Diophantine Equations Involving the Euler Totient Function

Number Theory Seminar, Dalhousie University

J.C. Saunders

Ben-Gurion University of the Negev

December 20, 2019

The Euler Totient Function

For a natural number n, the Euler totient function counts the number of positive integers up to n that are coprime to n and is denoted by $\varphi(n)$. For example, $\varphi(6) = 2$ because 1 and 5 are coprime to 6, but $2, 3, 4$ aren't.

For instance, if p is prime, then $\varphi(p) = p - 1$ and for a prime power p^e, then $\varphi(p^e) = p^e - p^{e-1} = p^{e-1}(p-1)$.

As well, the Euler totient function is multiplicative, that is, if $n, m \in \mathbb{N}$ are coprime, then $\varphi(nm) = \varphi(n)\varphi(m)$.

Properties of the Euler Totient Function

As a result, the Euler totient function of a number n can be expressed very nicely in terms of the prime factorisation of n. If

$$n = p_1^{e_1} p_2^{e_2} \cdots p_t^{e_t}$$

is the prime factorisation of n, then we have

$$\varphi(n) = p_1^{e_1-1}(p_1 - 1)p_2^{e_2-1}(p_2 - 1) \cdots p_t^{e_t-1}(p_t - 1).$$

If $p^2 \mid n$, then $p \mid \varphi(n)$. Conversely, if $p \mid \varphi(n)$, then either $p \mid n$ or there exists a prime q such that either $q \mid p - 1$.

Powers and the Euler totient function

Definition 1

A number $n \in \mathbb{N}$ is a powerful number if n does not have a prime factor to the power 1 in its prime factorisation. In other words, if

$$n = p_1^{e_1} p_2^{e_2} \cdots p_t^{e_t}$$

is the prime factorisation of n, then $e_i \geq 2$ for all $1 \leq i \leq t$.

Theorem 1 (Pollack (2014))

As $x \to \infty$, the number of $n \leq x$ for which $\varphi(n)$ is powerful is at most $x/L(x)^{1+o(1)}$ where

$$L(x) = \exp\left(\frac{\log x \cdot \log\log\log x}{\log\log x}\right)$$

Theorem 2 (Pollack and Pomerance (2019))

Let $V(x) := \#\{n \leq x : \text{ there exists } m \in \mathbb{N} \text{ such that } \varphi(m) = n^2\}$. *We have*

$$V(x) \leq x/(\log x)^{0.0063}$$

and

$$V(x) \gg x/(\log x \log\log x)^2.$$

Factorials and Powers

In 2010, Ford, Florian, and Pomerance proved that there exists $c > 0$ such that for all $k \in \mathbb{N}$ the Diophantine equation $\varphi(x) = k!$ has at least $(k!)^c$ solutions. In this way, the equation $\varphi(x) = k!$ has "many" solutions.

What about the equation $\varphi(ax^m) = r \cdot n!$ where $m \geq 2$ and $a \in \mathbb{N}$, $r \in \mathbb{Q}^+$ are fixed? We can also ask the same for $\varphi(r \cdot n!) = ax^m$.

The equation $\varphi(ax^m) = r \cdot n!$

Theorem 3 (S.)

Fix $a, b, c \in \mathbb{N}$ with $\gcd(b, c) = 1$. Then there are only finitely many solutions to $\varphi(ax^m) = \frac{b \cdot n!}{c}$ with $m \geq 2$ and these solutions satisfy $n \leq \max\{61, 3a, 3b, 3c\}$.

In particular, all of the integer solutions to $\varphi(x^m) = n!$ where $m \geq 2$ are $\varphi(1^m) = 1!$, $\varphi(2^2) = 2!$, $\varphi(3^2) = 3!$, $\varphi((3 \cdot 5)^2) = 5!$, $\varphi((3 \cdot 5 \cdot 7)^2) = 7!$, $\varphi((2^2 \cdot 3 \cdot 5 \cdot 7)^2) = 8!$, $\varphi((2^2 \cdot 3^2 \cdot 5 \cdot 7)^2) = 9!$, $\varphi((2^2 \cdot 3^2 \cdot 5 \cdot 7 \cdot 11)^2) = 11!$, and $\varphi((2^2 \cdot 3^2 \cdot 5 \cdot 7 \cdot 11 \cdot 13)^2) = 13!$.

