COLLOQUIUM MATHEMATICUM

VOL. 100 2004 NO. 1

ON THE NUMBER OF NONQUADRATIC RESIDUES WHICH ARE NOT PRIMITIVE ROOTS

BY

FLORIAN LUCA (Morelia) and P. G. WALSH (Ottawa)

Abstract. We show that there exist infinitely many positive integers r not of the form $(p-1)/2-\phi(p-1)$, thus providing an affirmative answer to a question of Neville Robbins.

For every positive integer n let $\phi(n)$ be the Euler function of n. For an odd prime number p put $f(p)=(p-1)/2-\phi(p-1)$. Note that $f(p)$ counts the number of quadratic nonresidues modulo p which are not primitive roots. At the 2002 Western Number Theory Conference in San Francisco Neville Robbins asked if there exist infinitely many positive integers r such that $f(p)=r$ has no solution. In this note, we show that the answer to this question is affirmative. Throughout, we use p and q for prime numbers. A related question from [3] regarding whether or not there exist infinitely many positive integers m not in the range of the function $n-\phi(n)$ has been treated in [1] and [2].

Theorem 1. *For every odd integer $w>1$ there exist infinitely many positive integers $r=2^\gamma w$ not represented by the function $f(p)=(p-1)/2-\phi(p-1)$ with an odd prime number p.*

Proof. We let $r=2^\gamma w$. We shall show that there exist infinitely many values of γ such that r is not of the form $f(p)$ for some prime p. Let us assume that $f(p)=r$. Write $p-1=2^\alpha m$ with some positive integers α and m where m is odd. Then $f(p)=2^{\alpha-1}(m-\phi(m))$, and we are led to the equation $m-\phi(m)=2^{\gamma-(\alpha-1)}w$. Since $m-\phi(m)$ is odd (because m is odd and $m>1$ because if $m=1$ then $m-\phi(m)=0$ contradicting the fact that $w>1$), it follows that the only possibility is $\gamma=\alpha-1$, i.e., $\alpha=\gamma+1$. Further, let $m_1,\ldots,m_k$ be all the solutions to the equation $m-\phi(m)=w$. It is clear that this equation has only finitely many solutions. Indeed, any such solution m is composite (because $w>1$), therefore $w=m-\phi(m)\ge m/p(m)\ge m^{1/2}$, where $p(m)$ is the smallest prime factor of m. Thus, $w=m-\phi(m)$ implies $m\le w^2$, which shows that k is finite. If $k=0$, then we are through. Assume

2000 *Mathematics Subject Classification*: Primary 11A25.

now that $k \geq 1$ (this is always the case when w is prime because $m = w^2$ is such a solution in this case). In fact, by letting $m = p_1 p_2$ with distinct primes p_1 and p_2 the equation $m - \phi(m) = w$ leads to $p_1 + p_2 = w + 1$ and Goldbach's conjecture would seem to suggest that such primes p_1 and p_2 should always exist, therefore that $k \geq 1$ holds always.

Backtracking, it follows that every solution of $f(p) = r$ is of the form $p - 1 = 2^{\gamma+1} m_i$ for some $i = 1, \ldots, k$. We conclude the proof with the following result.

LEMMA 2. *Let $m_1, \ldots, m_k$ be odd positive integers. Then there exist infinitely many positive integers n such that $2^n m_i + 1$ is composite for all $i = 1, \ldots, k$.*

Proof. We will prove more than asserted, namely that the positive integers n can be chosen to be primes. Assume that this is not true. Then there exists a positive constant c_1 such that if $p > c_1$ is a prime, then $2^p m_i + 1$ is prime for some $i = 1, \ldots, k$. We let $M = \mathrm{lcm}[m_1, \ldots, m_k]$. We may assume that $c_1 > M$. We set $\Pi = \{p > c_1\}$ and $\Pi_i = \{p > c_1 \mid 2^p m_i + 1 \text{ is prime}\}$ for $i = 1, \ldots, k$. Assume that $\Pi = \bigcup_{i=1}^k \Pi_i$. Let p_1 be the first prime number in Π. Up to relabeling the m_i's, we may assume that $P_1 = 2^{p_1} m_1 + 1$ is prime. Let $\mathcal{A}_1 = \{p > p_1 \mid p \equiv p_1 \pmod{2^{p_1} M}\}$. Since $p_1 > c_1 > M$, it follows, by Dirichlet's theorem on primes in arithmetic progressions, that $\mathcal{A}_1$ is infinite. Note that $P_1 - 1 \mid 2^{p_1} M$, and therefore, by Fermat's Little Theorem, if $p \in \mathcal{A}_1$, then $2^p \equiv 2^{p_1} \pmod{P_1}$. In particular, $2^p m_1 + 1 \equiv 2^{p_1} m_1 + 1 \pmod{P_1} \equiv 0 \pmod{P_1}$, and since $p > p_1$ it follows that $2^p m_1 + 1$ is composite. Thus, if $p \in \mathcal{A}_1$ it follows that $p \notin \Pi_1$. Hence, $\mathcal{A}_1 \subseteq (\bigcup_{i=2}^k \Pi_i) \setminus \Pi_1$.

