On the size of solutions of the inequality $\phi(ax + b) < \phi(ax)$

*Herman te Riele**

Abstract. An estimate is given of the size of a solution $n \in \mathbb{N}$ of the inequality $\phi(an+b) < \phi(an)$, $\gcd(a, b) = 1$. Experiments indicate that this gives a useful indication of the size of the *minimal* solution.

1991 Mathematics Subject Classification: 11A25, 11Y70.

1. Introduction

Let $\phi(m)$ be the Euler totient function. Recently, D.J. Newman [5] has shown that for any nonnegative integers a, b, c, and d with $ad \neq bc$, there exist infinitely many positive integers n for which

$$\phi(an + b) < \phi(cn + d). \tag{1}$$

For the case $a = c = 30$, $b = 1$, $d = 0$, Newman stated that there are no solutions n with $n < 20\,000\,000$ and that a solution may be beyond the reach of any possible computers. Two years later, Greg Martin [3] found the smallest solution for this case, which turned out to be a number as large as 1116 decimal digits.

In this paper, we will analyse Newman and Martin's approach to this problem which enables us, for the case $a = c$, $\gcd(a, b) = 1$, $d = 0$, to give an estimate of the size of an n satisfying (1). Experiments indicate that this estimate also gives a useful indication of where the *minimal* solution of (1) can be expected.

Notation. By p_k we mean the k-th prime and by P_k the product $p_1 p_2 \cdots p_k$.

Acknowledgements. I like to thank Greg Martin and two anonymous referees for their constructive criticism which led to an improved presentation of this paper.

* Part of this research was carried out while the author was visiting the Mathematical Sciences Research Institute (Berkeley, CA) in September 2000.

Public-Key Cryptography and Computational Number Theory
K. Alster, J. Urbanowicz and H. C. Williams (Eds.)

2. A solution of $\phi(30n+1) < \phi(30n)$

We first consider the special case $a = c = 30$, $b = 1$, $d = 0$. As Martin showed, if n satisfies $\phi(30n+1) < \phi(30n)$, then

$$\frac{\phi(30n+1)}{30n+1} < \frac{\phi(30n)}{30n+1} < \frac{\phi(30)n}{30n} = \frac{4}{15} = 0.26666\ldots, \tag{2}$$

(using $\phi(ab) \leq \phi(a)b\ \forall a, b \in \mathbb{N}$). Since ϕ is multiplicative and since $\phi(p^e)/p^e = \phi(p)/p$ for any prime p and any $e \geq 2$, the smallest m for which $\phi(m)/m$ has a given value, is squarefree. Therefore, we look for solutions of the inequality $\phi(30n+1) < \phi(30n)$ among the numbers

$$m_k := \prod_{i=4}^{k} p_i, \quad k = 4, 5, \ldots,$$

which satisfy

$$m_k \equiv 1 \bmod 30 \quad \text{and} \quad \frac{\phi(m_k)}{m_k} < \frac{4}{15}. \tag{3}$$

Such m_k exist with high probability because the numbers

$$\frac{\phi(m_k)}{m_k} = \prod_{i=4}^{k} \left(1 - p_i^{-1}\right), \quad k = 4, 5, \ldots$$

decrease monotonically to zero, and because the residues $m_k \bmod 30$, $k = 4, 5, \ldots$, seem to be uniformly distributed. For example, in the first 800 terms, the $\phi(30) = 8$ possible values

$$1, 7, 11, 13, 17, 19, 23, 29$$

occur with frequencies

$$100, 99, 107, 104, 110, 100, 85, 95,$$

respectively.