The equation $\varphi(r \cdot n!) = ax^m$

Theorem 4 (S.)

Fix $a, b, c \in \mathbb{N}$ with $\gcd(a, b) = 1$. Then there are only finitely many solutions to $\varphi\left(\frac{a \cdot n!}{b}\right) = cx^m$ with $m \geq 2$ and these solutions satisfy $n \leq \max\{61, 3a, 3b, 3c\}$.

In particular, all of the integer solutions to $\varphi(n!) = x^m$, where $m \geq 2$ and $n \geq 1$, are $\varphi(1!) = 1^m$, $\varphi(2!) = 1^m$, $\varphi(4!) = 2^3$, $\varphi(5!) = 2^5$, $\varphi(8!) = (2^5 \cdot 3)^2$, $\varphi(9!) = (2^5 \cdot 3^2)^2$, $\varphi(11!) = (2^6 \cdot 3^2 \cdot 5)^2$, and $\varphi(13!) = (2^8 \cdot 3^3 \cdot 5)^2$.

Proposition 1 (S.)

Let $x, n, m, a, b, c \in \mathbb{N}$ with $m \geq 2$ and $\varphi(ax^m) = \frac{b \cdot n!}{c}$ and let p be a prime such that $p > a, b, c$. If $p \mid x$, then $p \leq n$. Conversely, if $p \leq n$, $p \nmid x$, then $p = 2$ and $n = 3, 5$, or 7.

Suppose $p \mid x$. Then $p^2 \mid ax^m$. Thus $p \mid \varphi(ax^m)$, so that $p \mid \frac{b \cdot n!}{c}$. Thus $p \mid n!$ so that $p \leq n$.

Suppose that $p \leq n$, $p \nmid x$. Let q be the greatest prime at most n. Then $b < p \leq q$ so that $q \mid \frac{b \cdot n!}{c}$. Then $q \mid \varphi(ax^m)$. Either $q \mid ax^m$ or there exists a prime $q' \mid ax^m$ such that $q \mid q' - 1$. Consider the latter case. Then we have $q < q' \mid x$ But then $q' \leq n$, contradicting our choice of q. Thus $q \mid x$. Using the same reasoning, we can deduce that the highest prime dividing x is q.

We have $p \mid \frac{b \cdot n!}{c} = \varphi(ax^m)$. If $p \mid ax^m$, then $p \mid x$, so we must have that there exists a prime, say p', such that $p \mid p' - 1$ and $p' \mid ax^m$ so that $p' \mid x$. Observe that $a, b, c < p < p' \leq q \leq n$. We can therefore deduce that for all $e \in \mathbb{N}$ $p^e \mid \frac{b \cdot n!}{c}$ if and only if $p^e \mid (q_1 - 1)(q_2 - 1) \cdots (q_r - 1)$ where $q_1 < q_2 < \ldots < q_r = q$ are all the primes dividing x that are greater than $a, b,$, and c. Thus for all $e \in \mathbb{N}$ $p^e \mid n!$ if and only if $p^e \mid (q_1 - 1)(q_2 - 1) \cdots (q_r - 1)$. Observe that $q_1 - 1 < q_2 - 1 < \ldots < q_r - 1 < n$ and that $p \nmid \frac{n!}{(q_1-1)\cdots(q_r-1)}$. Thus $q_1 - 1, \ldots, q_r - 1$ must contain all of the positive multiples of p up to n. We must therefore have that $p = q_i - 1$ for some $1 \leq i \leq r$, which can only hold if $p = 2$. So $q_1 - 1, \ldots, q_r - 1$ contains all of the positive even numbers less than n and $n = q_r = p_k$. Thus $n = 3, 5$, or 7.

Powerful Numbers

Proposition 2 (S.)

Let $x, y, \in \mathbb{N}$ satisfy $\varphi(x) = \varphi(y)$ and suppose that x and y are both powerful numbers. Then $x = y$.

Let $P(n)$ denote the largest prime factor dividing n. For $x, y \in \mathbb{N}$ both powerful with $\varphi(x) = \varphi(y)$ implies that $P(x) = P(y)$ with their exponents in the factorisation of x and y being equal. The result then follows by induction on the number of prime factors of x.

Lemma 1 (S.)

