ILLINOIS JOURNAL OF MATHEMATICS
Volume 27, Number 2, Summer 1983

SETS OF PRIMES DETERMINED BY SYSTEMS OF POLYNOMIAL CONGRUENCES

BY

J. C. LAGARIAS

1. Introduction

Fermat considered the problem of characterizing the set Σ_Q of primes p for which

$$Q(x, y) = ax^2 + bxy + cy^2 = \pm p \tag{1.1}$$

for some integers x, y. In a letter to Mersenne dated December 26, 1640, he asserted that the form $x^2 + y^2$ represented all primes $p \equiv 1 \pmod 4$ and no primes $p \equiv 3 \pmod 4$. In a letter to Pascal written in 1654, he asserted that for the forms $x^2 + 2y^2$, $x^2 + 3y^2$ the sets Σ_Q consisted of all primes in certain arithmetic progressions. He conjectured the same for $x^2 + 5y^2$ (see [7, p. 3]). It is plausible that Fermat had proofs of his assertions, although he never revealed them [17, p. 104]. Some of Fermat's assertions were subsequently proved by Euler in 1761. Euler had already observed that for other forms, e.g., $x^2 + 11y^2$, there was no obvious characterization of the set Σ_Q in terms of primes in arithmetic progressions [7, p. 3].

The problem of characterizing the sets Σ_Q motivated many subsequent investigations. Gauss considered two binary quadratic forms Q_1 and Q_2 to be equivalent if one can be obtained from the other by a unimodular integer transformation of variables. Equivalent forms represent the same sets of primes. A form can represent infinitely many primes only if it is *primitive*, i.e., $(a, b, c) = 1$. The set of all primitive forms having the same *discriminant* $D = b^2 - 4ac$ fall into a finite set of equivalence classes, which we denote $\mathrm{Cl}(D)$. Gauss developed a theory of *genera* which restricted the values that could be represented by a given binary quadratic form to be those for which certain auxiliary quadratic congruences were solvable or unsolvable in specified ways. For example, for $D = -164 = -4.41$, there are eight classes in $\mathrm{Cl}(D)$. There are two auxiliary quadratic congruences:

$$\text{(A)} \quad x_1^2 \equiv 41 \pmod p, \tag{1.2}$$

$$\text{(B)} \quad x_2^2 \equiv -1 \pmod p. \tag{1.3}$$

Received April 20, 1982.

The eight classes fall into two *genera* as follows:

$$p = \begin{Bmatrix} x^2 + 41y^2 \\ 2x^2 + 2xy + 21y^2 \\ 5x^2 \pm 4xy + 9y^2 \end{Bmatrix} \Leftrightarrow \text{(A), (B) both solvable,} \tag{1.4}$$

$$p = \begin{Bmatrix} 3x^2 \pm 2xy + 14y^2 \\ \\ 6x^2 \pm 2xy + 7y^2 \end{Bmatrix} \Leftrightarrow \text{(A) solvable, (B) not solvable.} \tag{1.5}$$

Those p for which (A) is unsolvable are not represented by any form of discriminant -164. Thus, (1.4) shows that Σ_Q for $Q = x^2 + 41y^2$ satisfies

$$\Sigma_Q \subseteq \Sigma_A \cap \Sigma_B,$$

where Σ_A, Σ_B are the sets of primes for which (1.2) and (1.3), respectively, are solvable. The sets Σ_A and Σ_B consist of primes in certain arithmetic progressions (mod 41) and (mod 4) respectively; this is a consequence of the quadratic reciprocity law. The assertion (1.4) says that a prime p for which (A) and (B) are solvable is represented by at least one of the forms on the left side of (1.4), but does not specify which one(s).

A further separation of the sets of primes represented by classes of quadratic forms can be obtained using class field theory. For the example $D = -164$, using an explicit construction of the Hilbert class field of $\mathbf{Q}(\sqrt{-41})$, H. Cohn and G. Cooke [6] showed that the additional polynomial congruences

$$\text{(C)} \quad x_3^2 \equiv 32 + 5x_1x_2 \pmod{p},$$

$$\text{(D)} \quad x_4^2 \equiv (3 + x_1)(1 + x_2)x_3 \pmod{p},$$

can be used to refine (1.4) as follows:

$$p = x^2 + 41y^2 \qquad \Leftrightarrow \text{(A), (B), (C), (D) solvable,}$$

$$p = 2x^2 + 2xy + 21y^2 \Leftrightarrow \text{(A), (B), (C) solvable and (D) not solvable,}$$

$$p = 5x^2 \pm 4xy + 9y^2 \quad \Leftrightarrow \text{(A), (B) solvable and (C) not solvable.}$$

However, these congruences do not separate the forms in (1.5). Cohn and Cooke raised the question of whether there is any way to "congruentially" distinguish the primes represented by the forms $3x^2 \pm 2xy + 14y^2$ from those represented by the forms $6x^2 \pm 2xy + 7y^2$.

This paper considers Cohn and Cooke's question in the context of characterizing those sets of primes determined by systems of polynomial congruences. Let $\mathbf{P}$ denote the set of all primes. Let S denote a (simultaneous) system of polynomial congruences given by

$$f_1(x_1, \ldots, x_n) \equiv 0 \pmod{p}, \qquad f_m(x_1, \ldots, x_n) \equiv 0 \pmod{p}. \tag{1.6}$$

Let Σ_S denote the set of primes for which (1.6) is solvable, and $\Sigma_S^c = \mathbf{P} - \Sigma_S$ those for which it is not. We call a set Σ_S for S given by (1.6) an *elementary SPC-set*. (Here SPC is an abbreviation for Systems of Polynomial Congruences.) An *SPC-set* Σ is any set of primes in the Boolean algebra of subsets of $\mathbf{P}$ generated by all the sets Σ_S, i.e., Σ is a finite union of sets of the form

$$\Sigma_{S_1} \cap \cdots \cap \Sigma_{S_k} \cap \Sigma_{S_{k+1}}^c \cap \cdots \cap \Sigma_{S_l}^c.$$

In characterizing sets of primes, we define sets Σ_1 and Σ_2 of primes to be *equivalent*, written $\Sigma_1 \approx \Sigma_2$, if they differ by only a finite set of primes.

