Solution to a Problem of Lubelski and an Improvement of a Theorem of His

by

A. SCHINZEL

In memory of Salomon Lubelski

Summary. The paper consists of two parts, both related to problems of Lubelski, but unrelated otherwise. Theorem 1 enumerates for \( a = 1, 2 \) the finitely many positive integers \( D \) such that every odd positive integer \( L \) that divides \( x^2 + Dy^2 \) for \( (x, y) = 1 \) has the property that either \( L \) or \( 2^a L \) is properly represented by \( x^2 + Dy^2 \). Theorem 2 asserts the following property of finite extensions \( k \) of \( \mathbb{Q} \): if a polynomial \( f \in k[x] \) for almost all prime ideals \( p \) of \( k \) has modulo \( p \) at least \( v \) linear factors, counting multiplicities, then either \( f \) is divisible by a product of \( v + 1 \) factors from \( k[x] \setminus k \), or \( f \) is a product of \( v \) linear factors from \( k[x] \setminus k \).

S. Lubelski [4], [5] considered the following problem: given a non-negative integer \( a \), what positive integers \( D \) have the following property:

\( P_a \): every odd positive integer \( L \) that divides \( x^2 + Dy^2 \) for \( (x, y) = 1 \) has the property that either \( L \) or \( 2^a L \) is properly represented by \( x^2 + Dy^2 \).

For \( a = 0 \) or \( a \geq 3 \) Lubelski gave a definite answer (Satz VI in [5]). For \( a = 1 \) or 2 he only gave criteria (Satz II and III in [5], see Lemma 3 below) which enable one to check for any given \( D \) whether it has property \( P_a \), but from which it is not clear whether the number of suitable \( D \)’s is finite or not. We shall prove

**Theorem 1.** For \( a = 1 \) or 2 an integer \( D > 0 \) has property \( P_a \) if and only if \( D \in S_a \), where

\[
S_1 = \{1, 2, 3, 4, 5, 6, 7, 10, 13, 22, 37, 58\},
\]

\[
S_2 = \{1, 2, 3, 4, 7, 8, 11, 12, 16, 19, 28, 43, 67, 163\}.
\]

2010 Mathematics Subject Classification: Primary 11E16, 11R09.

Key words and phrases: binary quadratic form, polynomial modulo a prime ideal.
In another paper Lubelski proved the following (Satz IV in [7]): if a polynomial \( f \in \mathbb{Z}[x] \) for almost all primes \( p \) has modulo \( p \) at least \( v \) linear factors, then \( f \) is divisible by a product of \( v \) factors from \( \mathbb{Z}[x] \setminus \mathbb{Z} \). We shall improve and extend this theorem as follows.

**Theorem 2.** Let \( k \) be a finite extension of \( \mathbb{Q} \). If a polynomial \( f \in k[x] \) for almost all prime ideals \( p \) of \( k \) has modulo \( p \) at least \( v \) linear factors, counting multiplicities, then either \( f \) is divisible by a product of \( v + 1 \) factors from \( k[x] \setminus k \), or \( f \) is a product of \( v \) linear factors from \( k[x] \).

For \( v = 1 \) we obtain a result of Hasse [3].

The proof of Theorem 1 is based on five lemmas.

**Lemma 1 (Weber).** In every ideal class of a quadratic field there exists a prime ideal of degree one.

*Proof.* See [10, §165 and §166].

**Lemma 2 (Lubelski).** An integer \( D > 0 \) has property \( P_0 \) if and only if \( D \in \{1, 2, 3, 4, 7\} = S_1 \cap S_2 \).

*Proof.* See [5, Satz I].

**Lemma 3.** For \( a = 1 \) or \( 2 \) an integer \( D > 0 \), \( D \equiv \varepsilon \mod 2 \), \( \varepsilon = 0, 1 \), has property \( P_a \) if the least odd divisor \( Q > 1 \) of any number \( x^2 + Dy^2 \) for \( (x, y) = 1 \) satisfies

\[
Q = \frac{D + \varepsilon^2}{2^a}.
\]

The condition is also necessary for \( a = 1, \ D \neq 1, 2, 3, 4, 7 \) and \( a = 2, \ D \neq 1, 2, 3, 4, 7, 8, 16 \).