Now let p_2 be the first prime in $\mathcal{A}_1$. We may assume that $p_2 \in \Pi_2$. Write $P_2 = 2^{p_2} m_2 + 1$ and let $\mathcal{A}_2 = \{p > p_2 \mid p \equiv p_2 \pmod{2^{p_2} M}\}$. It is easy to see that $\mathcal{A}_2 \subset \mathcal{A}_1$. Moreover, the previous argument shows that $P_2 - 1 \mid 2^{p_2} M$, therefore $2^p \equiv 2^{p_2} \pmod{P_2}$ holds for all $p \in \mathcal{A}_2$. In particular, $2^p m_2 + 1$ is a multiple of P_2, and therefore $p \notin \Pi_2$. Hence, $\mathcal{A}_2 \subseteq (\bigcup_{i=3}^k \Pi_i) \setminus (\Pi_1 \cup \Pi_2)$. Inductively, we construct infinite sets of primes $\mathcal{A}_j$ such that $\mathcal{A}_j \subseteq (\bigcup_{i=j+1}^k \Pi_i) \setminus (\bigcup_{i=1}^j \Pi_i)$. Of course, this is absurd for $j = k$, which completes the proof of Lemma 2 and hence of Theorem 1. ∎

EXAMPLE 3. Let $w = 3$. The only solution of the equation $m - \phi(m) = 3$ is $m = 9$. Thus, if $r = 2^\gamma \cdot 3$, then $p = 2^{\gamma+1} \cdot 9 + 1$. Taking $\gamma = 4t - 1$ we note that $2^{\gamma+1} \cdot 9 + 1$ is always a multipe of 5, therefore it cannot be a prime. Hence, numbers of the form $2^{4t-1} \cdot 3$ are not of the form $f(p)$ with any odd prime number p. Similarly, taking $w = 5$, the only m such that $m - \phi(m) = 5$ is $m = 25$. Thus, $p = 2^{\gamma+1} \cdot 25 + 1$. Taking $\gamma = 2t$, we find that $2^{\gamma+1} \cdot 25 + 1$ is a multiple of 3, therefore it cannot be prime. Hence, numbers of the form $2^{2t} \cdot 5$ are not of the form $f(p)$ with any odd prime number p either.

REMARKS 4. The conclusion of Theorem 1 is probably false when $w = 1$. Indeed, let $\gamma \geq 0$. The well known Prime k-Tuplets Conjecture suggests that there should exist a pair of primes (p, q) (in fact, infinitely many such) with $p = 2^{\gamma+1}q + 1$ and for such primes p and q we certainly have $f(p) = 2^{\gamma}$.

Acknowledgments. This paper was written during a visit of P. G. W. at the Mathematical Institute of the UNAM in Morelia in February 2004. He thanks this Institute for its hospitality. The first author was supported in part by the grant SEP-CONACyT 37259E and the second author by the Natural Science and Engineering Research Council of Canada.

REFERENCES

[1] J. Browkin and A. Schinzel, *On integers not of the form $n - \phi(n)$*, Colloq. Math. 68 (1995), 55–58.

[2] A. Flammenkamp and F. Luca, *Infinite families of noncototients*, ibid. 86 (2000), 37–41.

[3] R. K. Guy, *Unsolved Problems in Number Theory*, Springer, 1994.

Instituto de Matemáticas
Universidad Nacional Autónoma de México
C.P. 58180, Morelia, Michoacán, México
E-mail: fluca@matmor.unam.mx

Department of Mathematics
University of Ottawa
585 King Eward Street
Ottawa, Ontario, Canada
E-mail: gwalsh@mathstat.uottawa.ca

Received 18 February 2004 (4429)