If $x, n, a, b, c \in \mathbb{N}$ with $n \geq 9$, $a, b, c \leq n/3$, and $\varphi(ax^2) = \frac{b \cdot n!}{c}$, then all of the primes in the interval $(n/3, n/2]$ are congruent to 2 (mod 3).

Notation 1

For a prime p and a natural number n, we write $p^e \parallel n$ if p^e is the highest power of p dividing n. In other words, if

$$n = p_1^{e_1} p_2^{e_2} \cdots p_t^{e_t}$$

is the prime factorisation of n, then $p_i^{e_i} \parallel n$ for all $1 \leq i \leq t$.

Let $p \in (n/3, n/2]$ be prime. By Proposition 1, we have $p \mid x$. Thus $p^{2e} \parallel ax^2$ for some $e \in \mathbb{N}$. Thus $p^{2e-1} \mid \varphi(ax^2)$. Notice that $p^2 \parallel \frac{c \cdot n!}{d}$. We can therefore deduce that there exists a prime $q \mid ax^2$ such that $p \mid q - 1$. Notice that $q \mid x$, and so, by Proposition 1, $q \leq n$. But since $n/3 < p$ we must therefore have that $2p = q - 1$. Since $n \geq 9$, we have $3 \nmid p, q$. Thus $p \equiv 2 \pmod 3$.

Proof of Theorem 3

Suppose that $\varphi(ax^m) = \frac{b \cdot n!}{c}$ where $m \geq 2$ and $\gcd(b, c) = 1$. Suppose that $n > \max\{61, 3a, 3b, 3c\}$.

Suppose that $m \geq 3$. Let p be the largest prime at most n. By Bertrand's Postulate, $n/2 < p$ and so $p^2 \nmid n!$. Also $p > a, b, c, d$. By Proposition 1, we have $p \mid x$, and so $p^3 \mid ax^m$. But then $p^2 \mid \varphi(ax^m) = \frac{b \cdot n!}{c}$ so that $p^2 \mid n!$, a contradiction.

Suppose that $m = 2$. By Lemma 1, all of the primes in the interval $(n/3, n/2]$ are congruent to 2 (mod 3). Bennett, Martin, O'Bryant, Rechnitzer showed in 2018 that for $x \geq 450$, we have

$$\frac{x}{2 \log x} < \pi(x; 3, 1) < \frac{x}{2 \log x} \left(1 + \frac{5}{2 \log x}\right).$$

where $(x; 3, 1)$ is the number of primes up to x congruent to 1 (mod 3), which we used to derive a contradiction.

Thus we must have $n \leq \max\{61, 3a, 3b, 3c\}$.

Special Case $\varphi(x^m) = n!$

For $m \geq 3$ we only have $\varphi(1^m) = 1!$ as a solution. For $n \geq 62$ there are no solutions.

For $26 \leq n \leq 56$, and $14 \leq n \leq 20$ there exists a prime in the interval $(n/3, n/2]$ that is congruent to 1 (mod 3) so we obtain no solutions here.

Assume $57 \leq n \leq 61$. By Proposition 1, $11 \mid x$. Suppose that $11^e \parallel x$. Then $11^{2e} \parallel x^2$. Also, $23 \mid x$ and 23 is the only prime up to n that is congruent to 1 (mod 11). Thus, $11^{2e-1+1} \parallel \varphi(x^2)$ or $11^{2e} \parallel \varphi(x^2)$. But $11^5 \parallel n!$, a contradiction since 5 is odd.

The rest of the cases are exhausted similarly.

Proof of Theorem 4

Suppose that $\varphi\left(\frac{a \cdot n!}{b}\right) = cx^m$ where $m \geq 2$ and $\gcd(a, b) = 1$ with $n > \max\{61, 3a, 3b, 3c\}$. We know there eixsts a prime $p \in (n/3, n/2]$ that is congruent to 1 (mod 3). Then $p^2 \parallel n!$, and so $p^2 \parallel \frac{a \cdot n!}{b}$. Thus $p \mid cx^m$, and so $p \mid x^m$. But then $p^2 \mid x^m$, and so $p^2 \mid cx^m$.

Therefore, there exists a prime $q \mid \frac{a \cdot n!}{b}$ such that $p \mid q - 1$. Since $q > p > a$, we have that $q \mid n!$, and so $q \leq n$. Since $p \in (n/3, n/2]$, we therefore have that $2p = q - 1$. But since $p \equiv 1 \pmod 3$, we have $3 \mid 2p + 1$, a contradiction.

