BULLETIN OF THE POLISH
ACADEMY OF SCIENCES
MATHEMATICS
Vol. 65, No. 1, 2017

NUMBER THEORY

An improvement of a lemma from Gauss's first proof of quadratic reciprocity

by

A. SCHINZEL and M. SKAŁBA

Summary. An upper estimate is given for the least prime q such that $(d/q) = 1$ and $(p/q) = -1$, where $d \neq 0$ is a given integer and p is a given prime satisfying $p \equiv 1 \pmod 8$ and $(d/p) = 1$.

In his proof (and the first proof altogether) of the quadratic reciprocity law Gauss applied the following statement:

(∗) *For every prime p of the form $8k+1$ there exists a prime $q < p$ satisfying*

$$\left(\frac{p}{q}\right) = -1. \tag{1}$$

For $p \equiv 1 \pmod 4$ and $q > 2$, (1) is equivalent to

$$\left(\frac{q}{p}\right) = -1, \tag{2}$$

and it is a well known problem to estimate the least prime q for which (2) holds. The best unconditional result is due to Burgess [1]:

$$q < p^{\frac{1}{4\sqrt{e}}+\varepsilon}$$

for every $\varepsilon > 0$ and $p > p_0(\varepsilon)$.

We shall improve, at least asymptotically, the statement (∗) by proving

THEOREM 1. *For every integer $d \neq 0$, every real number $\varepsilon > 0$ and every prime $p > p_0(d, \varepsilon)$ with $p \equiv 1 \pmod 8$ and $(d/p) = 1$ there exists a prime*

2010 *Mathematics Subject Classification*: Primary 11A15, 11L40.
Key words and phrases: quadratic residue, quadratic character.
Received 23 March 2017.
Published online 18 April 2017.

DOI: 10.4064/ba8109-4-2017

$q < p^{2/3+\varepsilon}$ *such that*

$$\left(\frac{d}{q}\right) = 1 \quad \text{and} \quad \left(\frac{p}{q}\right) = -1. \tag{3}$$

For $d = -1, 2$ and $\varepsilon = 1/3$ one can take $p_0(d, \varepsilon) = 0$.

The proof of the Theorem is based on three lemmas.

LEMMA 1. *Assume that* $p > 2$,

$$\left(\frac{d}{p}\right) = 1 \tag{4}$$

and $M > 0$. *The number of pairs* $(x, y) \in \mathbb{Z}^2 \cap (0, M]^2$ *such that*

$$x^2 - dy^2 \equiv 0 \pmod{p} \tag{5}$$

is $2M^2/p + O(M)$, *where the constant in the O-symbol is absolute.*

Proof. Since $d \equiv \delta^2$ and $\delta \not\equiv -\delta \pmod{p}$, (5) is equivalent to

$$x \equiv \pm\delta y \pmod{p}. \tag{6}$$

For every $y \in \mathbb{Z} \cap (0, M]$ there are $2M/p + O(1)$ integers $x \in (0, M]$ satisfying (6). Hence the lemma.

Let $\nu_q(d)$ be the exact exponent with which the prime q divides d.

LEMMA 2. *Let* $d \neq 0$ *be a cube free integer and let* $q_1, \dots, q_k$ *be all distinct prime divisors of* d *such that*

$$\left(\frac{q_i}{p}\right) = -1.$$

Let $e_i = \nu_{q_i}(d)$ $(1 \le i \le k)$ *and* S *be a subset of* $\{1, \dots, k\}$. *The number* $N(S)$ *of pairs* $(x, y) \in \mathbb{Z}^2 \cap (0, M]^2$ *such that*

$$x^2 - dy^2 \not\equiv 0 \pmod{p}, \qquad \nu_{q_i}(x^2 - dy^2) \equiv 1 \pmod{2} \quad (i \in S) \tag{7}$$

equals

$$M^2\left(1 - \frac{2}{p}\right)\prod_{i \in S} x_i + O(M)$$

for some $x_i < 1/2$, *where the constant in the O-symbol depends on* d.