We shall relate SPC-sets to the sets of primes having a given Artin symbol over a finite algebraic number field; these are exactly the sets of primes to which the Chebotarev density theorem applies [4]. Let K be a finite Galois extension of $\mathbf{Q}$ and let D_K be the discriminant of K. Let p be a prime with $p \nmid D_K$. To any prime ideal P lying over (p), we associate the *Frobenius automorphism* $\sigma = \sigma_P \in \mathrm{Gal}(K/\mathbf{Q})$ over $\mathbf{Q}$ which is the unique σ for which

$$\alpha^\sigma \equiv \alpha^p \pmod{P}$$

for all algebraic integers α in K. For $p \nmid D_K$ the *Artin symbol* is given by

$$\left[\frac{K/\mathbf{Q}}{(p)}\right] = \{\sigma_P : P \text{ lies over } (p) \text{ in } K\}.$$

It is a conjugacy class of $\mathrm{Gal}(K/\mathbf{Q})$. To each conjugacy class C of $\mathrm{Gal}(K/\mathbf{Q})$, we associate the *elementary Chebotarev set*

$$\Gamma(C, K) = \left\{p : \left[\frac{K/\mathbf{Q}}{(p)}\right] = C\right\}. \tag{1.7}$$

A *Chebotarev set* is any set in the Boolean algebra of subsets of $\mathbf{P}$ generated by the elementary Chebotarev sets. The set of primes Σ_Q represented by a binary quadratic form Q is equivalent to a Chebotarev set (see Theorem 4.1).

SPC-sets are related to a subclass of the Chebotarev sets which we call *Frobenius sets*.[1] To define these, we say elements τ_1, τ_2 of a group G are in the same *division* if there exists an element $\sigma \in G$ and an integer j with $(j, \mathrm{ord}(\tau_1)) = 1$ such that

$$\sigma\tau_1\sigma^{-1} = \tau_2^j. \tag{1.8}$$

This is an equivalence relation, and divides G up into cosets under this

[1] These sets are exactly the sets of primes described in the Frobenius density theorem (cf. [11, II, p. 129]), hence the choice of name.

equivalence which we call *divisions*. (This is a translation of the term *Abteilung* used by Frobenius [8], [11].) A division $\tilde{C}$ of G is a disjoint union of conjugacy classes. An *elementary Frobenius set* associated to a division $\tilde{C}$ of Gal($K/\mathbf{Q}$) is given by

$$\Gamma(\tilde{C}, K) = \left\{p : \left[\frac{K/\mathbf{Q}}{(p)}\right] \subseteq \tilde{C}\right\} = \bigcup_{C \subseteq \tilde{C}} \Gamma(C, K), \tag{1.9}$$

where C runs over the conjugacy classes of Gal($K/\mathbf{Q}$). A *Frobenius set* is any set in the Boolean algebra of subsets of $\mathbf{P}$ generated by the elementary Frobenius sets.

We characterize SPC-sets as follows.

THEOREM 1.1. *Any SPC-set is equivalent to a Frobenius set. Conversely, any Frobenius set is an SPC-set.*

We also show that elementary Frobenius sets can also be characterized as the minimal sets of primes determined by splitting conditions on the ideal (p) in an algebraic number field. This characterization has been known in principle since Frobenius' time, but I do not know of any explicit statement of it in the literature. To state this characterization precisely, let k be a finite extension of $\mathbf{Q}$, not necessarily Galois, and let p be a prime, $p \nmid D_k$. Then in the ring of integers of k one has the ideal factorization

$$(p) = \prod_{i=1}^{g} q_i$$

where the q_i are distinct prime ideals whose norms are given by

$$Nq_i = p^{f_i}.$$

We call the partition of $n = [k:\mathbf{Q}]$ given by

$$Spl(p; k) = \{f_i : 1 \leq i \leq g\}$$

the *splitting type* of p in k.

THEOREM 1.2. *Let K be a normal extension of* $\mathbf{Q}$. *Let $\tilde{C}_1$, $\tilde{C}_2$ be distinct divisions of* Gal($K/\mathbf{Q}$).

(i) *If p_1, p_2 are primes in $\Gamma(\tilde{C}, K)$ then*

$$Spl(p_1; k) = Spl(p_2; k)$$

for all subfields k of K.

(ii) *If $p_1 \in \Gamma(\tilde{C}_1, K)$ and $p_2 \in \Gamma(\tilde{C}_2, K)$ then there is a subfield k of K for which*

$$Spl(p_1; k) \neq Spl(p_2; k).$$

Theorem 1.1 cannot be used to decide if a given set of primes Σ is an SPC-set until we have criteria to recognize whether Σ is equivalent to a Frobenius set. Our next result is a finite criterion to decide whether or not certain Chebotarev sets are Frobenius sets. We say a Chebotarev set is *defined over K* if it is a union of elementary Chebotarev sets $\Gamma(C, K)$. It is a fact that every Chebotarev set is equivalent to a Chebotarev set defined over some field K (Lemma 3.1). We say analogously that a Frobenius set is *defined over K* if it is a union of elementary Frobenius sets $\Gamma(\tilde{C}, K)$. Every Frobenius set is equivalent to a Frobenius set defined over some field K (Lemma 3.2).

THEOREM 1.3. *A Chebotarev set defined over K is equivalent to a Frobenius set if and only if it is a Frobenius set defined over K.*

We apply Theorems 1.1 and 1.3 to decide whether or not certain specific sets of primes are equivalent to SPC-sets. The elementary Chebotarev sets for $\mathbf{Q}(\exp(2\pi i/d))$ are just sets of primes in arithmetic progressions (mod d). We obtain the following result.

THEOREM 1.4. *The set* $\{p \mid p \equiv a \pmod{d}\}$ *is equivalent to an SPC-set if and only if either a is of order* 1 *or* 2 *in* $(\mathbf{Z}/d\mathbf{Z})^*$ *or* $(a, d) > 1$.

