JOURNAL OF NUMBER THEORY 43, 168–172 (1993)

# On Nontotients

ZHANG MINGZHI

*Department of Mathematics, Sichuan University, Chengdu, Sichuan Province, People's Republic of China*

*Communicated by Hans Zassenhaus*

Received February 15, 1991; revised August 15, 1991

Let $\phi(x)$ be Euler's totient function. If the equation $\phi(x) = n$ has no solution, then $n$ is called a nontotient. In this paper, we prove that a nontotient can have an arbitrary divisor and we give two sorts of odd numbers such that for the odd number $k$ of the first sort, $2^\alpha \cdot k$ is a nontotient for a given positive integer $\alpha$ while for the odd number $k$ of the second sort, $2^\alpha \cdot k$ is a nontotient for arbitrary positive integer $\alpha$. 

Let $\phi(x)$ be Euler's totient function. If the equation

$$\phi(x) = n \tag{1}$$

has no solution, then $n$ is called a nontotient.

The Lehmers [1] have calculated that the number of nontotients less than $9 \cdot 10^4$ is 26663.

In 1956 Schinzel [2] proved that $n = 2 \cdot 7^k$ is a nontotient for every positive integer $k$.

In 1961 Ore [3] noted that for every $\alpha \geqslant 1$, there exists an odd number $k_\alpha$ such that $n = 2^\alpha \cdot k_\alpha$ is a nontotient.

In 1963 Selfridge [3] proved that for every $\alpha \geqslant 1$, $k_\alpha \leqslant 271129$.

In 1976 Mendelsohn [4] proved that there exist infinitely many primes $p$ such that for every $\alpha \geqslant 1$, $n = 2^\alpha p$ is a nontotient. In fact Selfridge [3] had proved this before.

In 1989 Spyropoulos [5] gave some sufficient conditions for $n$ to be a nontotient.

In this paper, we shall generalize Ore's result and give some sorts of nontotients. We first prove that a nontotient can have any divisor.

THEOREM 1. *For every positive integer $m$, there exists a prime $p$ such that $mp$ is a nontotient.*



0022-314X/93 $5.00

*Proof.* Let all divisors of $m$ be

$$d_1, d_2, ..., d_s$$

and the primes $q_i$ $(1 \leqslant i \leqslant s)$ satisfy $m < q_1 < q_2 < \cdots < q_s$. Clearly, $(d_i, q_i) = 1$. Suppose the congruence

$$d_i x \equiv -1 \pmod{q_i} \qquad (1 \leqslant i \leqslant s) \tag{2}$$

has the solution $x \equiv b_i \pmod{q_i}$. It follows from the Chinese remainder theorem that the system of congruences

$$\begin{aligned} x &\equiv b_1 \pmod{q_1} \\ x &\equiv b_2 \pmod{q_2} \\ &\cdots \\ x &\equiv b_s \pmod{q_s} \end{aligned}$$

has the solution $x \equiv b \pmod{q_1 q_2 \cdots q_s}$. Clearly, $(b, q_1 q_2 \cdots q_s) = 1$. From Dirichlet's theorem on the primes in arithmetic progressions, it follows that there exists a prime $p > q_s$ such that

$$p \equiv b \qquad (\text{mod } q_1 q_2 \cdots q_s). \tag{3}$$

Now, we show that $p$ is the required prime.

If the equation $\phi(x) = mp$ has a solution $x$, then $p^2 \mid x$ or there exists a prime $q$ such that $q \mid x$ and $p \mid q - 1$.

But if $p^2 \mid x$, then $p(p-1) \mid \phi(x) = mp$, and $p - 1 \mid m$, which contradicts $p > q_s > m$.

If there exists a prime $q$ such that $q \mid x$ and $p \mid q-1$, then $q - 1 = pd \mid \phi(x) = mp$, $d \mid m$, so that $d = d_i$, $q = pd_i + 1 > q_i$. But from (2) and (3) we have $q_i \mid pd_i + 1$, a contradiction.

The proof is complete.

Theorem 1 generalizes Ore's result.

