ROCKY MOUNTAIN
JOURNAL OF MATHEMATICS
Volume 36, Number 6, 2006

QUADRATIC RESIDUES OF CERTAIN TYPES

ALEXANDRU GICA

ABSTRACT. The main purpose of the paper is to show that if p is a prime different from $2, 3, 5, 7, 13, 37$, then there exists a prime number q smaller than p, $q \equiv 1 \pmod 4$, which is a quadratic residue modulo p. Also, it is shown that if p is a prime number which is not $2, 3, 5, 7, 17$, then there exists a prime number $q \equiv 3 \pmod 4$, $q < p$, which is a quadratic residue modulo p.

1. Introduction. In [**2**] it is shown that any $n \in \mathbf{N}$, $n > 3$, could be written as

$$n = a + b,$$

a, b being positive integers such that $\Omega(ab)$ is an even number. If $m \in \mathbf{N}$, $m \geq 2$, has the standard decomposition $m = p_1^{a_1} \cdot p_2^{a_2} \cdots p_r^{a_r}$ then the *length* of m is $\Omega(m) = \sum_{i=1}^{n} a_i$. We put $\Omega(1) = 0$. In connection with the above quoted result, the following open problem naturally arises.

Open problem. *What numbers n can be written as $n = a^2 + b$, where a, b are positive integers, the length of b being an even number?*

Trying to solve this problem was the starting point for the main result of this paper.

Theorem 1. *Let p be a prime number $p \neq 2, 3, 5, 7, 13, 37$. There exists a prime number q such that $q < p$, $q \equiv 1 \pmod 4$ and $(q/p) = 1$.*

We will prove also a similar result which has, however, an elementary proof:

2000 AMS *Mathematics Subject Classification.* Primary 11A15, 11E25, 11R29.
Key words and phrases. Quadratic residue, length, numerus idoneus.
Received by the editors on March 22, 2004, and in revised form on April 9, 2004.

Copyright ©2006 Rocky Mountain Mathematics Consortium

Theorem 2. *If p is a prime not equal to $2, 3, 5, 7, 17$, then there exists a quadratic residue modulo p, where $q < p$ and $q \equiv 3 \pmod 4$.*

We have to mention that finding the properties of $n'(p)$, the least prime number which is quadratic residue modulo a prime p, is a classical problem. We quote here [**6**] where it is shown that

$$n'(p) = O(p^{\alpha}),$$

where α is a fixed real number for which $\alpha > 1/4e^{-1/2}$.

2. The elementary cases. We will use below the following obvious

Lemma. *If x and y are positive integers, $x \neq y$, then $x^2 + y^2$ has a prime factor $q = 4k + 1, k \in \mathbf{N}$.*

We will prove now the main statement of the paper

Theorem 1. *Let p be a prime number not equal to $2, 3, 5, 7, 13, 37$. Then there exists a prime number q such that $q < p$, $q \equiv 1 \pmod 4$ and $(q/p) = 1$.*

We divide the proof of the theorem in several cases, depending on the class of p modulo 8. In this section we will treat the cases which have elementary proofs.

1. $p \equiv 1, 3 \pmod 8$, $p > 3$**.** In this case $p = x^2 + 2y^2$, where x and y are positive integers, $x \neq y$ (since $p > 3$). According to the lemma, there exists a prime divisor $q \equiv 1 \pmod 4$ of the number $x^2 + y^2$. We have that $p \equiv y^2 \pmod q$ and therefore $(q/p) = (p/q) = \left(y^2/q\right) = 1$. Since obviously $q < p$, the statement is true in this case.

2. $p \equiv 7 \pmod 8$, $p > 7$**.** We divide this case in two subcases, according to the class of p modulo 3.

2a. $p \equiv 1 \pmod 3$**.** In this situation we know that $p = x^2 + 3y^2$, x and y being positive integers. It is obvious that $(x, y) = 1$, y is odd and $x = 2t$, where t is an odd number. Since $p > 7$, we have $y \neq t$, and according to the lemma there is a prime $q \equiv 1$

(mod 4) which divides $t^2 + y^2$. We infer that $p \equiv -y^2 \pmod q$ and $(q/p) = (p/q) = \big(-y^2/q\big) = (-1/q) = 1$.