This theorem shows, for example, that $\{p \mid p \equiv 2 \pmod{5}\}$ is not equivalent to an SPC-set.

The primes represented by a given primitive form $Q(x, y)$ of discriminant D are an elementary Chebotarev set for a certain class field over $\mathbf{Q}(\sqrt{D})$. We obtain the following result.

THEOREM 1.5. *Let Q be a primitive binary quadratic form of discriminant D. The set*

$$\Sigma_Q = \{p \mid Q(x, y) = \pm p \text{ for some } x, y \in \mathbf{Z}\}$$

is equivalent to an SPC-set if and only if $[Q]$ *is of order* 1, 2, 3, 4 *or* 6 *in the form class group* $\mathrm{Cl}(D)$.

In particular the sets

$$\Sigma_1 = \{p : p = 3x^2 \pm 2xy + 14y^2\}, \qquad \Sigma_2 = \{p : p = 6x^2 \pm 2xy + 7y^2\},$$

in Cohn and Cooke's example arise from classes of order 8 in $\mathrm{Cl}(D)$. Theorem 1.5 asserts these are not equivalent to SPC-sets. Thus Cohn and Cooke's question is answered in the negative.

Theorem 1.4 shows that the set of primes Σ_Q representable by a given binary quadratic form Q cannot always be described in terms of polynomial congruences. Such sets Σ_Q can be characterized in other ways. Recently S. Gurak [9] has given criteria to recognize the set of primes Σ_Q represented by an arbitrary binary quadratic form Q in terms of the values of certain auxiliary linear recurrences (mod p).

Theorem 1.1 and 1.2 are proved in Section 2. The proof of Theorem 1.1 reduces the problem to considering SPC-sets determined by congruences in one variable by a result of Ax [1] (see also Odoni [12]). Factorization of polynomials in one variable (mod p) is related to splitting of primes in number fields, and the theorem follows using elementary group-theoretic arguments.

Theorem 1.3 is proved in Section 3 by simple group-theoretic arguments. The applications follow in Section 4.

2. SPC-sets and Frobenius sets

We observe first that if Σ_1 is an SPC-set and $\Sigma_1 \approx \Sigma_2$, then Σ_2 is an SPC-set. Indeed, if q is a prime, the set of primes for which

$$qx + 1 \equiv 0 \pmod{p} \tag{2.1}$$

is solvable is just $\mathbf{P} - \{q\}$. Consequently, using unions, intersections and complements of such sets, we can add or delete any finite set of primes to Σ_1 and still have an SPC-set.

Proof of Theorem 1.1. Let A_k denote the Boolean algebra generated by the elementary SPC-sets Σ_S where S is given by a set of polynomials

$$f_i(x_1, \ldots, x_k) \equiv 0 \pmod{p},$$

for $1 \leqslant i \leqslant m$ all lying in $\mathbf{Z}[x_1, \ldots, x_k]$. Clearly, $A_1 \subseteq A_2 \subseteq A_3 \subseteq \ldots$ and $A = \cup_{k=1}^{\infty} A_k$ is the collection of all SPC-sets. Ax [1] (see also Odoni [12, Theorem 1A]) proves the following result.

PROPOSITION 2.1. $A_1 = A$.

Let F denote the Boolean algebra of all Frobenius sets, and define

$$F^* = \{\Sigma : \Sigma \approx \Gamma \text{ for some } \Gamma \in F\}.$$

F^* is a Boolean algebra of sets. The assertion of Theorem 1.1 is that $F^* = A$.

To show $A \subseteq F^*$ it suffices by Proposition 2.1 to show $A_1 \subseteq F^*$. To do this it suffices to show that $\Sigma_S \in F^*$ for a set of Σ_S that generate A_1 as a Boolean algebra.

LEMMA 2.2. *A_1 is generated as a Boolean algebra by the sets Σ_S where $S = \{f(x)\}$ and $f(x)$ is a single polynomial irreducible over* $\mathbf{Z}[x]$.

Proof. We know A_1 is generated by sets Σ_S where

$$S = \{f_i(x)\}_{i=1}^{m}. \tag{2.2}$$

Suppose $F_1(x) = g_1(x)g_2(x)$ over $\mathbf{Z}[x]$. Then

$$\Sigma_S = \Sigma_{S_1} \cup \Sigma_{S_2} \quad \text{where } S_j = \{g_j(x)\} \cup \{f_i(x)\}_{i=1}^{n} \text{ for } j = 1, 2.$$

This shows that any Σ_S of the form (2.2) decomposes as a finite union of sets of the form (2.2) where all the $f_i(x)$ are distinct irreducible polynomials over $\mathbf{Z}[x]$, so that A_1 is generated by Σ_S of this special form.

We claim that if Σ_S involves two or more distinct irreducible polynomials, then Σ_S is a finite set. Indeed distinct irreducible polynomials are relatively prime over $\mathbf{Q}[x]$, so we can find $h_1(x)$, $h_2(x) \in \mathbf{Z}[x]$ such that

$$f_1(x)h_1(x) + f_2(x)h_2(x) = N,$$

where N is a nonzero integer. Hence,

$$f_i(x) \equiv 0 \pmod{p}$$

for $i = 1, 2$ implies $N \equiv 0 \pmod{p}$ so Σ_S is finite. But all sets Σ can be obtained as unions of complements of sets Σ_S where $S = \{qx + 1\}$ as in (2.1). The lemma follows. ■

We next show that sets Σ_S where $S = \{f(x)\}$ and $f(x)$ is irreducible are described in terms of Artin symbols in the normal closure of a field $\mathbf{Q}(\theta)$ generated by a root θ of $f(x)$.

