ON THE DISTRIBUTION OF TOTIENTS

Jan-Christoph Puchta
Mathematics Institut, Albert-Ludwigs-Universität Freiburg
Eckerstraße 1, 79104 Freiburg, Germany
(Submitted November 1999-Final Revision July 2000)

An integer n is called a totient if there is some integer x such that $\varphi(x)=n$, where φ is Euler's function. If this equation is not solvable, n is called a *nontotient*. In 1956, Schinzel [4] proved that, for any positive k, $2\cdot 7^k$ is a nontotient. In 1961, Ore (see [1]) proved that, for every α, there is some odd number k such that $2^\alpha \cdot k$ is a nontotient. In 1963, Selfridge [1] showed that the same is true with k restricted by $k \le 271129$. Recently, Mingzhi [3] proved that, for any given d, there are infinitely many primes p such that dp is a nontotient. In fact, his proof gives the existence of a, q with $(a,q)=1$ such that, for any sufficiently large prime $p \equiv a \pmod q$, dp is a nontotient. Thus, by the prime number theorem for arithmetic progressions, a positive percentage of all primes p has this property. However, here $q > d^{\tau(d)}$, where $\tau(n)$ denotes the number of divisors of n; thus, this percentage is quite small. In this note we will show this is true for almost all primes p. Further, we describe explicitly a large class of nontotients. We will prove the following theorems.

Theorem 1: There is an absolute constant c such that, for any integer d, the number of primes $p \le x$ such that dp is a totient is bounded above by $c\tau(d^2)\frac{x}{\log^2 x}$.

Here and in the sequel, the letter c denotes absolute positive constants and the letters p and q denote prime numbers only.

Theorem 2: Set $m = 3\cdot 5\cdot 7\cdot 13\cdot 19\cdot 37\cdot 73$, $a = 35274404$. If d is an integer relatively prime to m such that, for every prime divisor p of d, p is a quadratic residue (mod 73), and $q \equiv a \pmod m$ is a prime number such that $q-1 \nmid d$, then dq is a nontotient.

It will be apparent from the proof that the value of a is by no means unique. Also, m may be subject to variation. We only use the fact that m has many prime divisors, and that the least common multiple of all $p-1$, where p ranges over the prime divisors of m, is very small. However, for other values of m, the computations would become extremely long.

The proof of Theorem 1 is based on the following theorem of Erdös [2].

Theorem 3: There is an absolute constant c such that, for any integer a, we have, for the number $N_a(x)$ of primes $p \le x$ such that $ap+1$ is also prime, the inequality

$$N_a(x) \le c\frac{x}{\log^2 x}\prod_{q\mid a}\left(1-\frac{1}{q}\right)^{-1}.$$

Proof of Theorem 1: Assume that p is some prime such that dp is a totient, say $dp=\varphi(n)$. Since φ is multiplicative and, for prime numbers q, we have $\varphi(q)=q-1$, there is either some prime divisor q of n such that $q \equiv 1 \pmod p$, say $q=ap+1$, or n is divisible by p^2. In the latter case we have $n=p^k m$, where $(p,m)=1$. Thus, we get $dp=(p-1)p^{k-1}\varphi(m)$ and $p-1 \mid d$. So the number of such p is $\le \tau(d)$. In the first case, we have $n=qm$ with $(q,m)=1$; therefore, we get $dp=(q-1)\varphi(m)=ap\varphi(m)$. Especially, a is some divisor of d. We now fix some a, and count the number of primes $p \le x$ such that the equation $dp=\varphi(qm)$ is solvable when $q=ap+1$ is

prime. This is at most the number of $p \le x$ such that $q = ap+1$ is prime, and by Theorem 2 this number is

$$\le c\frac{x}{\log^2 x}\prod_{q|a}\left(1-\frac{1}{q}\right)^{-1}.$$

Since a is a divisor of d, the total number of solutions is at most

$$c\frac{x}{\log^2 x}\sum_{a|d}\prod_{q|a}\left(1-\frac{1}{q}\right)^{-1}.$$

We have

$$\prod_{q|a}\left(1-\frac{1}{q}\right)^{-1} = \prod_{q|a}\left(1+\frac{1}{q}\right)\prod_{q|a}\left(1-\frac{1}{q^2}\right)^{-1}$$
$$< \frac{\pi^2}{6}\prod_{q|a}\left(1+\frac{1}{q}\right) \le c\sum_{t|a}\frac{1}{t}.$$