Proof. All q_i are odd, because of the condition $p \equiv 1 \pmod{8}$. The condition (7) is equivalent to the conjunction of $x^2 - dy^2 \not\equiv 0 \pmod{p}$ and

$$\nu_{q_i}(x) > \nu_{q_i}(y) \quad \text{if } e_i = 1,$$

$$\nu_{q_i}(x) = 1 + \nu_{q_i}(y),\ \nu_{q_i}(x^2 q_i^{-2\nu_{q_i}(x)} - d q_i^{-2} y^2 q_i^{-2\nu_{q_i}(y)}) \equiv 1 \pmod{2} \ \text{ if } e_i = 2.$$

In order to get the estimate we set

$$x_i = \frac{1}{q_i+1} \qquad \text{if } e_i = 1,$$
$$x_i = \frac{2}{(q_i+1)^2} \qquad \text{if } e_i = 2,\ \left(\frac{dq_i^{-2}}{q_i}\right) = 1,$$
$$x_i = 0 \qquad \text{if } e_i = 2,\ \left(\frac{dq_i^{-2}}{q_i}\right) = -1,$$

and apply the Chinese Remainder Theorem together with Lemma 1. We only give the rationale for the formula on x_i in case $e_i = 2$, because it is more involved.

Let $x = q_i^{\nu_{q_i}(x)}\alpha$, $y = q_i^{\nu_{q_i}(y)}\beta$ and $q_i \nmid \alpha\beta$. Then the second of conditions (7) is equivalent to

$$\nu_{q_i}(x) = 1 + \nu_{q_i}(y) \quad \text{and} \quad \nu_{q_i}(\alpha^2 - d'\beta^2) \equiv 1 \pmod 2 \quad \text{where } d' = d/q_i^2.$$

Let $B = \mathbb{Z}^2 \cap (0, M]^2$, $B' = \{(\alpha,\beta) \in B \mid q_i \nmid \alpha\beta\}$. First if $(d'/q_i) = -1$, then

$$\{(x,y) \in B \mid \nu_{q_i}(x^2 - dy^2) \equiv 1 \pmod 2\} = \emptyset,$$

so we set $x_i = 0$. Secondly, if $(d'/q_i) = 1$, then

$$\operatorname{card} B' = \left(\frac{q_i - 1}{q_i}\right)^2 \operatorname{card} B + O(M),$$

and for any fixed $k \geq 1$,

$$\begin{aligned} b_k &:= \operatorname{card}\{(\alpha,\beta) \in B' \mid \nu_{q_i}(\alpha^2 - d'\beta^2) \geq k\} \\ &= \operatorname{card} B' \cdot \frac{2(q_i^k - q_i^{k-1})}{(q_i^k - q_i^{k-1})^2} + O(M). \end{aligned}$$

Hence

$$\begin{aligned} &\operatorname{card}\{(\alpha,\beta) \in B' \mid \nu_{q_i}(\alpha^2 - d'\beta^2) \equiv 1 \pmod 2\} = b_1 - b_2 + b_3 - \cdots \\ &= \frac{2}{q_i - 1}\left(1 - \frac{1}{q_i} + \frac{1}{q_i^2} - \cdots\right) \operatorname{card} B' + O(M) = \frac{2q_i}{q_i^2 - 1} \operatorname{card} B' + O(M), \end{aligned}$$

and finally

$$\begin{aligned} &\operatorname{card}\{(x,y) \in B \mid \nu_{q_i}(x^2 - dy^2) \equiv 1 \pmod 2\} \\ &\qquad = \left(\frac{1}{q_i} + \frac{1}{q_i^3} + \cdots\right) \frac{2q_i}{q_i^2 - 1} \left(\frac{q_i - 1}{q_i}\right)^2 \operatorname{cardB} + O(M) \\ &\qquad = \frac{2}{(q+1)^2} \operatorname{card} B + O(M), \end{aligned}$$

which justifies the definition of x_i in case $(d'/q_i) = 1$.