LEMMA 2.3. *Let $f(x)$ be an irreducible polynomial over $\mathbf{Z}[x]$. Let θ be a root of $f(x)$, set $k = \mathbf{Q}(\theta)$, and let K be the Galois closure of k. Let*

$$D = \operatorname{disc}(K) \cdot \operatorname{disc}(f(x))N_{K/Q}(\theta).$$

When $(p, D) = 1$, the following are equivalent:

(i) *The congruence $f(x) \equiv 0 \pmod{p}$ is solvable.*
(ii) *There is a prime ideal of degree one lying over (p) in $\mathbf{Q}(\theta)$.*
(iii) *The conjugacy class*

$$\left[\frac{K/\mathbf{Q}}{(p)}\right]$$

of $\operatorname{Gal}(K/\mathbf{Q})$ *contains an element* $\tau \in \operatorname{Gal}(K/k)$.

Proof. (i) ⇔ (ii) This is a result of Kummer; cf. Lang [13, p. 27].

(ii) ⇒ (iii) Let O_K denote the ring of integers of K. Let $\bar{p}$ be a prime ideal of degree 1 in k lying over (p), and P a prime ideal of K lying over $\bar{p}$. Note (p) is unramified in K since $p \nmid \operatorname{disc}(K)$. Now there is a

$$\sigma \in \left[\frac{K/k}{\bar{p}}\right]$$

such that

$$x^{\sigma} \equiv x^{N\bar{p}} = x^{p} \pmod{P}$$

for all $x \in O_K$. For the same P, there is some

$$\tau \in \left[\frac{K/\mathbf{Q}}{(p)}\right]$$

such that $x^\tau \equiv x^p \pmod{P}$ for all $x \in O_K$. Hence,

$$x^{\sigma\tau^{-1}} - x \equiv 0 \pmod{P}.$$

Hence $\sigma\tau^{-1}$ is in the inertia group, which is trivial since (p) is unramified, so $\sigma = \tau$. But $\sigma \in \mathrm{Gal}(K/k)$.

(iii) $\Rightarrow$ (i) By hypothesis there exists a prime ideal P in K lying over (p) with $\sigma = \sigma_P$ and $\sigma \in \mathrm{Gal}(K/k)$ such that

$$x^\sigma \equiv x^p \pmod{P} \tag{2.3}$$

for all $x \in O_K$. Let P lie over $\tilde{p}$, where $\tilde{p}$ is in k. Since σ leaves k fixed (2.3) yields

$$x \equiv x^p \pmod{P},$$

for all $x \in O_k$. Applying $\tau \in \mathrm{Gal}(K/k)$ we obtain $x \equiv x^p \pmod{P^\tau}$, for all $x \in O_k$. This implies that

$$x^p \equiv x \pmod{\tilde{p}}, \tag{2.4}$$

by the Chinese remainder theorem, since $\tilde{p}O_K = \Pi_\tau P^\tau$ where τ runs over all elements of $\mathrm{Gal}(K/k)$. In particular (2.4) gives $\theta^p \equiv \theta \pmod{\tilde{p}}$. Since θ is prime to $\tilde{p}$, we obtain

$$\theta^{p-1} \equiv 1 \pmod{\tilde{p}}.$$

However, the elements $1, 2, \ldots, p - 1$ are the complete set of roots to $x^{p-1} \equiv 1 \pmod{\tilde{p}}$, so $\theta = a \pmod{\tilde{p}}$ for some $a \in \mathbf{Z}$. Hence $f(a) \equiv 0 \pmod{\tilde{p}}$ so that $f(a) \equiv 0 \pmod{p}$. ■

We continue the proof of Theorem 1.1. It is now easy to show $A \subseteq F^*$. Given Σ_S with $S = \{f(x)\}$ an irreducible polynomial, then by Lemma 2.3,

$$\Sigma_S \approx \cup' \Gamma(C, K) \tag{2.5}$$

where the prime indicates the union is over all conjugacy classes C containing an element of $\mathrm{Gal}(K/k)$. Now the right side of (2.5) is actually a union of divisions. To see this, suppose C_1, C_2 are two conjugacy classes in the same division, so that there exist $\tau_i \in C_i$ with $\tau_1^j = \tau_2$ for some integer j. If $\sigma \in \mathrm{Gal}(K/k)$ is in C_1 then $\sigma = \mu\tau_1\mu^{-1}$ for some μ. Then

$$\mu\tau_2\mu^{-1} = \mu\tau_1^j\mu^{-1} = (\mu\tau_1\mu^{-1})^j = \sigma^j$$

is in $\mathrm{Gal}(K/k) \cap C_2$. Hence, the right side of (2.5) is a Frobenius set. By Lemma 2.2 we conclude $A \subseteq F^*$.

To show $F^* \subseteq A$, it suffices to show $F \subseteq A$, by the remarks preceding the proof. To show $F \subseteq A$ we need only show that each elementary Frobenius set Σ is equivalent to a set in A. Let $\tilde{C}'$ be a division of $G = \mathrm{Gal}(K/\mathbf{Q})$. Take $\sigma \in \tilde{C}'$, let $H = \langle\sigma\rangle$ be the cyclic subgroup generated by σ, and let k be the fixed field of H. By the theorem of the primitive element, we can write $k = \mathbf{Q}(\theta)$, where θ is an algebraic integer, and let $f(x)$ be the irreducible polynomial over $\mathbf{Q}$ of which θ is a root. If $S = \{f\}$, then by Lemma 2.3, $\Sigma_S \approx \bigcup'\Gamma(\tilde{C}, K)$ where the prime indicates the union is over all divisions $\tilde{C}$ with $\sigma^i \in \tilde{C}'$ for some i. Let $n = \mathrm{ord}(\sigma)$ and let $p_1, \ldots, p_m$ be the primes dividing n. Repeat the construction above for the cyclic groups $H_i = \langle\sigma^{p_i}\rangle$ with associated fixed fields $\mathbf{Q}(\theta_i)$ and polynomials $f_i(x)$. If $S_i = \{f_i(x)\}$, then

$$\Sigma_{S_i} \approx \bigcup{}'\Gamma(\tilde{C}, K)$$

where the prime indicates the union is over all divisions $\tilde{C}$ with $\sigma^{jp_i} \in \tilde{C}'$ for some j. Consequently,

$$\Sigma_S \cap \left(\bigcap_{i=1}^{m}(\mathbf{P} - \Sigma_{S_i})\right] \approx \bigcup_{\substack{\sigma^j \in \tilde{C} \\ (j,n)=1}} \Gamma(\tilde{C}, K). \tag{2.6}$$