Let $n = 2^\alpha k$, $2 \nmid k$. Obviously, if $n$ is a nontotient, then $2^t k$ $(0 \leqslant t \leqslant \alpha)$ is likewise a nontotient. Therefore, we shall try to find some sort of odd $k$ such that $2^\alpha k$ is a nontotient for a given $\alpha$, or more generally, for all $\alpha \geqslant 1$.

For $\alpha = 1$, we can obtain

THEOREM 2. *Let $n = 2p_1^{\alpha_1} p_2^{\alpha_2} \cdots p_s^{\alpha_s}$, $2 < p_1 < p_2 < \cdots < p_s$, where $p_i$ are primes. Then necessary and sufficient conditions for $n$ to be a nontotient are*

(i) $n + 1$ *is composite*;

(ii) $p_s - 1 \neq 2p_1^{\alpha_1} p_2^{\alpha_2} \cdots p_{s-1}^{\alpha_{s-1}}$.

*Proof.* Suppose (i) and (ii) hold. If $\phi(x) = n$ has a solution, then $x = p^\beta$ or $x = 2p^\beta$, $p > 2$. Hence, $\phi(x) = p^{\beta-1}(p-1) = 2p_1^{\alpha_1}p_2^{\alpha_2}\cdots p_s^{\alpha_s}$.

If $\beta = 1$, then $n + 1 = p$, a contradiction.

If $\beta > 1$, then $p$ is the largest prime divisor of $n$, $p = p_s$, $\alpha_s = \beta - 1$, and $p - 1 = 2p_1^{\alpha_1}p_2^{\alpha_2}\cdots p_{s-1}^{\alpha_{s-1}}$, a contradiction again. Hence, $n$ is a nontotient.

Suppose (i) or (ii) does not hold.

If $n + 1$ is a prime, then $\phi(n+1) = n$.

If $p_s - 1 = 2p_1^{\alpha_1}p_2^{\alpha_2}\cdots p_{s-1}^{\alpha_{s-1}}$ then $\phi(p_s^{\alpha_s+1}) = n$.

The proof is complete.

Theorem 2 is effective for small $n$. For example, there are altogether 210 nontotients for $n \leqslant 1000$, of which 156 numbers can be found by Theorem 2.

Let $p$ be a prime, $n = 2^\alpha p$. Selfridge [3] noted that necessary and sufficient conditions for $n$ to be a nontotient are that for $1 \leqslant t \leqslant \alpha$, $p \neq 2^t + 1$ and $2^t p + 1$ is composite. Starting from such $n$, we can obtain

THEOREM 3. *Let $n = 2^\alpha p p_1^{\alpha_1}p_2^{\alpha_2}\cdots p_s^{\alpha_s}$, where $p, p_1, p_2, ..., p_s$ are distinct odd primes and the numbers $2^t p + 1$ $(1 \leqslant t \leqslant \alpha)$ are composite. Let $q_t$ be a prime divisor of $2^t p + 1$, and let $M$ be the least common multiple of $q_1, q_2, ..., q_\alpha$. If $p_1, p_2, ..., p_s$ satisfy:*

(i) *There exists an odd prime $q$ such that $q \mid p - 1$, and*

$$q \neq p_i \qquad (1 \leqslant i \leqslant s), \qquad or \qquad 2^\beta \mid p - 1, \beta > \alpha;$$

(ii) $p_i \equiv 1 \pmod M$ $(1 \leqslant i \leqslant s)$.

*Then for any set of positive integers $\alpha_1, \alpha_2, ..., \alpha_s$, $n$ is a nontotient.*

*Proof.* If $\phi(x) = 2^\alpha p p_1^{\alpha_1}p_2^{\alpha_2}\cdots p_s^{\alpha_s}$ has a solution, then $p^2 \mid x$ or $x$ has a prime divisor $r = pd + 1$.

If $p^2 \mid x$, then $p(p-1) \mid \phi(x)$, $p - 1 \mid 2^\alpha p_1^{\alpha_1}p_2^{\alpha_2}\cdots p_s^{\alpha_s}$, which contradicts (i).