With help of the GP/Pari package [1], we have found that

$$m_{388} \equiv 1 \bmod 30 \quad \text{and} \quad \frac{\phi(m_{388})}{m_{388}} = 0.26631\ldots < \frac{4}{15}, \tag{4}$$

and that there is no m_k with $4 \leq k < 388$ which satisfies these conditions. Now we check whether the number $n_{388} := (m_{388} - 1)/30$ actually is a solution of the inequality $\phi(30n+1) < \phi(30n)$. It turns out that $n_{388} = 2^3 n'$ where $n' = 5.502175051\ldots \times 10^{1124}$ has no prime divisors $\leq p_{50000} = 611953$. Using the well-known result that if n' has no prime divisors $\leq B$ then

$$\frac{\phi(n')}{n'} > \left(1 - \frac{1}{B}\right)^{\log n' / \log B},$$

we find

$$\frac{\phi(30n_{388})}{30n_{388}} = \frac{\phi(240n')}{240n'} = \frac{4}{15}\frac{\phi(n')}{n'}$$
$$> \frac{4}{15}\left(1 - \frac{1}{611953}\right)^{\log n'/\log 611953} = 0.26658\ldots.$$

Since

$$\frac{30n_{388}}{30n_{388}+1} = 1 - 7.57... \times 10^{-1128},$$

we conclude that

$$\frac{\phi(30n_{388})}{30n_{388}+1} > 0.26657.$$

Combining this with (4) we have

$$\frac{\phi(30n_{388}+1)}{30n_{388}+1} = 0.26631... < 0.26657 < \frac{\phi(30n_{388})}{30n_{388}+1}$$

which implies that $\phi(30n_{388}+1) < \phi(30n_{388})$.

So $n_{388} = 4.401740040... \times 10^{1125}$ is a solution of the inequality $\phi(30n+1) < \phi(30n)$, but it is *not* the smallest one. Martin [3] found this by computing the minimum number of distinct prime factors of such an n, viz., 382, by explicitly giving a solution with 382 distinct prime factors, and by showing that there are no smaller ones. Martin's minimum solution is given by

$$n = (z-1)/30, \quad \text{where} \quad z = \left(\prod_{i=4}^{383} p_i\right) p_{385}p_{388},$$

and

$$n = 2.329098101... \times 10^{1115}.$$

3. An estimate of the size of a solution of $\phi(an+b) < \phi(an)$, $\gcd(a,b) = 1$

In this section we will mimic and analyse the step described in Section 2 to find an $m_k \equiv 1 \bmod 30$ for which $\phi(m_k)/m_k < \phi(30)/30$, for the more general case $a = c$, $\gcd(a,b) = 1$, $d = 0$ in (1). So we consider the inequality

$$\phi(an+b) < \phi(an), \quad \gcd(a,b) = 1, \tag{5}$$

and look for a number $m_k \equiv b \bmod a$ for which $\phi(m_k)/m_k < \phi(a)/a$. We expect this m_k to be a solution of (5) and, also, that its size is not too far from the size of the *smallest* solution of (5) as we have seen in Section 2 for the case $a = 30$, $b = 1$.

As in Section 2, consider the products of the small primes which are not in a:

$$m_k := \frac{P_k}{\gcd(P_k, a)} \quad \text{for} \quad k = 1, 2, \ldots, \tag{6}$$

which satisfy

$$m_k \equiv b \bmod a \quad \text{and} \quad \frac{\phi(m_k)}{m_k} < \frac{\phi(a)}{a}. \tag{7}$$

Write $m_k = an_k + b$. We derive an estimate of the expected size of the smallest m_k satisfying (7) as follows. This m_k must satisfy

$$\phi(an_k + b) \approx \phi(an_k). \tag{8}$$

We assume that $b \ll an_k$ so that $an_k + b \approx an_k$. Dividing gives

$$\frac{\phi(an_k + b)}{an_k + b} \approx \frac{\phi(an_k)}{an_k}. \tag{9}$$

For the left hand side of (9) we have, using (6) [1)]

$$\frac{\phi(an_k + b)}{an_k + b} = \frac{\phi(m_k)}{m_k} = \frac{a}{\phi(a)} \frac{\phi(P_k)}{P_k} = \frac{a}{\phi(a)} \prod_{p \le p_k} \left(1 - \frac{1}{p}\right).$$

For the right hand side of (9) we assume that

$$\frac{\phi(an_k)}{an_k} \approx \frac{\phi(a)}{a}.$$

This requires that the prime divisors of n_k which are *not* in a are not too small. Substitution in (9) gives

$$\prod_{p \le p_k} \left(1 - \frac{1}{p}\right) \approx \left(\frac{\phi(a)}{a}\right)^2.$$