But if $\sigma \in \tilde{C}'$ then all σ^i with $(i, n) = 1$ are in $\tilde{C}'$. Thus the right side of (2.6) is just $\Gamma(\tilde{C}', K)$ while the left side is an SPC-set. ∎

Proof of Theorem 1.2. To prove (i), we show how to recover $Spl(p; k)$ for any given subfield k of K from the Artin symbol

$$\left[\frac{K/\mathbf{Q}}{(p)}\right],$$

and then show that $Spl(p; k)$ depends only on the division $\tilde{C}$ of $\mathrm{Gal}(K/\mathbf{Q})$ which

$$\left[\frac{K/\mathbf{Q}}{(p)}\right]$$

is in.

Let (p) be unramified over K, let $\tilde{p}$ be a prime of k lying over (p), and $\mathbf{P}$ a prime of K lying over $\tilde{p}$. Set $N\tilde{p} = N_{k/Q}\tilde{p} = p^f$.

The following proposition (Hasse [10], Bd. III, pp. 123–4) describes how $Spl(p; k)$ may be recovered from

$$\left[\frac{K/\mathbf{Q}}{(p)}\right].$$

PROPOSITION 2.4. *Consider a prime $p \nmid D_k$ and a prime ideal $\mathbf{P}$ of K lying over (p). Let $G = \mathrm{Gal}(K/\mathbf{Q})$, $H = \mathrm{Gal}(K/k)$ and let $Z = Z(\mathbf{P}) = \langle\sigma_{\mathbf{P}}\rangle$ be* *the cyclic subgroup of G generated by the Frobenius automorphism $\sigma_{\mathbf{P}}$. Choose double coset representatives $\{\tau_i\colon 1 \leqslant i \leqslant r\}$ for $H\ G\backslash Z$ so that G is the disjoint union*

$$G = \bigcup_{i=1}^{r} H\tau_i Z.$$

Then the ideal factorization of (p) over k has the form

$$(p) = \prod_{i=1}^{r} q_i.$$

The prime ideals q_i are given by

$$q_i = \prod \tau(\mathbf{P}),$$

where the product is over all distinct prime ideals of K of the form $\tau(\mathbf{P})$ for some $\tau \in H\tau_i Z$. In addition

$$N_{k/Q} q_i = p^{f_i}$$

where f_i is the smallest positive integer such that $(\sigma_i)^{f_i} \in H$ where $\sigma_i = \tau_i \sigma_{\mathbf{P}} \tau_i^{-1}$.

Note that for any i the integer f_i depends only on Z and not on the particular choice of generator σ_i of Z. Now let

$$C_1 = \left[\frac{K/\mathbf{Q}}{(p_1)}\right]$$

and let

$$C_2 = \left[\frac{K/\mathbf{Q}}{(p_2)}\right]$$

be another conjugacy class in $\tilde{C}$, so that $C_2 = C_1^k$ for some k with $(k, \text{ord } C_1) = 1$. Then we observe that there are prime ideals $\mathbf{P}_1$, $\mathbf{P}_2$ in K lying over (p_1), (p_2) respectively whose Frobenius automorphisms $\sigma_{\mathbf{P}_1}$, $\sigma_{\mathbf{P}_2}$ satisfy $\sigma_{\mathbf{P}_2} = (\sigma_{\mathbf{P}_1})^k$. Since $Z(\mathbf{P}_1) = Z(\mathbf{P}_2)$ in this case, Proposition 2.4 immediately implies that

$$Spl(p_1; k) = Spl(p_2; k).$$

This proves (i).

To prove (ii), let

$$\left[\frac{K/\mathbf{Q}}{(p_1)}\right] \quad \text{and} \quad \left[\frac{K/\mathbf{Q}}{(p_2)}\right]$$

lie in different divisions $\tilde{C}_1$ and $\tilde{C}_2$ of Gal($K/\mathbf{Q}$). In particular, by interchanging

p_1 and p_2 if necessary, we can find an element

$$\sigma \in \left[\frac{K/\mathbf{Q}}{(p_1)}\right]$$

such that $\sigma^j \notin \tilde{C}_2$ for all $j \geq 1$. To see this, suppose $\sigma^j = \tau$ for some $\tau \in \tilde{C}_2$. Then necessarily $(j, \operatorname{ord}(\sigma)) > 1$ since $\tilde{C}_1$ and $\tilde{C}_2$ are distinct divisions. Hence $\operatorname{ord}(\tau) < \operatorname{ord}(\sigma)$. Since $\operatorname{ord}(\tau^j) \leq \operatorname{ord}(\tau)$ for all j, and since all elements of a division have the same order, $\tau^j \notin \tilde{C}_1$ for all j.

Now let k be the field fixed under the group $H = \{\sigma^k : 1 \leq k \leq \operatorname{ord} \sigma\}$. Then Lemma 2.3 shows there is a prime ideal of degree 1 lying over (p_1) in k, i.e., $1 \in Spl(p_1; k)$. On the other hand, Lemma 2.3 also shows $1 \notin Spl(p_2; k)$ because $\tilde{C}_2$ contains no element of $\operatorname{Gal}(K/k) = H$. Hence $Spl(p_1; k) \neq Spl(p_2; k)$. ∎

3. Frobenius sets and Chebotarev sets

Our first step in relating Chebotarev and Frobenius sets is to show that any Chebotarev (resp. Frobenius) set is equivalent to a finite union of elementary Chebotarev (resp. Frobenius) sets defined over a single field K.

LEMMA 3.1. *Let Γ be a Chebotarev set. There is a finite normal extension K of $\mathbf{Q}$ and a set of conjugacy classes C_i of* $\operatorname{Gal}(K/\mathbf{Q})$ *such that* $\Gamma = \bigcup_i \Gamma(C_i, K)$.