Luca's and Stanica's Results

Let F_n be the nth term of the Fibonacci sequence with $F_0 = 0$ and $F_1 = 1$, and let L_n be the nth term of the Fibonacci sequence with $L_0 = 2$ and $L_1 = 1$

Theorem 5 (Luca, Stanica (2013))

Let $\mathcal{N} := \{n : \text{there exists } m \text{ such that } \varphi(F_n) = m!\}$ *and* $\mathcal{N}(x) := \mathcal{N} \cap [1, x]$. *Then*

$$\#\mathcal{N}(x) \ll \frac{x \log\log x}{\log x},$$

and the only primes in $\mathcal{N}$ *are* 2 *and* 3.

Theorem 6 (Luca, Stanica (2013))

The only solutions in nonnegative integers of the equation $\varphi(L_n) = 2^a 3^b$ *are*

$$(n, a, b) = (0, 0, 0), (1, 0, 0), (2, 1, 0), (3, 1, 0), (4, 1, 1), (6, 1, 1), (9, 2, 2).$$

Lucas sequences

Definition 2

Let $a, b, c \in \mathbb{N}$. A Lucas sequence of the first kind $(u_n)_n$ is defined by $u_0 = 0$, $u_1 = 1$, and $u_n = bu_{n-1} + cu_{n-2}$ for all $n \geq 2$. A Lucas sequence of the second kind $(v_n)_n$ is defined by $v_0 = 2$, $v_1 = b$, and $v_n = bv_{n-1} + cv_{n-2}$ for all $n \geq 2$.

The equation $\varphi(g_p) = m!$

Theorem 7 (S.)

Let $b^2 + 4c$ be prime with $b^2 + 4c > a$. Then there are at most finitely many primes p for which $\varphi(au_p)$ is a factorial. Moreover, such primes p are bounded above by

$$\max\left\{ ea^{1/2}\left(\frac{b+\sqrt{b^2+4c}}{2}\right), \frac{\frac{10}{9}\log(8\cdot(b^2+4c-1)!) - \log a + \frac{\log(b^2+4c)}{2}}{\log\left(\frac{b+\sqrt{b^2+4c}}{2}\right)} \right.$$

Powers of 2 and 3

Theorem 8 (S.)

The only solutions to $\varphi(v_n) = 2^x 3^y$ *are:*

1) For $b = 3$, $c = 1$*:*

$$(n, x, y) = (0, 0, 0), (1, 1, 0), (3, 2, 1), (4, 5, 1), (9, 6, 5).$$

2) For $b = 5$, $c = 1$*:*

$$(n, x, y) = (0, 0, 0), (1, 2, 0), (2, 0, 2), (3, 4, 3).$$

3) For $b = 7, c = 1$*:*

$$(n, x, y) = (0, 0, 0), (1, 1, 1), (2, 5, 0), (3, 5, 2), (6, 9, 4).$$

Lucas proved that for any prime p not dividing c we have that there exists $k \in \mathbb{N}$ such that $p \mid u_l$ if and only if $k \mid l$. Such a k is called the index of appearance of p. Denote the index of appearance of a prime p by $z(p)$.

Lucas also proved the following.

Lemma 2 (Lucas)

If $p \mid b^2 + 4c$, then $z(p) \mid p$. Let p be a prime other than $b^2 + 4c$ with $p \nmid c$. If $b^2 + 4c$ is a quadratic residue $\pmod p$, then $z(p) \mid p - 1$. If $b^2 + 4c$ is not a quadratic residue $\pmod p$, then $z(p) \mid p + 1$. Let $\alpha = \frac{b+\sqrt{b^2+4c}}{2a}$ and $\beta = \frac{\sqrt{b^2+4c}-b}{2a}$. Then

$$u_n = \frac{(\alpha^n - \beta^n)}{\sqrt{b^2 + 4c}}.$$

Lemma 3 (Rosser, Schoenfield)

Let c be the Euler-Mascheroni constant

$$c = \lim_{n\to\infty}\left(-\log n + \sum_{k=1}^{n}\frac{1}{k}\right) = 0.57721\ldots$$