If $x$ has a prime divisor $r = pd + 1$, then $pd \mid \phi(x)$, therefore $d = 2^t p_1^{\beta_1}p_2^{\beta_2}\cdots p_s^{\beta_s}$, $0 \leqslant t \leqslant \alpha$, $0 \leqslant \beta_i \leqslant \alpha_i$. Hence $r = pd + 1 \equiv 2^t p + 1 \equiv 0 \pmod{q_t}$. This contradicts $r \geqslant 2^t p + 1 > q_t$.

The proof is complete.

EXAMPLE 1. Let $p = 17$, $\alpha = 2$. We can take $q_1 = 5$, $q_2 = 3$. From $31 \equiv 61 \equiv 151 \equiv 1 \pmod{3 \cdot 5}$ it follows that the integers

$$n = 2^2 \cdot 17 \cdot 31^{\alpha_1} \cdot 61^{\alpha_2} \cdot 151^{\alpha_3}$$

are nontotients for all $\alpha_1, \alpha_2, \alpha_3 \geqslant 1$.

EXAMPLE 2. Let $p=47$. Selfride [3] noted that $47\cdot 2^t+1$ is composite for $1\leqslant t\leqslant 582$, but is prime for $t=583$. If we take $\alpha=30$, then it is easy to verify that $47\cdot 2^t+1$ $(1\leqslant t\leqslant 30)$ is divided by one of the primes of the set $\{3, 5, 7, 11, 13, 19\}$. Since 2282281, 3993991, and 5135131 are primes and $2282281\equiv 3993991\equiv 5135131\equiv 1 \pmod{3\cdot 5\cdot 7\cdot 11\cdot 13\cdot 19}$, we have that the integers

$$n=2^{30}\cdot 47\cdot 2282281^{\alpha_1}\cdot 3993991^{\alpha_2}\cdot 5135131^{\alpha_3}$$

are nontotients for all $\alpha_1, \alpha_2, \alpha_3\geqslant 1$.

Now we consider the odd $k$ such that $2^\alpha\cdot k$ are nontotients for all $\alpha\geqslant 1$.

THEOREM 4. *Let $k$ be an odd number such that the numbers $2^\alpha\cdot k$ are nontotients for all $\alpha\geqslant 1$. If $k=k_1k_2$, $(k_1, k_2)=1$, then either $2^\alpha\cdot k_1$ are nontotients for all $\alpha\geqslant 1$ or $2^\alpha\cdot k_2$ are nontotients for all $\alpha\geqslant 1$.*

*Proof.* Suppose not. Then there exist $\alpha_1$ and $\alpha_2$ such that $\phi(x)=2^{\alpha_1}\cdot k_1$ has a solution $x=x_1$ and $\phi(x)=2^{\alpha_2}k_2$ has a solution $x=x_2$ and we assume that each $\alpha_i$ is the smallest.

Let $p=2^l+1$ be a Fermat prime, if $p\mid x_i$ $(i=1, 2)$, then $p^2\mid x_i$. In fact, if $x_i=py_i$, $(p, y_i)=1$, then

$$\phi(x_i)=2^l\phi(y_i)=2^{\alpha_i}k_i$$
$$\phi(y_i)=2^{\alpha_i-l}k_i.$$

This contradicts the assumption that $\alpha_i$ is the minimum.

Let $(x_1, x_2)=d$, then $\phi(d)\mid(\phi(x_1), \phi(x_2))=2^{\min\{\alpha_1, \alpha_2\}}$, and $\phi(d)=2^\beta$ for some $\beta\leqslant\min\{\alpha_1, \alpha_2\}$. Therefore, $d=2^t$ or $d=2^tp_1p_2\cdots p_s$, where $p_i$ are distinct Fermat primes. But the second case cannot occur. In fact, $p_i\mid x_1, x_2$ implies $p_i^2\mid x_1, x_2$, and $p_i^2\mid d$, a contradiction. Hence $d=2^t$.