Proof. We are given a finite Boolean expression for Γ in terms of elementary Chebotarev sets over different fields. Using the fact that

$$\Gamma(C, K)^c = \mathbf{P} - \Gamma(C, K) \approx \bigcup_{C' \neq C} \Gamma(C', K), \tag{3.1}$$

we may eliminate complements from the expression. By distributing unions over intersections, we may suppose that

$$\Gamma \approx \bigcup_{i=1}^{m} \left(\bigcap_{j=1}^{N_i} \Gamma(C_{ij}, K_{ij}) \right). \tag{3.2}$$

Next suppose that a normal extension K over $\mathbf{Q}$ contains two normal extensions K_1, K_2 over $\mathbf{Q}$. The restriction map

$$i_{K_1} : \operatorname{Gal}(K/\mathbf{Q}) \to \operatorname{Gal}(K_1/\mathbf{Q})$$

sending $\sigma \to \sigma|_{K_1}$ is a homomorphism, as is

$$\sigma_2 : \operatorname{Gal}(K/\mathbf{Q}) \to \operatorname{Gal}(K_2/\mathbf{Q}).$$

Hence, if $\sigma_1 = \tau\sigma_2\tau^{-1}$ in $\operatorname{Gal}(K/\mathbf{Q})$ then

$$\sigma_1|_{K_1} = \tau|_{K_1}\sigma_2|_{K_1}\tau^{-1}|_{K_1} \tag{3.3}$$

and similarly for K_2. From the property of Artin symbols

$$\left[\frac{K_1/\mathbf{Q}}{(p)}\right] = \left[\frac{K/\mathbf{Q}}{(p)}\right]\Bigg|_{K_1}$$

we see that $\Gamma(C_1, K_1)$ is equivalent to a finite union of elementary Chebotarev sets in K. The same is true for $\Gamma(C_2, K_2)$, hence,

$$\Gamma(C_1, K_1) \cap \Gamma(C_2, K_2) \approx \cup_c' \Gamma(C, K), \tag{3.4}$$

where the prime indicates C runs over a certain subset of the conjugacy classes of $\mathrm{Gal}(K/\mathbf{Q})$.

Take K to be the compositum of the fields K_{ij}. By repeatedly applying (3.4) in (3.2), we obtain

$$\Gamma \approx \bigcup_i \Gamma(C_i, K). \qquad \blacksquare$$

LEMMA 3.2. *Let Γ be a Frobenius set. There is a finite normal extension K of $\mathbf{Q}$ and a set of divisions $\tilde{C}_i$ of* $\mathrm{Gal}(K/\mathbf{Q})$ *such that* $\Gamma = \cup_i \Gamma(\tilde{C}_i, K)$.

Proof. Similar to that of Lemma 3.1. We note that (3.3) generalizes to

$$\sigma_1|_{K_1} = \tau|_{K_1}(\sigma_2)^j|_{K_1}\tau^{-1}|_{K_1} \tag{3.5}$$

which shows that if $K_1 \subset K$ and both K_1, K_2 are normal over $\mathbf{Q}$, then $\Gamma(\tilde{C}, K_1) = \cup_i \Gamma(\tilde{C}_i, K)$ for some set $\tilde{C}_i$ of divisions of $\mathrm{Gal}(K/\mathbf{Q})$. $\blacksquare$

Theorem 1.3 is a consequence of the following easy group-theoretic lemma.

LEMMA 3.3. *Let $f : H \to G$ be a surjective homomorphism. Let $\tilde{C}$ be a division of G composed of conjugacy classes $\{C_i\}$ and let $\tilde{C}'$ be a division of H. The following are equivalent.*

(i) $f(\tilde{C}') \cap \tilde{C} \neq \emptyset$.
(ii) $f(\tilde{C}') \cap C_i = C_i$ *for all* i.
(iii) $f(\tilde{C}') \cap \tilde{C} = \tilde{C}$.

Proof. (ii) $\Rightarrow$ (iii) $\Rightarrow$ (i) is obvious.

(i) $\Rightarrow$ (ii) Since $f(C_1) \cap \tilde{C} \neq \emptyset$, pick C_i and $\sigma_i \in C_i$ such that $\sigma_i = f(\sigma_i^*)$, $\sigma_i^* \in \tilde{C}'$. Now let σ_j be an arbitrary element of C_j. There exists an element μ_j and an integer m_j such that

$$\sigma_j = \mu_j(\sigma_i)^{m_j}\mu_j^{-1}, \tag{3.6}$$

where $(m_j, \mathrm{ord}(\sigma_i)) = 1$. Since $\mathrm{ord}(\sigma_i) \mid \mathrm{ord}(\sigma_i^*)$, by adding a suitable multiple of $\mathrm{ord}(\sigma_i)$ to m_j we may suppose $(m_j, \mathrm{ord}(\sigma_i^*)) = 1$. Pick $\mu_j^* \in H$

with $f(\mu_j^*) = \mu_j$. Then set

$$\sigma_j^* = \mu_j^*(\sigma_i^*)^{m_j}(\mu_j^*)^{-1} \tag{3.7}$$

so $\sigma_j^* \in \tilde{C}'$. Applying f to (3.7) and applying (3.6) gives $f(\sigma_j^*) = \sigma_j$ so $\sigma_j \in f(\tilde{C}') \cap C_j$. ■

Proof of Theorem 1.3. We apply Lemma 3.3. Suppose Γ is a Chebotarev set defined over K which is not a Frobenius set defined over K. Hence, there exist conjugacy classes C_1, C_2 in a division such that

$$\Gamma(C_1, K) \subseteq \Gamma, \qquad \Gamma(C_2, K) \cap \Gamma = \emptyset. \tag{3.8}$$