2b. $p \equiv 2 \pmod 3$**.** In this case $(3/p) = 1$ and there exists $m \in \mathbf{Z}$ such that $m^2 \equiv 3 \pmod p$. The element p is not prime in the norm Euclidean ring $\mathbf{Z}[\sqrt{3}]$ since $p \mid m^2 - 3 = (m - \sqrt{3})(m + \sqrt{3})$ but p does not divide $m \pm \sqrt{3}$. Therefore $p = \alpha\beta$, with $\alpha, \beta \in \mathbf{Z}[\sqrt{3}]$, not units. If $\alpha = x + y\sqrt{3}$, $x, y \in \mathbf{Z}$, one gets that $x^2 - 3y^2 = \pm p$. Since $p \equiv 2 \pmod 3$, one obtains that $x^2 - 3y^2 = -p$. Considering the positive integers x, y such that $x^2 - 3y^2 = -p$ with x minimal and tacking into account that $(|2x - 3y|, |2y - x|)$ is also a solution of the above equation (we multiplied $x - y\sqrt{3}$ with $2 + \sqrt{3}$, the fundamental unit of $\mathbf{Z}[\sqrt{3}]$), we immediately get that $|2x - 3y| \geq x$. If $2x - 3y \geq x$ one gets $x \geq 3y$, while $-p = x^2 - 3y^2 \geq 6y^2$ gives a contradiction. So it must be the case that $3y - 2x \geq x$ and $y \geq x$. Therefore $-p = x^2 - 3y^2 \leq -2y^2$, $y^2 \leq p/2$ and further $x^2 = 3y^2 - p \leq (3p/2) - p = p/2$. The fact that the last two inequalities are strict follows since p is odd. Therefore x, y are positive integers such that $x^2 - 3y^2 = -p$ and $x^2 < p/2$, $y^2 < p/2$. Since $x \neq y$, then, according to the lemma, there exists a prime $q \equiv 1 \pmod 4$ such that q divides $x^2 + y^2$. Obviously, $q \leq x^2 + y^2 < p/2 + p/2 = p$ and $p \equiv (2y)^2 \pmod q$. We proved Theorem 1 in this case.

3. The difficult case. We will solve in this section the case $p \equiv 5 \pmod 8$, $p > 37$. In [**4**] Schinzel shows that a positive integer n could be written as $n = x^2 + y^2 + z^2$, where x, y, z are positive integers such that $(x, y, z) = 1$ if and only if

i) $n \not\equiv 0, 4, 7 \pmod 8$ and

ii) n is divisible by a prime $\equiv 3 \pmod 4$ or is not a "numerus idoneus."

Euler called a number n "*numerus idoneus*" (convenient number) if it satisfies the following criterion:

Let m be an odd number such that $m = x^2 + ny^2, x, y \in \mathbf{Z}$, $(x, y) = 1$. If the equation $m = x^2 + ny^2$ has only one solution with $x \geq 0, y \geq 0$, then m is a prime number.

Gauss gave a list of 65 numbers n with this property and Weinberger [**7**] showed that besides these values, there exists at most one convenient number.

We apply Schinzel's result to $n = p$. The only possibility for p to not be written as $p = x^2 + y^2 + z^2$, with x, y, z positive integers, is to be a "numerus idoneus." Since $p \equiv 1 \pmod 4$ is prime and "numerus idoneus," we then infer that the ideal class group of the field $\mathbf{Q}(\sqrt{-p})$ has 2^r elements, where r is the number of odd prime divisors of p, see [**1**, Theorem 3.22, Proposition 3.11] for a proof of these results. We have $r = 1$ and therefore the ideal class group of the field $\mathbf{Q}(\sqrt{-p})$ has two elements. The list of the quadratic imaginary fields of discriminant d for which $h(d) = 2$ is given in [**3, 5**]. The list of the numbers d is the following:

$$-d = 15,20,24,35,40,51,52,88,91,115,123,148,187,232,235,267, 403,427.$$

We observe that in our case $d = -4p$, where $p \equiv 5 \pmod 8$ is a prime number. The only values of p which fit in the above list are $p = 5$, $p = 13$, $p = 37$ (corresponding to $d = -4p = -20, -52, -148$). But $p > 37$ and we arrive at a contradiction. Therefore, there exist the positive integers x, y, z such that $p = x^2 + y^2 + z^2$. Two of the above three numbers are different; let us suppose that $x \neq y$.

