

QUADRATIC RESIDUES AND RELATED PROBLEMS

Bui Minh Phong (Ho Chi Minh City, Vietnam)

J.P. Jones (Calgary, Canada)

I. Introduction and basic properties

For each odd positive integer n we denote by $\left(\frac{x}{n}\right)$ the Jacobi symbol, that is

$$\left(\frac{x}{n}\right) = \prod_{p^e \parallel n} \left(\frac{x}{p}\right)^e \quad \text{if } (x, n) = 1$$

and $(x/n) = 0$ if $(x, n) > 1$, where (x/p) is the Legendre symbol. Recently, we proved in [1] that for every fixed relatively prime positive integer n and j there is a positive integer a such that

$$(1) \quad (a, n) = 1 \quad \text{and} \quad \left(\frac{a^2 - j^2}{n}\right) = -1$$

if and only if $(n, 3) = 1$ and n is not a square. Our purpose in this note is to consider a similar problem, when $a^2 - j^2$ is replaced by $P(a)$, where $P(x)$ is a polynomial with integer coefficients. We shall obtain a complete solution for the case when $P(x) = Ax^2 + Bx + C$.

Let

$$P(x) = A_0 + A_1x + \dots + A_mx^m \quad (m \geq 1)$$

be a polynomial of degree m with integer coefficients. We shall denote by $N(P)$ the set of all odd positive integers n for which $(P(c), n) = 1$ holds for some integer c . For a positive integer n let

$$n = p_1^{\alpha_1} \dots p_s^{\alpha_s}$$

be the canonical representation of n as the product of prime-powers. It is obvious that

$$n \in N(P) \quad \text{if and only if} \quad p_1 \in N(P), \dots, p_s \in N(P),$$

moreover for a prime q we have

$$q \notin \mathbf{N}(P) \quad \text{if and only if} \quad P(x) = (x^q - x)P'(x) + qR(x),$$

where $P'(x)$, $R(x)$ are polynomials with integer coefficients and $\deg R(x) \leq q - 1$. Let w be an integer whose possible values are ± 1 . Let $G_w = G_w(P)$ denote the set of all $n \in \mathbf{N}(P)$ for which there is a positive integer a such that

$$(2) \quad (P(a), n) = 1 \quad \text{and} \quad \left(\frac{P(a)}{n} \right) = w.$$

Let

$$G(P) = G_1(P) \cap G_{-1}(P) \quad \text{and} \quad G_w^*(P) = G_w(P) \setminus G(P).$$

For each positive integer n let $k(n)$ denote the square free kernel of n . Then n can be represented in the form $n = k(n) \cdot m^2$, where $k(n)$ is square free and m is an integer.

Lemma 1. *Let $P(x)$ be a polynomial with integer coefficients and let $n \in \mathbf{N}(P)$. Then*

$$n \in G_w(P) \quad \text{if and only if} \quad k(n) \in G_w(P).$$

Proof. It is obvious that $n \in G_w(P)$ implies that $k(n) \in G_w(P)$.

Assume that for a positive integer $n \in \mathbf{N}(P)$ we have

$$(3) \quad k(n) \in G_w(P).$$

We can write n in the form $n = kM^2N^2$, where $k = k(n)$, $(k, M) = 1$ and k, N have the same prime divisors. From (3) one can deduce that there exists a positive integer b such that

$$(4) \quad (P(b), k) = 1 \quad \text{and} \quad \left(\frac{P(b)}{k} \right) = w.$$

Since $n \in \mathbf{N}(P)$ and $n = kM^2N^2$, we have $M \in \mathbf{N}(P)$. Thus there is an integer c such that

$$(5) \quad (P(c), M) = 1.$$

Let c be an integer which satisfies (5). Since $(k, M) = 1$, there is a positive integer h such that

$$(6) \quad kh + b \equiv c \pmod{M^2}.$$

Let $a := kh + b$. By using (4) – (6), we have

$$(P(a), n) = (P(kh + b), kM^2N^2) = 1$$

and

$$\left(\frac{P(a)}{n}\right) = \left(\frac{P(kh + b)}{k}\right) \left(\frac{P(a)}{M^2}\right) \left(\frac{P(a)}{N^2}\right) = \left(\frac{P(b)}{k}\right) = w.$$

These imply that $n \in G_w(P)$. The proof of Lemma 1 is completed.

Lemma 2. *Let $P(x)$ be a polynomial with integer coefficients and let $nm \in N(P)$. Assume that $w, w' \in \{1, -1\}$. If*

$$k(n) \in G_w(P), \quad k(m) \in G_{w'}(P) \quad \text{and} \quad (k(n), k(m)) = 1,$$

then $nm \in G_{ww'}(P)$.