Now we suppose Γ is equivalent to a Frobenius set and obtain a contradiction. By Lemma 3.2 we may suppose $\Gamma \approx \bigcup_i \Gamma(\tilde{C}_i, L)$, and without loss of generality we may suppose $K \subseteq L$. Let f : $\mathrm{Gal}(L/\mathbf{Q}) \to \mathrm{Gal}(K/\mathbf{Q})$ be the restriction map and observe that

$$\Gamma(C_i, K) \approx \bigcup_{f(C)=C_i} \Gamma(C, L), \quad \text{for } i = 1, 2.$$

Consequently, there is some division $\tilde{C}_i$ of $\mathrm{Gal}(L/\mathbf{Q})$ and $C \subseteq \tilde{C}_i$ with $f(C) = C_1$. By Lemma 3.3 there exists another conjugacy class $C' \subseteq \tilde{C}_i$ such that $f(C') = C_2$. Then

$$\Gamma(C', L) \subseteq \Gamma(\tilde{C}_i, L) \cap \Gamma(C_2, K) \subseteq \Gamma \cap \Gamma(C_2, K)$$

is an infinite set of primes, contradicting (3.8). ■

4. Applications

Proof of Theorem 1.4. In the case that $(a, d) > 1$ the set $\{p : p \equiv a \pmod{d}\}$ is finite, hence is an SPC-set.

The classes $\Sigma_a = \{p \mid p \equiv a \pmod{d}\}$ are equivalent to the elementary Chebotarev sets defined over the cyclotomic field $K = \mathbf{Q}(\zeta_d)$ where

$$\zeta_d = \exp\left(\frac{2\pi i}{d}\right).$$

To be precise, let $\sigma_a \in \mathrm{Gal}(K/\mathbf{Q})$ be defined by $(\zeta_d)^{\sigma_a} = (\zeta_d)^a$, and note the mapping $a \to \sigma_a$ gives an isomorphism $(\mathbf{Z}/d\mathbf{Z})^* \cong \mathrm{Gal}(K/\mathbf{Q})$. Since $(\mathbf{Z}/d\mathbf{Z})^*$ is abelian, the conjugacy classes C are single elements a and

$$\Gamma(\sigma_a, K) \approx \{p : p \equiv a \pmod{d}\}$$

(cf. Birch [2, p. 86]). Next note that the division $\tilde{C}_a$ containing an element a of an abelian group A is obviously $\tilde{C}_a = \{a^k : (k, \mathrm{ord}(a)) = 1\}$. If $\mathrm{ord}(a) = n$ then $\tilde{C}_a$ contains $\phi(n)$ elements. The only values of n for which $\phi(n) = 1$ are $n = 1, 2$. Finally σ_a has order 1 or 2 if and only if a has order 1 or 2 in $(\mathbf{Z}/d\mathbf{Z})^*$. ■

Proof of Theorem 1.5. We recall the following facts. Given a discriminant D, we can uniquely write $D = df^2$ where d is a field discriminant, i.e. $d = -4$, ± 8 or $d \equiv 1 \pmod 4$ and d is squarefree or $d/4 \equiv 1 \pmod 4$ and $d/4$ is squarefree. There is an isomorphism ψ between the group of form classes $\mathrm{Cl}(D)$ and the ring class group (mod f) over $\mathbf{Q}(\sqrt{d})$, which we denote by $\mathrm{Cl}_f(\mathbf{Q}(\sqrt{d}))$. Here

$$\mathrm{Cl}_f(\mathbf{Q}(\sqrt{d})) \cong I_f/P_f,$$

where I_f is the (multiplicative) group of integral ideals of $\mathbf{Q}(\sqrt{d})$ with norm relatively prime to f and P_f is the subgroup of I_f consisting of those principal ideals (α) which have a generator α such that

$$\alpha \equiv k \pmod{(f)}, \quad k \in \mathbf{Z}, \tag{4.1}$$

and if $D > 0$ then α is also required to be totally positive. Furthermore, for any prime with $(p, D) = 1$, a form Q in the class $[Q]$ integrally represents p if and only if the corresponding ring class (mod f) contains a prime ideal of norm p. (For these facts see Bruckner [3], Cohn, Chapters 14B, 14C [5], or Stark [15]).

By the fundamental theorem of class field theory, there exists a field K_D called the *ring class field* (mod f) *over* $\mathbf{Q}(\sqrt{d})$ having the following two properties.

(1) *K_D is Galois over* $\mathbf{Q}(\sqrt{d})$.

(2) *The Artin map* $i : I_f \to \mathrm{Gal}(K/\mathbf{Q}(\sqrt{d}))$ *induces an isomorphism*

$$\bar{i} : \mathrm{Cl}_f(\mathbf{Q}(\sqrt{d})) \cong \mathrm{Gal}(K/\mathbf{Q}(\sqrt{d})).$$

We note that the Artin map sends a prime ideal P of $\mathbf{Q}(\sqrt{d})$ to the Artin symbol

$$\left[\frac{K/\mathbf{Q}(\sqrt{d})}{P}\right].$$

We next show that

(3) *K is normal over* $\mathbf{Q}$.

Indeed let $\sigma : K \to \sigma K$ be an isomorphism of K onto one of its conjugate fields. The set of prime ideals that split completely in K are those in P_f, so the ones that split completely in σK are those in $\sigma(P_f)$. But $\sigma(P_f) = P_f$ since (4.1) is invariant under σ and total positivity is also preserved. By the uniqueness of the class-field correspondence, $\sigma K = K$.

We next have the following fact [3, Satz 8].

(4) $\mathrm{Gal}(K/\mathbf{Q})$ *is a generalized dihedral group over* $A = \mathrm{Gal}(K/\mathbf{Q}(\sqrt{d}))$. *It has the presentation*: $\sigma^2 = e$, $\sigma a \sigma^{-1} = a^{-1}$ *for all* $a \in A$.

In this case

$$\mathrm{Gal}(K/\mathbf{Q}) = \{a : a \in A\} \cup \{\sigma a : a \in A\} \tag{4.2}$$

is the semi-direct product of Gal $(k/\mathbf{Q}(\sqrt{d}))$ by $\mathbf{Z}/2\mathbf{Z}$ with the specified dihedral action.