Then for all $n \geq 3$, we have

$$n/\varphi(n) < e^c \log\log n + 5/(2\log\log n)$$

except when $n = 223092870 = 2\cdot 3\cdot 5\cdot 7\cdot 11\cdot 13\cdot 17\cdot 19\cdot 23$, in which case

$$n/\varphi(n) < e^c \log\log n + 2.50637/(\log\log n)$$

Let $\varphi(au_p) = m!$. Suppose that $m \geq b^2 + 4c$. Then $b^2 + 4c \mid \varphi(au_p)$ so either $b^2 + 4c \mid au_p$ or there exists a prime $q \mid g_p$ such that $q \equiv 1 \pmod{b^2 + 4c}$. In the former case, we thus have $b^2 + 4c \mid p$ and so $p = b^2 + 4c$. Thus assume the latter case. Since $b^2 + 4c \equiv 1 \pmod 4$ and $b^2 + 4c$ is prime, we have by quadratic reciprocity that $b^2 + 4c$ is a quadratic residue $\pmod q$. By Lemma 2, we thus have that $z(q) \mid \gcd(p, q-1)$. Since $g_1 = a < b^2 + 4c$, we must have that $z(q) = p$ and so $p \mid q - 1$. Thus $p \mid m!$ so that $p \leq m$. By Lemma 2, we have

$$a\alpha^p > au_p > \varphi(au_p) \geq p! > (p/e)^p.$$

Since $p \geq 2$, we have $p < ea^{1/2}\alpha$.

Now assume that $m < b^2 + 4c$ and $p \geq ea^{1/2}\alpha$. Thus, $p \geq 5$. We can work out that $au_5 = a(b^4 + 3b^2c + c^2)$ and so $u_p \geq u_5 \geq 5$. Thus,

$$\frac{au_p}{(b^2 + 4c - 1)!} \leq \frac{au_p}{m!} = \frac{au_p}{\varphi(au_p)}.$$

The right-hand side of the above inequality can be bounded with Lemma 3 and the result can be deduced.

Let $a = c = 1$.

Proposition 3

Let $c = 1$ and $b^2 + 4$ be prime and let $d = \nu_3(b)$ if $3 \mid b$ or $d = \nu_3(b^2 + 2)$ if $3 \nmid b$. Suppose that $\varphi(v_n) = 2^x 3^y$ for some $x, y, n \geq 0$ and $n = 2^e m$ where $e \geq 0$ and m is odd. Then $e \leq 2$ and at least one of the following conditions hold:

1) $n = 0, 1, 2, 3, 4, 6, 12$

2) n is a power of 3

3) there exists a prime $p > 3$ dividing n and for all such primes p, there eixst primes $q_1, \ldots, q_l$ such that $q_i = 2 \cdot 3^{b_{q_i}} + 1$ for some $b_{q_i} \in \mathbb{N}$ for all $1 \leq i \leq l$ with $v_{2^e p} = v_{2^e} q_1 \cdots q_l$, but $q_i \nmid v_{2^e}$ for all $1 \leq i \leq t$. Moreover, let q_1 be the smallest q_i. Then $b_{q_1} \leq 4d$.

Example: $b = 3$

If we substitute $b = 3$ into Proposition 3 and assume that $n > 12$, then we obtain that either n is a power of 3, or there exists a prime $p > 3$ such that $2^e p \mid n$, $q \mid v_{2^e p}$, but $q \nmid v_{2^e}$, where $e = 1, 2$, and $q = 7, 19$, or 163 since here $d = 1$.

We can deduce that $17 \mid \varphi(v_{27})$, eliminating the power of 3 possibility since $v_{n_1} \mid v_{n_2}$ if $n_1 \mid n_2$.

Suppose that $q = 163$. We can deduce that 13 is not a quadratic residue (mod 163), and so we have $p \mid 164$ and so $p = 41$. We can verify that $e = 1$. But $41 \mid \varphi(v_{82})$. Thus $\varphi(v_{82})$ does not have the form $2^x 3^y$ and so neither does $\varphi(v_n)$. The cases of $q = 7$ and 19 are similar.

I would like to thank my postdoc supervisor Dr. Daniel Berend for his encouragement and advice in pursuing this direction of research, to Dr. Florian Luca for helpful comments, and to the Azrieli Foundation for the award of an Azrieli International Postdoctoral Fellowship, which made this research possible.

Thanks for listening!

Any questions?