Assume that $x_1=2^t\cdot y_1$, $2\nmid y_1$, then $(y_1, x_2)=1$. From $\phi(x_1)=2^{t-1}\cdot\phi(y_1)=2^{\alpha_1}k_1$, we have that $\phi(y_1)=2^{\alpha_1-t+1}k_1$. Hence

$$\phi(y_1x_2)=\phi(y_1)\cdot\phi(x_2)=2^{\alpha_1+\alpha_2-t+1}k_1k_2,$$

a contradiction.

The proof is complete.

From Theorem 4 we naturally consider the case $k=p^\beta$ first. As noted above, for $\beta=1$ the existence and infiniteness of such $p$ are known. Sierpinski [3] has noted that for the prime $p=271129$ and every positive integer $\alpha$, $2^\alpha p+1$ is divided by one of the primes of the set $\{3, 5, 7, 13, 17, 241\}$. Clearly, every prime $p$ which satisfies the congruence $p\equiv 271129 \pmod{3\cdot 5\cdot 7\cdot 13\cdot 17\cdot 241}$ has the same covering set of primes as 271129 and the number of such primes is infinite from Dirichlet's theorem on the primes in arithmetic progressions. Similarly, Selfridge [1] noted that $2^{\alpha} \cdot 78557+1$ is divided by one of the primes of the set $\{3, 5, 7, 13, 19, 37, 73\}$. Therefore, every prime $p$ which satisfies the congruence $p \equiv 78557 \pmod{3 \cdot 5 \cdot 7 \cdot 13 \cdot 19 \cdot 37 \cdot 73}$ has the same covering set of primes as 78557.

Starting from such primes, we can obtain

THEOREM 5. *Let $p, q_1, q_2, ..., q_r$ be distinct odd primes such that $p$ is not a Fermat prime and for every $t \geqslant 1$, there exists a $q_i$ $(1 \leqslant i \leqslant r)$ such that $q_i \leqslant 2^t p+1$ and $2^t p+1 \equiv 0 \pmod{q_i}$. Let the primes $p_j$ $(1 \leqslant j \leqslant s)$ satisfy:*

(i) *There exists an odd prime $q$ such that $q \mid p-1$ and $q \neq p_j$ $(1 \leqslant j \leqslant s)$;*

(ii) $p_j \equiv 1 \pmod{q_1 q_2 \cdots q_r}$.

*Then for any set of positive integers $\alpha, \alpha_1, \alpha_2, ..., \alpha_s$, the integers*

$$n = 2^{\alpha} p p_1^{\alpha_1} p_2^{\alpha_2} \cdots p_s^{\alpha_s}$$

*are nontotients.*

We omit the proof of Theorem 5, since it is similar to that of Theorem 3.

EXAMPLE. Let $p = 271129$, where $S = \{3, 5, 7, 13, 17, 241)$ is the covering set of primes. Take $p_1 = 78293671$, $p_2 = 100663291$, $p_3 = 111848101$. Then from $p_1 \equiv p_2 \equiv p_3 \equiv 1 \pmod{3 \cdot 5 \cdot 7 \cdot 13 \cdot 17 \cdot 241}$ it follows that the integers

$$n = 2^{\alpha} \cdot 271129 \cdot 78293671^{\alpha_1} \cdot 100663291^{\alpha_2} \cdot 111848101^{\alpha_3}$$

are nontotients for any set of positive integers $\alpha, \alpha_1, \alpha_2, \alpha_3$.

## ACKNOWLEDGMENT

The author thanks the referee for his helpful suggestions.

## REFERENCES

1. R. K. GUY, "Unsolved Problems in Number Thery," pp. 42, 51, Springer-Verlag, New York, 1980.
2. A. SCHINZEL, Sur l'équation $\phi(x) = m$, *Elem. Math.* **11** (1956), 75–78.
3. J. L. SELFRIDGE AND P. T. BATEMAN, Solution to problem 4995, *Amer. Math. Monthly* **70** (1963), 101–102.
4. N. S. MENDELSOHN, The equation $\phi(x) = k$, *Math. Mag.* **49** (1976), 37–39.
5. K. SPYROPOULOS, Euler's equation $\phi(x) = k$ with no solution, *J. Number Theory* **32** (1989), 254–256.