THE SMALLEST SOLUTION OF $\phi(30n+1) < \phi(30n)$ IS ...

GREG MARTIN

In a previous issue of the *American Mathematical Monthly*, D. J. Newman [1] showed that for any positive integers a, b, c, and d with $ad \neq bc$, there exist infinitely many positive integers n for which $\phi(an+b) < \phi(cn+d)$, where $\phi(m)$ is the familiar Euler totient function, the number of positive integers less than and relatively prime to m. In particular, it must be the case that $\phi(30n+1) < \phi(30n)$ infinitely often; however, Newman mentions that there are no solutions of this inequality with $n \leq 20{,}000{,}000$, and he states that a solution "is not explicitly available and it may be beyond the reach of any possible computers". The purpose of this note is to describe a method for computing solutions to inequalities of this type that avoids the need to factor large numbers. In particular, we explicitly compute the smallest number n satisfying $\phi(30n+1) < \phi(30n)$.

It is quite easy to compute values of n for which $\phi(30n+1)$ is relatively small by imposing many congruence conditions on n modulo primes, so that $30n+1$ is highly composite. However, the numbers n that arise in this way are quite large, having hundreds of digits. Computing $\phi(30n)$ exactly relies on the factorization of $30n$, which for integers of this size is not possible to find in a reasonable amount of time with today's computers and factoring algorithms. The idea underlying our method is to use partial knowledge of the factorization of a large number m to get an estimate for $\phi(m)$. We rely on the following claim:

Claim 1. *Let p_i denote the i^{th} prime number. Let $q = \prod_{i=r+1}^{r+s} p_i$ for some positive integers r and s, and let m be an integer that is not divisible by any of the primes $p_1, \dots, p_r$. Then:*
(a) *if $m \leq q$, then m has at most s distinct prime factors;*
(b) *if m has at most s distinct prime factors, then $\phi(m)/m \geq \phi(q)/q$.*

Proof. Let t be the number of distinct prime factors of m, and let the prime factors be $p_{i_1}, \dots, p_{i_t}$ with $i_1 < \cdots < i_t$. Since none of the primes $p_1, \dots, p_r$ divide m, it must be the case that $i_1 \geq r+1$, $i_2 \geq r+2$, and so on. So if we define $k = \prod_{j=r+1}^{r+t} p_j$, we see that $k \leq \prod_{j=1}^{t} p_{i_j} \leq m$. But $m \leq q$ by assumption, and so $k \leq q$, which can clearly only be the case if $t \leq s$. This proves part (a) of the claim.

As for part (b), we use the fact that the function $\phi(m)/m$ can be written as a product over primes dividing m:

$$\frac{\phi(m)}{m} = \prod_{p|m} \Big(1 - \frac{1}{p}\Big).$$

With k defined as above, notice that

$$\frac{\phi(m)}{m} = \prod_{j=1}^{t} \Big(1 - \frac{1}{p_{i_j}}\Big) \geq \prod_{j=1}^{t} \Big(1 - \frac{1}{p_{r+j}}\Big) = \frac{\phi(k)}{k},$$

1991 *Mathematics Subject Classification.* 11A25.

since $1 - 1/p$ is an increasing function of p. On the other hand, since $t \le s$ by assumption, we have

$$\frac{\phi(k)}{k} = \prod_{j=r+1}^{r+t} \Big(1 - \frac{1}{p_j}\Big) \ge \prod_{j=r+1}^{r+s} \Big(1 - \frac{1}{p_j}\Big) = \frac{\phi(q)}{q},$$

since each $1 - 1/p$ is less than 1. This proves part (b) of the claim.

We now proceed to find the smallest solution of $\phi(30n+1) < \phi(30n)$, though it must be pointed out that the method applies to any inequality of the form $\phi(an+b) < \phi(cn+d)$. Clearly $30n+1 \equiv 1 \pmod{30}$ no matter what n is. Also, if n is a solution of $\phi(30n+1) < \phi(30n)$, then we must have

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

since the inequality $\phi(ab) \le \phi(a)b$ holds for any numbers a and b. Thus it makes sense to look for numbers that satisfy both these conditions.

Claim 2. *Let $z = (p_4 p_5 \cdots p_{383}) p_{385} p_{388}$. Then z is the smallest positive integer satisfying $z \equiv 1 \pmod{30}$ and $\phi(z)/z < 4/15$.*

Proof. A computation shows that z is indeed congruent to 1 (mod 30) and that

$$\frac{\phi(z)}{z} = \bigg(\prod_{i=4}^{383} \Big(1 - \frac{1}{p_i}\Big)\bigg)\Big(1 - \frac{1}{p_{385}}\Big)\Big(1 - \frac{1}{p_{388}}\Big) = 0.2666117\dots < \frac{4}{15}.$$

Suppose m is an integer satisfying $m \equiv 1 \pmod{30}$ and $\phi(m)/m < 4/15$. Because of the congruence condition, m cannot be divisible by 2, 3, or 5. If we define $q_1 = \prod_{i=4}^{384} p_i$, then we can compute that $\phi(q_1)/q_1 = 0.26671\dots$, and so $\phi(q_1)/q_1 > \phi(m)/m$. Thus if we apply part (b) of Claim 1 with $r = 3$ and $s = 381$, we conclude that m must have more than 381 distinct prime factors.

