)^{2^{t+1}}$ and $\mathcal{H}_2(d)^{2^{t+1}}$ is of type $(2^{((t_1-t-1))}, \ldots, 2^{((t_s-t-1))})$, where $((r)) = \max\{r, 0\}$, the assertions 1. and 2. of Theorem 4 follow.

If in addition $m = 1$, then clearly $|\omega_d(\Delta')| = 1$. Also, for every prime p with $\left(\frac{d}{p}\right) = 1$, the residue class $p + d^*\mathbb{Z}$ is uniquely determined by $p + a\mathbb{Z}$. Therefore Čebotarev's theorem implies $\mathbb{Q}^{(d^*)} \subset \mathbb{Q}^{(a)}(\sqrt{d})$. $\square$

References

[1] H. Cohn, *A Classical Invitation to Algebraic Numbers and Class Fields.* Springer, 1978.
[2] D. A. Cox, *Primes of the form $x^2 + ny^2$.* J. Wiley, 1989.
[3] F. Halter-Koch, *Representation of primes by binary quadratic forms of discriminant $-256q$ and $-128q$.* Glasgow Math. J. **35** (1993), 261–268.
[4] F. Halter-Koch, *A Theorem of Ramanujan Concerning Binary Quadratic Forms.* J. Number Theory **44** (1993), 209–213.
[5] F. Halter-Koch, *Geschlechtertheorie der Ringklassenkörpers.* J. Reine Angew. Math. **250** (1971), 107–108.
[6] H. Hasse, *Number Theory.* Springer, 1980.
[7] P. Kaplan, K. S. Williams, *Representation of Primes in Arithmetic Progressions by Binary Quadratic Forms.* J. Number Theory **45** (1993), 61–67.
[8] T. Kusaba, *Remarque sur la distribution des nombres premiers.* C. R. Acad. Sci. Paris Sér. A **265** (1967), 405–407.
[9] A. Meyer, *Über einen Satz von Dirichlet.* J. Reine Angew. Math. **103** (1888), 98–117.

Franz Halter-Koch
Institut für Mathematik
Karl-Franzens-Universität Graz
Heinrichstraße 36
8010 Graz
Austria
E-mail : franz.halterkoch@uni-graz.at