Hence, the sum above can be estimated as

$$\sum_{a|d}\prod_{q|a}\left(1-\frac{1}{q}\right)^{-1} \le c\sum_{a|d}\sum_{t|a}\frac{1}{t}.$$

The function $f(d) = \sum_{a|d}\sum_{t|a}\frac{1}{t}$ is multiplicative, since it is the Dirichlet convolution of multiplicative functions. For prime powers, we have

$$f(p^k) = \sum_{0\le l\le k}\ \sum_{0\le m\le l} p^{-m} = \sum_{0\le m\le k}(k-m+1)p^{-m} < 2k+1 = \tau(p^{2k}).$$

By multiplicativity, we get $f(n) \le \tau(n^2)$ for any n. Hence, the total number of primes $p \le x$ such that dp is totient is at most

$$c\frac{x}{\log^2 x}\tau(d^2)+\tau(d),$$

and by increasing c slightly, the second term may be neglected. This proves Theorem 1.

Proof of Theorem 2: Note that, if the equation $\varphi(x) = dq$ is solvable, either $q^2 | x$ or there is some prime $p \equiv 1 \pmod{q}$ such that $p-1 | dq$. In the first case, we have

$$q(q-1) = \varphi(q^2) \,|\, \varphi(x) = dq,$$

contradicting our first assumption on d. In the second case, number the prime divisors of m by r_j, $1 \le j \le 7$, and choose some primitive root π_j for each j. We may assume that p does not divide m; thus, the condition that p is prime implies $r_j \nmid p$. This is equivalent to $d'q \not\equiv 1 \pmod{r_j}$ for a certain divisor d' of d. Write

$$d' = \prod_{i=1}^{n} p_i^{x_i},$$

define a_{ij} by $\pi_j^{a_{ij}} \equiv p_i \pmod{r_j}$, and define b_j by $\pi_j^{b_j} \equiv q \equiv a \pmod{r_j}$. Then the condition on p implies the system of incongruences

$$\sum_{i=1}^{n} a_{ij}x_i \not\equiv -b_j \pmod{r_j - 1}.$$

Now, choosing π_j to be the least primitive root (mod r_j), i.e., $\pi_j = 2$ for $j \neq 3, 7$, $\pi_3 = 3$, and $\pi_7 = 5$, we obtain $b_1 = 1$, $b_2 = 2$, $b_3 = 4$, $b_4 = 8$, $b_5 = 12$, $b_6 = 24$, $b_7 = 0$. (Note that here we have much more freedom; we could choose different primitive roots, and we could use different values for the b_j, each resulting in different values for a.) To prove our claim, note first that by assumption all p_i are quadratic residues (mod 73), so all α_{i7} are even. Thus, since b_7 is even, too, we may divide the seventh incongruence by 2, obtaining an incongruence (mod 36). Further, for all j, we have $r_j - 1 | 36$, so every incongruence (mod $r_j - 1$) may be written as a set of incongruences (mod 36). Now, the solvability of the system is equivalent to the existence of some residue class (mod 36) that is not contained in one of the following seven sets, each defined by one of the seven incongruences:

$$\{1, 3, 5, 7, 9, 11, 13, 15, 17, 19, 21, 23, 25, 27, 29, 31, 33, 35\},$$
$$\{2, 6, 10, 14, 18, 22, 26, 30, 34\},$$
$$\{4, 10, 14, 20, 26, 32\},$$
$$\{8, 20, 32\}, \{12, 30\}, \{24\}, \{36\}.$$

By construction, the first four sets define residue classes (mod 12), and one easily checks that all but the class 0 are covered, whereas the last three sets contain the remaining class. Thus, our initial assumption on the solvability of the equation $\varphi(x) = dq$ was wrong, proving Theorem 2.

REFERENCES

1. P. T. Bateman & J. L. Selfridge. "Solution to Problem 4995." *Amer. Math. Monthly* **70** (1963):101-02.
2. P. Erdös. "On the Normal Number of Prime Factors of $p-1$ and Some Related Problems Concerning Euler's φ-Function." *Q. J. Math.* Oxf. Ser. 6 (1935):205-13.
3. Z. Mingzhi. "On Nontotients." *Number Theory* **43** (1993):168-72.
4. A. Schinzel. "Sur l'equation $\phi(x) = m$." *Elem. Math.* **11** (1956):75-78.

AMS Classification Number: 11A25

❖❖❖