LEMMA 3. *Let $f(x,y) = x^2 + axy + by^2$ be an integral quadratic form reducible mod p, but not congruent mod p to a perfect square. Let χ be a non-principal character mod p and $B = \mathbb{Z}^2 \cap (0, M]^2$. For every $\varepsilon > 0$ there*

exists $\delta > 0$ such that

$$\sum_{(x,y)\in B} \chi(f(x,y)) = O(M^2 p^{-\delta}) \quad \text{for every } M > p^{1/3+\varepsilon}. \tag{8}$$

Proof. See Burgess [2].

Proof of the Theorem. Without loss of generality we can assume that for each prime q dividing d one has $\nu_q(d) \le 2$. In Lemma 3, set $f(x,y) = x^2 - dy^2$, $\chi = (\cdot/p)$, $M = p^{(1+\varepsilon)/3}$. By the condition $(d/p) = 1$ the assumptions of the lemma are satisfied. By the lemma, (8) holds for a certain $\delta > 0$. On the other hand, by Lemma 1, $\chi(x^2 - dy^2) = 0$ for at most $2M^2/p + O(M)$ terms of the sum over B. Let $q_1, \dots, q_k$ be all distinct prime divisors of d such that $(q_i/p) = -1$, and for $S \subset \{1, \dots, k\}$ let $N(S)$ be as in Lemma 2. Assuming that there is no prime $q < p^{2/3+\varepsilon}$ satisfying (3), the number of terms in the sum (8) in which $\chi(x^2 - dy^2) = -1$ is

$$M^2\left(1 - \frac{2}{p}\right) \sum_{\operatorname{card} S \text{ odd}} \prod_{i\in S} x_i \prod_{i\notin S}(1 - x_i) + O(M)$$
$$= M^2\left(1 - \frac{2}{p}\right)\left(\frac{1}{2} - \frac{1}{2}\prod_{i=1}^{k}(1 - 2x_i)\right) + O(M),$$

which can be justified as follows: for given l natural numbers $i_1 < \dots < i_l \le k$ we compare the coefficients of $x_{i_1} \cdots x_{i_l}$; on the left-hand side the relevant coefficient equals

$$M^2\left(1 - \frac{2}{p}\right)(-1)^{l-1} \sum_{j\equiv 1 \,(\mathrm{mod}\, 2)} \binom{l}{j} = M^2\left(1 - \frac{2}{p}\right)(-2)^{l-1},$$

and on the right-hand side the coefficient has the same value. Now we obtain

$$\sum_{(x,y)\in B} \chi(f(x,y)) = \operatorname{card} B - M^2\,\frac{2}{p} - O(M)$$
$$- M^2\left(1 - \frac{2}{p}\right)\left(1 - \prod_{i=1}^{k}(1 - 2x_i)\right) + O(M)$$
$$= M^2\left(1 - \frac{2}{p}\right)\prod_{i=1}^{k}(1 - 2x_i) + O(M),$$

which is not $O(M^2 p^{-\delta})$. The contradiction proves the existence of a prime q satisfying (3).

References

[1] D. A. Burgess, *The distribution of quadratic residues and non-residues*, Mathematika 4 (1957), 106–112.

[2] D. A. Burgess, *A note on character sums of binary quadratic forms*, J. London Math. Soc. 43 (1968), 271–274.

A. Schinzel
Institute of Mathematics
Polish Academy of Sciences
Śniadeckich 8
00-656 Warszawa, Poland
E-mail: schinzel@impan.pl

M. Skałba
Institute of Mathematics
University of Warsaw
Banacha 2
02-097 Warszawa, Poland
E-mail: skalba@mimuw.edu.pl