Applying the lemma we obtain that there exists a prime divisor $q \equiv 1 \pmod 4$ of the number $x^2 + y^2$. The prime number q has the desired properties since $q < p$, $q \equiv 1 \pmod 4$, $(q/p) = 1$.

4. A final remark. We give now a similar result to Theorem 1 but with an elementary proof.

Theorem 2. *If p is a prime not equal to $2, 3, 5, 7, 17$, then there exists a quadratic residue modulo p, where $q < p$ and $q \equiv 3 \pmod 4$.*

We divide the proof again into four cases.

1. $p \equiv 3 \pmod 8$, $p > 3$**.** We have $(p+9)/4 < p$ and $(p+1)/4 \geq 3$. One of the consecutive odd numbers $(p+1)/4$ and $(p+9)/4$ has the form $4h + 3 \geq 3$ and has therefore a prime divisor q, $q \equiv 3 \pmod 4$. We have that $q \leq (p+9)/4 < p$, $p \equiv -1 \pmod q$ or $p \equiv -9 \pmod q$. In both cases we have $(q/p) = -(p/q) = -(-1) = 1$.

2. $p \equiv 5 \pmod 8$, $p > 5$**.** The proof follows as above considering the numbers $(p-1)/4$ and $(p-9)/4$.

3. $p \equiv 7 \pmod 8$, $p > 7$. Let us consider the numbers $a = (p+1)/8$, $a+1 = (p+9)/8$, $a+3 = (p+25)/8$, $a+6 = (p+49)/8 < p$. These four positive integers represent all the classes modulo 4 and therefore one of these numbers has a prime divisor $q \equiv 3 \pmod 4$. We have $p \equiv -1 \pmod q$ or $p \equiv -9 \pmod q$ or $p \equiv -25 \pmod q$ or $p \equiv -49 \pmod q$. In all four cases we have $(p/q) = -1$ and $(q/p) = -(p/q) = -(-1) = 1$.

4. $p \equiv 1 \pmod 8$, $p > 17$. Since $(23/41) = (41/23) = (18/23) = (2/23) = 1$, we can suppose that $p \geq 73$. The proof follows now as in the previous case considering the numbers $(p-1)/8$, $(p-9)/8$, $(p-25)/8$, $(p-49)/8 > 0$.

Acknowledgment. I thank the anonymous referee for his hints which helped me improve the exposition of the paper.

REFERENCES

1. D.A. Cox, *Primes of the form x^2+ny^2: Fermat, classified theory and complex multiplication*, John Wiley & Sons, New York, 1989.

2. A. Gica, *The proof of a conjecture of additive number theory*, J. Number Theory **94** (2002), 80–89.

3. H.L. Montgomery and P.J. Weinberger, *Notes on small class numbers*, Acta Arith. **24** (1973/74), 529–542.

4. A. Schinzel, *Sur les sommes de trois carrés*, Bull. Acad. Polon. Sci. Ser. Sci. Math. Astr. Phys. **7** (1959), 307–309.

5. H.M. Stark, *On complex quadratic fields with class-number two*, Math. Comp. **29** (1975), 289–302.

6. A.I. Vinogradov and Y.V. Linnik, *Hypoelliptical curves and the least prime quadratic residue*, Dokl. Akad. Nauk SSSR **168** (1966), 259–261.

7. P.J. Weinberger, *Exponents of the class groups of complex quadratic fields*, Acta Arith. **22** (1973), 117–124.

Department of Mathematics, University of Bucharest, Str. Academiei 14, RO-010014 Bucharest 1, Romania
E-mail address: alex@al.math.unibuc.ro