*Proof.* If (1) holds, then \( 2^aQ \) is properly represented by \( x^2 + Dy^2 \) and \( D \) has property \( P_a \) by Satz III of [5]. Conversely, if \( D \) has property \( P_a \) for \( a = 1, 2 \) then either \( Q \) or \( 2^aQ \) is properly represented by \( x^2 + Dy^2 \). By Satz II of [5] in the former case \( Q \leq 7 \), hence \( D \leq 2^a \cdot 7 \); in the latter case \( Q = \lfloor \frac{1+D}{2^a} \rfloor \).

The last equality is equivalent to (1), unless \( a = 2, \ D \equiv 2 - \varepsilon^2 \mod 4 \). However, then \( 2^aQ = x^2 + Dy^2 \) implies \( x \equiv y \mod 2 \). The remaining assertion for \( D \leq 28 \) can be checked case by case.

**Lemma 4 (Stark).** If \( -d \) is a fundamental discriminant and the number of ideal classes of \( \mathbb{Q}(\sqrt{-d}) \) is at most two, then \( d \in S \), where

\[
\]

*Proof.* See [9].
Lemma 5 (Oesterlé). If $-d$ is a fundamental discriminant and the number of ideal classes of $\mathbb{Q}(\sqrt{-d})$ is three, then $d \in T$, where

$$T = \{23, 31, 59, 83, 107, 139, 211, 293, 307, 331, 499, 547, 643, 883, 907\}.$$

Proof. See [7] for a proof that $d \leq 907$. The list is taken from [1, Tables 4 and 5].

Proof of Theorem 1. Sufficiency of the condition follows from Lemma 3. It also follows from that lemma that no $D \in S_{3-a} \setminus S_a$ ($a = 1$ or 2) has property $P_a$. It remains to show that if $D \notin S_1 \cup S_2$, then $D$ has neither property $P_1$ nor $P_2$. If $D = 2^a \notin S_1 \cup S_2$, then $D \geq 32$. On the other hand, $Q = 3$ for $\alpha$ odd and $Q = 5$ for $\alpha$ even. Since $5 < \left\lfloor \frac{1+32}{4} \right\rfloor$ it follows from Lemma 3 that $D$ has neither property $P_1$ nor $P_2$.

If $D \equiv 0 \mod 4$, $D \neq 2^a$, then $Q = D/4$ and, by Lemma 3, $D$ does not have property $P_1$. On the other hand, if $D$ has property $P_2$, then $D/4$ has property $P_0$ and, by Lemma 2, $D \in S_1 \cap S_2$.

If $D \not\equiv 0 \mod 4$, then taking in the definition of $P_a$ for $L$ the least odd prime factor of $D$ we infer that

$$(2) \quad D = L \text{ or } 2L,$$

hence the discriminant of the field $\mathbb{Q}(\sqrt{-D})$ equals $D$ for $D \equiv 3 \mod 4$ and $4D$ otherwise. Put $\omega = (1+\sqrt{-D})/2$ for $D \equiv 3 \mod 4$, $\omega = \sqrt{-D}$ otherwise. If $D \equiv 3 \mod 8$, then (2) remains prime in $\mathbb{Q}(\sqrt{-D})$. If $D \equiv 1, 2 \mod 4$, then by Dedekind’s theorem, $(2) = \mathfrak{p}^2$, where $\mathfrak{p}$ is a prime ideal of $\mathbb{Q}(\sqrt{-D})$. Finally, if $D \equiv 7 \mod 8$, then (2) = $\mathfrak{p} \mathfrak{p}'$, where $\mathfrak{p}'$ is conjugate to $\mathfrak{p}$.

