Bull. Korean Math. Soc. **45** (2008), No. 2, pp. 273–275

AN ELEMENTARY PROOF IN THE THEORY OF QUADRATIC RESIDUES

Winfried Kohnen

Reprinted from the
Bulletin of the Korean Mathematical Society
Vol. 45, No. 2, May 2008

Bull. Korean Math. Soc. **45** (2008), No. 2, pp. 273–275

AN ELEMENTARY PROOF IN THE THEORY OF QUADRATIC RESIDUES

Winfried Kohnen

Abstract. We will give a short and elementary proof of the existence of infinitely many primes p such that a given positive integer a congruent 3 modulo 4 is a quadratic non-residue modulo p.

Let p be an odd prime and let a be an integer with $(a,p)=1$. Recall that the quadratic residue symbol $(\frac{a}{p})$ is defined to be 1 or -1 according as the congruence $x^2 \equiv a \pmod{p}$ is solvable or not.

It is not difficult to see that for a given a there exist infinitely many primes p such that $(\frac{a}{p}) = 1$. Indeed, it is rather straightforward to prove that if $f(X) \in \mathbf{Z}[X]$ is *any* polynomial with integral coefficients of positive degree, then there exist infinitely many primes p and positive integers n such that $p|f(n)$ [2, chap. II, sect. 1, Satz 1.2]. Note that the analytic proof of Dirichlet's theorem on primes in arithmetic progressions in fact shows that if a is not a perfect square, then the number of p such that $(\frac{a}{p}) = 1$ has density $\frac{1}{2}$ [3, part II, chap. VI, sect. 4, Propos. 14].

If a is not a perfect square, then there exist infinitely many primes p with $(\frac{a}{p}) = -1$ as well, but the proof is more difficult and uses deeper tools.

For example, one can proceed as follows. Say $a > 0$ and write $a = a_0^2 p_1 \cdots p_r$ with $p_1, \ldots, p_r$ different primes. Assume first that all the p_ν $(\nu = 1, \ldots, r)$ are odd. If $p \equiv 1 \pmod{4}$, we have

$$(\frac{a}{p}) = (\frac{p}{a}) = (\frac{p_1}{a}) \cdots (\frac{p_r}{a})$$

("Jacobi symbols") by quadratic reciprocity. Now by Dirichlet's prime number theorem, in conjunction with the Chinese remainder theorem, we can find infinitely many primes p such that

$$p \equiv 1 \pmod{4}, \;\; p \equiv 1 \pmod{p_\nu} \, (\nu = 1, \ldots, r-1), \;\; p \equiv \alpha_0 \pmod{p_r},$$

where α_0 is a fixed quadratic non-residue modulo p_r. For those p we then have $(\frac{a}{p}) = -1$.

Received March 4, 2007.
2000 *Mathematics Subject Classification.* 11A07, 11A041.
Key words and phrases. prime, quadratic residue.

If p_1 is even and $r \geq 2$ we take $p \equiv 1 \pmod 8$ and proceed in a similar way observing that $(\frac{2}{p}) = 1$. If $a = 2a_0^2$ we let $p \equiv 5 \pmod 8$ and note that

$$(\frac{a}{p}) = (\frac{2}{p}) = -1$$

for such p. If $a < 0$ one can proceed in a an analogous manner.

It is easy to see that with a similar reasoning as above one can also produce infinitely many primes $p \equiv 3 \pmod 4$ satisfying $(\frac{a}{p}) = -1$.

The purpose of this note is to give a very short and elementary proof of the existence of infinitely many primes p with $(\frac{a}{p}) = -1$ if $a > 0$, $a \equiv 3 \pmod 4$. This proof is modeled on Euclid's classical proof for the existence of infinitely many primes and as it seems has not yet been given in the literature.

Note that basically we give an elementary proof of the existence of infinitely many primes which do not split completely in $\mathbf{Q}(\sqrt{a})$. Similar ideas in a more general context can be found in [1].

Theorem. *Let a be a positive integer with $a \equiv 3 \pmod 4$. Then there exist infinitely many primes $p \equiv 3 \pmod 4$ with $(\frac{a}{p}) = -1$.*

Proof. For $x \in \mathbf{R}$, $x \geq 2$ let

$$m := \Big(\prod_{q \leq x, a \not\equiv 0 \pmod q} q \Big)^2 + a, \tag{1}$$

where in (1) the product extends over all primes $q \leq x$ that do not divide a. Then $m > 1$ and $m \equiv 3 \pmod 4$. Let p be a prime dividing m with $p \equiv 3 \pmod 4$. Then necessarily, by definition of m, we must have $p > x$.

On the other hand, we find from (1) that

$$-a \equiv \Big(\prod_{q \leq x, a \not\equiv 0 \pmod q} q \Big)^2 \pmod p. \tag{2}$$

In (2) we take $\frac{p-1}{2}$-powers. Taking into account Euler's criterion

$$a^{\frac{p-1}{2}} \equiv (\frac{a}{p}) \pmod p$$

and Fermat's Little Theorem, we deduce that

$$(\frac{a}{p}) \equiv (-1)^{\frac{p-1}{2}} \equiv -1 \pmod p,$$

where in the last congruence we have used that $p \equiv 3 \pmod 4$.

This proves the assertion. □

References

[1] M. Ram Murty and N. Thain, *Primes in certain arithmetic progressions*, Preprint 2007.
[2] W. Schwarz, *Einführung in Methoden und Ergebnisse der Primzahltheorie*, Bibliographisches Institut, Mannheim-Vienna-Zurich, 1969.
[3] J.-P. Serre, *A Course in Arithmetic*, Translated from the French. Graduate Texts in Mathematics, No. 7. Springer-Verlag, New York-Heidelberg, 1973.

Mathematisches Institut der Universität
INF 288, D-69120 Heidelberg, Germany
E-mail address: winfried@mathi.uni-heidelberg.de