Another computation reveals that the only numbers with at least 382 distinct prime factors that are less than z are the numbers $p_4 p_5 \cdots p_{382} m'$, where $m' \in \{p_{383}p_{384}p_{385},\ p_{383}p_{384}p_{386},\ p_{383}p_{385}p_{386},\ p_{383}p_{384}p_{387},\ p_{383}p_{385}p_{387},\ p_{384}p_{385}p_{386},\ p_{383}p_{384}p_{388},\ p_{383}p_{386}p_{387}\}$; and none of these numbers are congruent to 1 (mod 30).

Let us define $n = (z-1)/30$, which by Claim 2 is both an integer and the smallest possible solution of $\phi(30n+1) < \phi(30n)$. (Small wonder that we haven't stumbled across any solutions of this inequality—n has 1,116 digits!) It would be quite gracious of n to be an actual solution, and indeed it is.

First we show that $\phi(30n+1)/(30n+1) < \phi(30n)/30n$. We have already computed that

$$\frac{\phi(30n+1)}{30n+1} = \frac{\phi(z)}{z} = 0.2666117\dots. \tag{1}$$

It turns out that n is divisible by both 60 and $p_{4{,}874} = 47{,}279$, so let us define $n' = n/(60 p_{4{,}874})$. We can compute that n' is not divisible by any of the first 80,000 primes. This computation can be done most quickly by multiplying the primes together in blocks of 1,000, say, and computing the greatest common divisor of n' and the product. Since computing greatest common divisors is a very fast operation, checking that n' is not divisible by any of the first 80,000 primes takes only a few minutes on a workstation—much more reasonable than trying to factor a number with over a thousand digits.

Now define $q_2 = \prod_{i=80,001}^{80,186} p_i$. We compute that q_2 has 1,118 digits and so $q_2 > n > n'$. By using parts (a) and (b) of Claim 1 with $r = 80{,}000$ and $s = 186$, we see that $\phi(n')/n' \geq \phi(q_2)/q_2$. Therefore, since $\phi(ab) = \phi(a)\phi(b)$ when a and b are relatively prime, we compute that

$$\frac{\phi(30n)}{30n} = \frac{\phi(30 \cdot 60p_{4,874})}{30 \cdot 60p_{4,874}} \frac{\phi(n')}{n'} \geq \frac{4}{15}\Big(1 - \frac{1}{47,279}\Big)\frac{\phi(q_2)}{q_2} = 0.2666124\dots. \tag{2}$$

This shows that $\phi(30n+1)/(30n+1) < \phi(30n)/30n$, which doesn't quite imply that $\phi(30n+1) < \phi(30n)$, but only $\phi(30n+1) < \phi(30n)(1 + 1/(30n))$. However, the numbers computed in (1) and (2) differ in the sixth decimal place, while multiplying by $1 + 1/(30n)$ leaves a number unchanged until past the 1100th decimal place.

Therefore we have proved:

Theorem. *The smallest solution of* $\phi(30n+1) < \phi(30n)$ *is*

n=232,909,810,175,496,793,814,049,684,205,233,780,004,859,885,966,051,235,363,345,311,075,888,344,528,723,154,527,984,
260,176,895,854,182,634,802,907,109,271,610,432,287,652,976,907,467,574,362,400,134,090,318,355,962,121,476,785,712,
891,544,538,210,966,704,036,990,885,292,446,155,135,679,717,565,808,063,766,383,846,220,120,606,143,826,509,433,540,
250,085,111,624,970,464,541,380,934,486,375,688,208,918,750,640,674,629,942,465,499,369,036,578,640,331,759,035,979,
369,302,685,371,156,272,245,466,396,227,865,621,951,101,808,240,692,259,960,203,091,330,589,296,656,888,011,791,011,
416,062,631,565,320,593,772,287,118,913,728,608,997,901,791,216,356,108,665,476,306,080,740,121,528,236,888,680,120,
152,479,138,327,451,088,404,280,929,048,314,912,122,784,879,758,304,016,832,436,751,532,255,185,640,249,324,065,492,
491,511,072,521,585,980,547,438,748,689,307,159,363,481,233,965,802,331,725,033,663,862,618,957,168,974,043,547,448,
879,663,217,971,081,445,619,618,789,985,472,074,303,100,303,636,078,827,273,695,551,162,089,725,435,110,246,701,964,
021,045,849,081,811,604,427,331,227,553,783,590,821,510,091,607,567,178,842,569,576,699,548,038,217,673,171,895,383,
249,326,800,667,432,993,531,186,437,659,910,632,865,419,892,370,957,722,154,266,351,039,808,548,150,828,868,968,820,
675,198,820,381,135,523,646,361,202,383,915,218,571,017,801,463,011,491,108,784,343,253,284,393,511,650,254,506,597,
923,969,653,616,813,897,710,621,756,693,827,471,154,701,151,222,320,443,347,408,180,047,964,860.

I would like to thank Mike Bennett for verifying the above computations and to acknowledge the support of National Science Foundation grant DMS 9304580.

References

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

School of Mathematics, Institute for Advanced Study, Olden Lane, Princeton, NJ 08540, U.S.A.
gerg@math.ias.edu