The next two lemmas supply the information needed to apply Theorem 1.2.

LEMMA 4.1. (i) *The conjugacy classes of* $\mathrm{Gal}(K/\mathbf{Q})$ *are* $\{e\}$, $\{\sigma\}$, *together with* $\{a\}$, $\{\sigma a\}$ *for elements* a *of order two in* A *and* $\{a, a^{-1}\}$, $\{\sigma a, \sigma a^{-1}\}$ *for elements* a *of order greater than two in* A.

(ii) *The divisions of* $\mathrm{Gal}(K/\mathbf{Q})$ *are* $\{e\}$, $\{\sigma\}$, *together with* $\{a\}$, $\{\sigma a\}$ *for elements* a *of order* 2 *in* A *and the sets*

$$\{a^j : (j, \mathrm{ord}\, a) = 1\}, \qquad \{\sigma a^j : (j, \mathrm{ord}\, a) = 1\},$$

for elements a *of order greater than two in* A.

Proof. The assertions of the lemma are easily verified by calculations using the representation (4.2), the presentation (4) and the fact that A is abelian. ■

LEMMA 4.2. *The primes* p *represented by the quadratic form* Q *of discriminant* D *with* $(p, D) = 1$ *are exactly those for which*

$$\left[\frac{K/\mathbf{Q}}{(p)}\right] = \{a, a^{-1}\}$$

where a *is that element of* $\mathrm{Gal}(K/\mathbf{Q}(\sqrt{d}))$ *corresponding to* $[\mathbf{Q}]$ *under the isomorphism*

$$\bar{i} \circ \psi : \mathrm{Cl}(D) \to \mathrm{Cl}_f(\mathbf{Q}(\sqrt{d})) \to \mathrm{Gal}(K/\mathbf{Q}(\sqrt{d})).$$

Proof. Let p be a prime represented by the form Q with $(p, D) = 1$. As remarked earlier, the class $\phi([Q])$ in $\mathrm{Cl}_f(\mathbf{Q}(\sqrt{d}))$ contains a prime ideal P of norm p. Set

$$a = \left[\frac{K/\mathbf{Q}(\sqrt{d})}{P}\right]$$

and note by property (2) above that $a = \bar{i} \circ \psi([Q])$. By the definition of the Artin symbol, for each prime $\tilde{P}$ of K lying over P,

$$x^a \equiv x^{NP} \pmod{\tilde{P}} \tag{4.3}$$

for all $x \in O_K$, where $NP = N_{Q(\sqrt{d})/Q}\, P = p$. But (4.3) shows that $a \in$

$\left[\frac{K/\mathbf{Q}}{(p)}\right]$. By Lemma 4.1 (i),

$$\left[\frac{K/\mathbf{Q}}{(p)}\right] = \{a, a^{-1}\}. \qquad \blacksquare$$

We now complete the proof of Theorem 1.5. By Lemma 4.1, for each $a \in \mathrm{Gal}(K/\mathbf{Q}(\sqrt{d}))$ we have

$$\{\text{the division containing } a\} = \{a, a^{-1}\}$$

if and only if $\phi(\text{ord } a) = 1$ or 2, where $\phi(\cdot)$ is Euler's totient function. This holds only if ord a = 1, 2, 3, 4, or 6. Since $\bar{i} \circ \psi$ is an isomorphism, this is true if and only if [Q] has order 1, 2, 3, 4 or 6 in the form class group Cl(D). ■

References

1. J. Ax, *Solving diophatine equations modulo every prime,* Ann. of Math., vol. 85 (1967), pp. 161–183.
2. B. J. Birch, "Cyclotomic fields and Kummer extensions" in *Algebraic Number Theory* (J. W. S. Cassels and A. Fröhlich, Eds.), Academic Press, N.Y., 1967, pp. 85–93.
3. G. Brückner, *Characterisierung der galoisschen Zahlkörper deren zerlegte Primzahlen durch binäre quadratische Formen gegeben sind,* Math. Nach., vol. 32 (1966), pp. 317–326.
4. N. Chebotarev, *Die Bestimmung der Dichtigkeit einer Merge von Primzahlen, welche zu einer gegebenen Substitutionenklasse gehören,* Math. Ann., vol. 95 (1926), pp. 191–228.
5. H. Cohn, *A classical invitation to algebraic numbers and class fields,* Springer-Verlag, New York, 1978.
6. H. Cohn and G. Cooke, *Parametric form of an eight class field,* Acta. Arith., vol. 30 (1976), pp. 61–71.
7. L. E. Dickson, *History of the theory of numbers,* Chelsea (Reprint 1966), New York, vol. III, pp. 2–5.
8. G. Frobenius, *Über Beziehungen zwischen den Primidealen eines algebraischen Körpers und den Substitutionen seiner Gruppe,* Jber. preuss. Akad. Wiss., 1896, pp. 689–703.
9. S. Gurak, *On the representation theory for full decomposable forms,* J. Number Theory, vol. 13 (1981), pp. 421–442.
10. H. Hasse, *Bericht über neuere Untersuchungen und Probleme aus der Theorie der algebraischen Zahlkörper,* Physica-Verlag, Würzberg, 1970.
11. S. Lang, *Algebraic number theory,* Addison-Wesley, Reading, Mass., 1970.
12. R. W. K. Odoni, *A proof by classical methods of a result of Ax on polynomial congruences modulo a prime,* Bull. Lond. Math. Soc., vol. 11 (1979), pp. 55–58.
13. H. M. Stark, *Values of L-functions at s = 1 I. L-functions for quadratic forms,* Advances in Math., vol. 7 (1971), pp. 301–343.
14. W. Weber, *Über Zahlgruppen in algebraischen Körpern,* Math. Ann., vol. 48 (1897), pp. 433–473; vol. 49 (1897), pp. 83–100; vol. 50 (1898), pp. 1–26.
15. A. Weil, *Two lectures on number theory, past and present,* Enseign. Math., vol. 20 (1974), pp. 87–110, esp. pp. 104–105.

Bell Laboratories
Murray Hill, New Jersey