With Mertens's Theorem [2, §22.8]:

$$\prod_{p \le x} \left(1 - \frac{1}{p}\right) \sim \frac{e^{-\gamma}}{\log x} \quad \text{as} \quad x \to \infty,$$

where γ is Euler's constant ($= 0.5772\ldots$), it follows that

$$\log p_k \approx e^{-\gamma} \left(\frac{a}{\phi(a)}\right)^2. \tag{10}$$

We estimate the corresponding size of n_k as follows. We have

$$an_k + b = m_k = \frac{P_k}{\gcd(P_k, a)},$$

1) with k such that $p_k \ge$ the largest prime in a.

so that

$$\log n_k \approx \log P_k - \log a - \log(\gcd(P_k, a)).$$

By the Prime Number Theorem [2, Chapter 22],

$$\log P_k = \sum_{p \le p_k} \log p = \theta(p_k) \sim p_k, \quad \text{as} \quad p_k \to \infty,$$

where $\theta(\cdot)$ is Chebyshev's function. So we could simplify our estimate of $\log n_k$ by replacing $\log P_k$ by p_k, but this introduces an undesirable error. Summarizing, we have the following

Estimate. *An estimate of the size of a solution of the inequality*

$$\phi(an+b) < \phi(an), \quad \textit{with} \quad \gcd(a,b) = 1,$$

is given by $\log n \approx \log P_k - \log a - \log(\gcd(P_k, a))$, *where* k *is such that* $\log p_k \approx e^{-\gamma}(a/\phi(a))^2$.

For $a = 30$, $b = 1$ this gives: $p_k \approx 2685$, $\log n \approx 2600$, $\log_{10} n \approx 1129$ while in Section 2 we found $k = 388$, $p_{388} = 2677$ and $\log_{10} n_{388} = 1125.643\ldots$.

Remark. Greg Martin [4] pointed out that when a is the product of several primes, $a/\phi(a)$ has order of magnitude $\log\log a$ and if such an a has D digits, then it follows from the analysis given above that the smallest solution to $\phi(an+b) < \phi(an)$ will have about $\exp(c(\log D)^2)$ digits, for some constant c. In particular, there is in general no polynomial-time algorithm for finding the least solution to this inequality, for the simple reason that just writing down the answer takes longer than any polynomial function of D!

4. A program for finding a solution of $\phi(an+b) < \phi(an)$, $\gcd(a,b) = 1$

We have written a GP/Pari program[2)] which finds a solution of (5), for given a and b, in the same way as we found the solution of $\phi(30n+1) < \phi(30n)$ in Section 2. This program has two steps:

Step 1. Find the smallest $k \in \mathbb{N}$ for which m_k as defined in (6) satisfies (7).

Step 2. For this m_k define $n_k := (m_k - b)/a$. Find a lower bound for the quotient $\phi(an_k)/(an_k)$ by dividing out all the prime factors of n_k up to some fixed bound B. Let

$$n_k := n'n''n''',$$

2) This program is available from the author upon request.

where
— n' consists of the prime factors of n_k which are in a,
— n'' consists of the (known) prime factors of n_k which are *not* in a, and which are not greater than B, and
— n''' consists of the (unknown) prime factors of n_k which are greater than B.
Then

$$\frac{\phi(an_k)}{an_k} = \frac{\phi(a)}{a}\frac{\phi(n'')}{n''}\frac{\phi(n''')}{n'''} > \frac{\phi(a)}{a}\frac{\phi(n'')}{n''}\left(1-\frac{1}{B}\right)^{\log n'''/\log B} =: R.$$

Now check whether $\phi(m_k)/m_k$, as computed in Step 1, satisfies

$$\frac{\phi(m_k)}{m_k} < R\frac{an_k}{an_k+b}.$$

If so, it follows that

$$\frac{\phi(an_k+b)}{m_k} < \frac{\phi(an_k)}{m_k},$$

so that n_k is a solution of (5). If not, continue with Step 1 to find the next smallest solution of (7). □