Proof. In order to prove Lemma 2 by using Lemma 1 it suffices to show that $k(nm) \in G_{ww'}(P)$. First we note that from our assumptions $k(n) \in G_w(P)$ and $k(m) \in G_{w'}(P)$, there are positive integers u and v such that

$$(P(u), k(n)) = 1 \quad \text{and} \quad \left(\frac{P(u)}{k(n)}\right) = w$$

and

$$(P(v), k(m)) = 1 \quad \text{and} \quad \left(\frac{P(v)}{k(m)}\right) = w'.$$

By using $(k(n), k(m)) = 1$, we can choose a positive integer t such that

$$k(n)t + u \equiv v \pmod{k(m)}.$$

Let $a := k(n)t + u$. Then

$$P(a) \equiv P(u) \pmod{k(n)} \quad \text{and} \quad P(a) \equiv P(v) \pmod{k(m)}.$$

These imply

$$(7) \quad (P(a), k(nm)) = (P(a), k(n)k(m)) = 1$$

and

$$(8) \quad \left(\frac{P(a)}{k(nm)}\right) = \left(\frac{P(a)}{k(n)}\right) \left(\frac{P(a)}{k(m)}\right) = \left(\frac{P(u)}{k(n)}\right) \left(\frac{P(v)}{k(m)}\right) = ww'.$$

Thus, (7) and (8) show that $k(nm) \in G_{ww'}(P)$. This completes the proof of Lemma 2.

Lemma 3. *Let $P(x)$ be a polynomial with integer coefficients and let p be a prime for which $p \in \mathbf{N}(P)$. Then*

$$p \in G_1(P) \cup G_{-1}(P).$$

Proof. From the condition $p \in \mathbf{N}(P)$ it follows that there is a positive integer c such that $(P(c), p) = 1$. Thus, we have either

$$\left(\frac{P(c)}{p}\right) = 1 \quad \text{or} \quad \left(\frac{P(c)}{p}\right) = -1,$$

from which $p \in G_1(P) \cup G_{-1}(P)$ follows.

By using Lemma 3, we see that every positive integer $n > 1$ with condition $n \in \mathbf{N}(P)$ can be represented in the form

$$(9) \quad n = n_1 n_G n_{-1},$$

where every prime divisor p of n_1 (resp. n_{-1}) satisfies $p \in G_1^*(P)$ (resp. $G_{-1}^*(P)$) and every prime divisor q of n_G satisfies $q \in G(P)$. Hence $G_w^*(P) = G_w(P) \setminus G(P)$ and $G(P) = G_1(P) \cap G_{-1}(P)$. It is obvious that

$$(10) \quad (n_1, n_G) = (n_1, n_{-1}) = (n_G, n_{-1}) = 1.$$

Theorem 1. *Let $P(x)$ be a polynomial with integer coefficients. Let $n > 1$ be an integer for which $n \in \mathbf{N}(P)$ and let $n = n_1 n_G n_{-1}$ be the representation of n in the form (9). Then we have*

- (I) $n \in G(P)$ if $k(n_G) > 1$
- (II) $n \in G_w(P)$ if $k(n_{-1}) \in G_w(P)$.

Proof. We first note by (10) that

$$k(n) = k(n_1)k(n_G)k(n_{-1}).$$

(I) Assume that $k(n_G) > 1$. Then by Lemma 2 it is easily seen that

$$k(n_G) \in G(P) \quad \text{and} \quad k(n) \in G(P).$$

Thus, by Lemma 1, we have $n \in G(P)$.

(II) Assume that $k(n_G) = 1$. Then $k(n) = k(n_1)k(n_{-1})$, and so by Lemma 2

$$k(n_1) \in G_1(P)$$

and

$$k(n) \in G_w(P) \quad \text{if} \quad k(n_{-1}) \in G_w(P)$$

follow. From Lemma 1 the proof of Theorem 1 is finished.

II. Applications to the polynomial $P(x) = Ax^2 + Bx + C$

We shall apply Theorem 1 to get a complete solution for the case when $P(x) = Ax^2 + Bx + C$. First we prove

Lemma 4. *Let $P(x) = Ax^2 + Bx + C$ be a polynomial of degree 2 with integer coefficients and let $\Delta = B^2 - 4AC$. Let p be an odd prime for which $(p, A, B, C) = 1$. Then we have $p \in G(P)$, except the following cases:*

- (a) $p | (A, B)$,
- (b) $p | \Delta$ and $A \not\equiv 0 \pmod{p}$,
- (c) $p = 3$ if $A\Delta \not\equiv 0 \pmod{3}$ and $(\Delta/3) = 1$.

If p satisfies (a), (b) and (c) respectively, then

$$p \in G_{(C/p)}^*(P), \quad p \in G_{(A/p)}^*(P) \quad \text{and} \quad p = 3 \in G_{-(A/3)}^*(P),$$

respectively.

Proof. Let p be an odd prime for which $(p, A, B, C) = 1$.