If $D \notin S_1 \cup S_2$ and $D \not\equiv 0 \mod 4$, then either $d$ has an odd square factor $> 1$ or $D \in \{15, 35, 51, 91, 115, 123, 187, 267, 403, 427\}$ or $D \in T$ or disc $\mathbb{Q}(\sqrt{-D}) \notin S \cup T$. The first two cases are excluded by (2), in the third case we find either $D \leq 211$, $Q \leq 5 < (1+D)/4$, or $D \geq 293$, $Q \leq 13 < (1+D)/4$, so this case is excluded by Lemma 3. In the fourth case by Lemma 4 there are at least four ideal classes in $\mathbb{Q}(\sqrt{-D})$ and, by Lemma 1, there exists there a prime ideal $q$ equivalent neither to (1) nor to $p^a$ nor to $p^{a'}$. If $q$ is the norm of $q$, then $q = (q, b + c\omega)$, where $b, c \in \mathbb{Z}$ and $(b, c) = 1$. If $\omega = \sqrt{-D}$, then $q \mid b^2 + Dc^2$, while if $\omega = (1+\sqrt{-D})/2$, then $q \mid (2b + c)^2 + Dc^2$ for $c$ odd and $q \mid (b + c/2)^2 + D(c/2)^2$ for $c$ even, thus by $P_a$ for some integers $x, y$ we have either $q = N(x+y\sqrt{-D})$ or $2^{a}q = N(x+y\sqrt{-D})$. Since $q$ is prime, this gives either $(x+y\sqrt{-D}) = q$ or $q'$ or $p^aq$ or $p^aq'$ or $p^{a'}q$ or $p^{a'}q'$ or $a = 2$, $(x+y\sqrt{-D}) = (2)q$ or $(x+y\sqrt{-D}) = (2)q'$. In each case $q$ is equivalent to either (1) or $p^a$ or $p^{a'}$, contrary to the choice of $q$.

The problem considered by Lubelski in [6], where 2 is replaced by an odd prime $p$, can be solved by similar methods.
The proof of Theorem 2 is based on

**Lemma 6.** For a finite permutation group $G$ with the orbits $O_1, \ldots, O_l$, let $a_{i\sigma}$ be the number of letters of the orbit $O_i$ left invariant by a permutation $\sigma$ of $G$. Then for each $i \leq l$,

$$\sum_{\sigma \in G} a_{i\sigma} = |G|.$$

**Proof.** See [2, p. 190].

**Proof of Theorem 2.** Consider the polynomial

$$f(x) = c \prod_{i=1}^{l} f_i(x)^{e_i},$$

where $c \in k \setminus \{0\}$, $f_i$ are coprime polynomials irreducible over $k$, and $e_i$ are positive integers. Let $G$ be the Galois group of the polynomial $\prod_{i=1}^{l} f_i(x)$ over $k$. Then $G$ has $l$ orbits $O_1, \ldots, O_l$ consisting of the zeros of $f_1, \ldots, f_l$ respectively. By the Frobenius density theorem for every permutation $\sigma \in G$ there exist infinitely many prime ideals $p$ of $k$ such that $f_i$ has exactly $a_{i\sigma}$ linear factors modulo $p$, where $a_{i\sigma}$ is as in Lemma 6. The assumption gives

$$(3) \quad \sum_{i=1}^{l} e_i a_{i\sigma} \geq v \quad \text{for every } \sigma \in G$$

and unless

$$(4) \quad v \geq \sum_{i=1}^{l} e_i$$

we have the assertion. For $\sigma$ being the identity (id) we have $a_{i\sigma} = |O_i|$ ($1 \leq i \leq l$), hence by Lemma 6,

$$\sum_{\sigma \in G \setminus \{\text{id}\}} a_{i\sigma} = |G| - |O_i| \quad (1 \leq i \leq l).$$

It follows that

$$\sum_{\sigma \in G \setminus \{\text{id}\}} \sum_{i=1}^{l} e_i a_{i\sigma} = \sum_{i=1}^{l} e_i \sum_{\sigma \in G \setminus \{\text{id}\}} a_{i\sigma} = \sum_{i=1}^{l} e_i (|G| - |O_i|) < \sum_{i=1}^{l} e_i (|G| - 1),$$

unless

$$(5) \quad |O_i| = 1 \quad (1 \leq i \leq l).$$

Therefore, unless (5) holds, there exists $\sigma \in G$ such that $\sum_{i=1}^{l} e_i a_{i\sigma} < \sum_{i=1}^{l} e_i$, contrary to (3) and (4).
References


A. Schinzel
Institute of Mathematics
Polish Academy of Sciences
Śniadeckich 8
00-956 Warszawa, Poland
E-mail: schinzel@impan.pl

Received March 28, 2011