We have run this program for $b = 1$ and $a = 6, 30, 42$ with $B = p_{15000} = 163841$ and for $b = 1$, $a = 210$ with $B = p_{100000} = 1299709$, and compared the values of p_k and $\log_{10} n$, as estimated using Section 3, with the values of p_k and $\log_{10} n$ computed with this program. The results are given in Table 1.

	estimated		computed			
a $(b=1)$	p_k	$\log_{10} n$	k	p_k	$\log_{10} n$	$\tilde{k}$
$6 = 2\cdot 3$	157	57.796...	36	151	57.796...	35
$30 = 2\cdot 3\cdot 5$	2685	1129.072...	388	2677	1125.643...	385
$42 = 2\cdot 3\cdot 7$	971	397.081...	171	1019	421.063...	161
$210 = 2\cdot 3\cdot 5\cdot 7$	46476	20048.160...	4981	48413	20880.507...	4789

Table 1. Comparison of estimated (according to Section 3) and computed values of p_k and $\log_{10} n$, where the computed value of $n = (m_k - b)/a$, with $m_k = P_k/\gcd(P_k, a)$, satisfies $\phi(an+b) < \phi(an)$, $\gcd(a,b) = 1$. The last column lists the minimal value $\tilde{k}$ of k for which $\phi(m_k)/m_k < \phi(a)/a$.

The main reason for the difference between the estimated and computed values of p_k and $\log_{10} n$ is that the condition $m_k \equiv 1 \bmod a$ is only satisfied in about 1 in every $\phi(a)$ cases (on the assumption of the uniform distribution of the residues $m_k \bmod a$).

The last column of Table 1 lists the minimal value $\tilde{k}$ of k for which $\phi(m_k)/m_k < \phi(a)/a$, where $m_k = P_k/\gcd(P_k, a)$. Since this inequality is a *necessary condition* for any solution, we can use our computed solution and this $\tilde{k}$ to find the minimal solution. For example, for $a = 6$, $b = 1$, we have $\tilde{k} = 35$, so

$$m = p_3 p_4 \cdots p_{35} = 5 \cdot 7 \cdots 149$$

is the smallest product of consecutive primes ≥ 5 which satisfies the inequality $\phi(m)/m < 1/3$. In addition, for this m we have $m \equiv 1 \bmod 6$, $\phi(m) = 8.2531... \times 10^{55}$ and

$$\phi(m-1) = \phi(2 \cdot 3 \cdot 1381 \cdot 70140112179047 \cdot p39) = 8.2838... \times 10^{55},$$

where $p39$ is a prime of 39 decimal digits, easily computable from $m-1$ and the other given factors of $m-1$. So this m is also the *minimal* solution $\equiv 1 \bmod 6$ of the inequality $\phi(m) < \phi(m-1)$.

Table 1 lists sizes of estimated and computed solutions for various values of a, with $b = 1$. In fact, our program finds solutions for *all* those values of b for which $\gcd(a,b) = 1$, and since we have no indications that the residues $m_k \bmod a$ are *not* uniformly distributed, we expect the solutions for $b \neq 1$ to have about the same size as those given for $b = 1$ in Table 1.

References

[1] Batut, C., Bernardi, D., Cohen, H., Olivier, M., User's Guide to PARI-GP. http://www.parigp-home.de. PARI-GP was developed at Bordeaux by a team led by Henri Cohen. It is maintained now by Karim Belabas at the Université Paris-Sud Orsay with the help of many volunteer contributors.

[2] Hardy, G.H., Wright, E.M., An Introduction to the Theory of Numbers, fifth edition. Clarendon Press, Oxford 1995.

[3] Martin, G., The smallest solution of $\phi(30n+1) < \phi(30n)$ is .... Amer. Math. Monthly 106 (1999), 449–451.

[4] —, Private communication, January 24, 2001.

[5] Newman, D.J., Euler's ϕ function on arithmetic progressions. Amer. Math. Monthly 104 (1997), 256–257.