By using

$$P(x) = Ax^2 + Bx + C$$

and

$$(11) \quad 4AP(x) = (2Ax + B)^2 - \Delta,$$

it is easily seen that

$$\begin{aligned} p &\in G_{(C/p)}^*(P) \quad \text{if} \quad p | (A, B), \\ p &\in G_{(A/p)}^*(P) \quad \text{if} \quad p | \Delta \quad \text{and} \quad A \not\equiv 0 \pmod{p}, \\ p = 3 &\in G_{-(A/3)}^*(P) \quad \text{if} \quad A\Delta \not\equiv 0 \pmod{3} \quad \text{and} \quad (\Delta/3) = 1. \end{aligned}$$

Assume now that (a), (b) and (c) are not satisfied.

If $A \equiv 0 \pmod{p}$, then $B \not\equiv 0 \pmod{p}$ and $P(x) \equiv Bx + C \pmod{p}$. In this case one can deduce that $p \in G(P)$, because $p > 2$.

Assume that $A \not\equiv 0 \pmod{p}$. Then $\Delta \not\equiv 0 \pmod{p}$.

If $\left(\frac{\Delta}{p}\right) = 1$, then $p > 3$ and $\Delta \equiv j^2 \pmod{p}$ for some positive integer j with $(p, j) = 1$. Thus, from a result of [1] mentioned above and using (11), we have $p \in G_{-(A/p)}(P)$. On the other hand, since $p > 3$, there is a positive integer h such that

$$(12) \quad (h(h+1), p) = 1 \quad \text{and} \quad \left(\frac{h(h+1)}{p}\right) = 1.$$

Indeed, we can choose h as follows: $h = 1$ if $(2/p) = 1$; $h = 2$ if $(2/p) = (3/p) = -1$ and $h = 3$ if $(3/p) = 1$. Let d be a positive integer such that

$$2Ad + B \equiv j(2h+1) \pmod{p}.$$

Then from (11) we have

$$4AP(d) \equiv (2Ad + B)^2 - \Delta \equiv 4j^2h(h+1) \pmod{p},$$

which with (12) implies that $p \in G_{(A/p)}(P)$. Thus, from $p \in G_{-(A/p)}(P)$ and $p \in G_{(A/p)}(P)$ it follows that $p \in G(P)$.

Finally, let $A \not\equiv 0 \pmod{p}$ and $\left(\frac{\Delta}{p}\right) = -1$. Then it is easily seen that the following $(p+1)/2$ numbers

$$-\Delta, 1^2 - \Delta, \dots, [(p-1)/2]^2 - \Delta$$

are incongruent $\pmod{p}$ and $\not\equiv 0 \pmod{p}$. Thus, there are integers y_1, y_2 such that

$$(13) \quad (y_i^2 - \Delta, p) = 1 \quad \text{and} \quad \left(\frac{y_i^2 - \Delta}{p}\right) = (-1)^i \quad (i = 1, 2).$$

Let x_i ($i = 1, 2$) be such integers which satisfy

$$2Ax_i + B \equiv y_i \pmod{p}.$$

Then

$$4AP(x_i) = (2Ax_i + B)^2 - \Delta \equiv y_i^2 - \Delta \pmod{p},$$

and so by (13) we have $p \in G(P)$.

The proof of Lemma 4 is finished.

Let $\mathcal{B}(P)$ denote the set of all odd primes p which satisfy one of the conditions (a), (b) and (c), i.e.

- (a) $p|(A, B)$,
- (b) $p|\Delta$ and $A \not\equiv 0 \pmod{p}$,
- (c) $p=3$ if $A\Delta \not\equiv 0 \pmod{3}$ and $(\Delta/3) = 1$.

By using Lemma 4, we can define a function $t : \mathcal{B}(P) \rightarrow \{1, -1\}$ by the relation

$$t(p) = \begin{cases} 1 & \text{if } p \in G_1^*(P) \\ -1 & \text{if } p \in G_{-1}^*(P) \end{cases} \quad (p \in \mathcal{B}(P)).$$

From Theorem 1 and Lemma 4 we have

Theorem 2. *Let $P(x) = Ax^2 + Bx + C$ be a polynomial of degree 2 with integer coefficients and let $\Delta = B^2 - 4AC$. Let n be an odd positive integer with $(n, A, B, C) = 1$. Then*

- (i) *if there is a prime $q \notin \mathcal{B}(P)$ such that $q|k(n)$, then $n \in G(P)$;*
- (ii) *if $k(n) = p_1 \dots p_s$ with $p_1, \dots, p_s \in \mathcal{B}(P)$, then*

$$n \in G_{t(p_1) \dots t(p_s)}^*(P).$$

Reference

- [1] **Jones J.P. and Phong B.M.**, Some results on quadratic residues and the differences of two squares, manuscript.

(Received December 2, 1991)

B.M. Phong
 Computer Center
 Eötvös Loránd University
 XI. Bogdánfy u. 10/B
 H-1117 Budapest, Hungary

J.P. Jones
 The University of Calgary
 Calgary, Alberta, T2N 1N4
 Canada

