An interesting property of Euler's totient function

Moreno Borrallo, Juan

March 3, 2020

e-mail: juan.morenoborrallo@gmail.com

"Entia non sunt multiplicanda praeter necessitatem" (Ockam, W.)

"Dios no juega a los dados con el Universo" (Einstein, Albert)

"Te doy gracias, Padre, porque has ocultado estas cosas a los sabios y entendidos y se las has revelado a la gente sencilla" (Mt 11,25)

Abstract

In this brief paper it is proved that, for some positive integer n and some prime number $q < n$ such that $\gcd(q,n) = 1$, it holds that the set $S = \{x : 0 \leq x \leq n, \gcd(x, qn) = 1\}$ has no less than $\frac{\varphi(qn)}{2q}$ elements.

2010MSC: 11A99

1 Theorem

Let $\varphi(n) = n\prod_{p|n}\left(\frac{p-1}{p}\right)$ denote the Euler's totient function, which counts the number of elements of the set $\{x : 0 \leq x \leq n, \gcd(x,n) = 1\}$. In this paper it is proved the following

Theorem. Let it be some positive integer n, and some prime number $q < n$ such that $\gcd(q,n) = 1$. Then, it holds that $S = \{x : 0 \leq x \leq n, \gcd(x,qn) = 1\}$ has no less than $\frac{\varphi(qn)}{2q}$ elements.

1.1 Proof for n being some prime number

If $n = p$, where p is some prime number, applying the multiplicative properties of $\varphi(n)$ and taking into account that $\gcd(q,n) = 1$, then we have that

$$\frac{\varphi(qn)}{2q} = \frac{\varphi(n)\varphi(q)}{2q} = \frac{\varphi(n)}{2}\left(\frac{q-1}{q}\right) = \frac{\varphi(n)}{2}\left(1 - \frac{1}{q}\right)$$

Other hand, if p is some prime number and $q < p$, then $\lfloor\frac{p}{q}\rfloor$ numbers less than p are relatively prime to p and not relatively prime to qp; thus, we have that

$$\mid S \mid = \varphi(n) - \lfloor\frac{n}{q}\rfloor$$

Therefore, and noting that

$$\lfloor\frac{n}{q}\rfloor < \frac{n}{q}$$

We can affirm that

$$\mid S \mid > \varphi(n) - \frac{n}{q}$$

Operating, we have that

$$\frac{n}{q} = \frac{n}{q\varphi(n)}\varphi(n)$$

$$\varphi(n) - \frac{n}{q} = \varphi(n)\left(1 - \frac{n}{q\varphi(n)}\right)$$

$$\varphi(n)\left(1 - \frac{n}{q\varphi(n)}\right) = \frac{\varphi(n)}{2}\left(2 - \frac{2n}{q\varphi(n)}\right)$$

Thus, for proving the theorem for n being some prime number it suffices to show that

$$\frac{\varphi(n)}{2}\left(2-\frac{2n}{q\varphi(n)}\right)>\frac{\varphi(n)}{2}\left(1-\frac{1}{q}\right)$$

Operating,

$$\frac{\varphi(n)}{2}\left(2-\frac{2n}{q\varphi(n)}\right)-\frac{\varphi(n)}{2}\left(1-\frac{1}{q}\right)>0$$

$$\frac{\varphi(n)}{2}\left(\left(2-\frac{2n}{q\varphi(n)}\right)-\left(1-\frac{1}{q}\right)\right)>0$$

As $\frac{\varphi(n)}{2}>0$, then it follows that $\frac{\varphi(n)}{2}\left(\left(2-\frac{2n}{q\varphi(n)}\right)-\left(1-\frac{1}{q}\right)\right)>0$ when $\left(2-\frac{2n}{q\varphi(n)}\right)-\left(1-\frac{1}{q}\right)>0$; subsequently, we need to evaluate only this last expression.

Operating,

$$\left(2-\frac{2n}{q\varphi(n)}\right)-\left(1-\frac{1}{q}\right)=\frac{q+1}{q}-\frac{2n}{q\varphi(n)}=\left(\frac{q+1-\frac{2n}{\varphi(n)}}{q}\right)$$

As $q>0$, then it follows that $\frac{q+1-\frac{2n}{\varphi(n)}}{q}>0$ when $q+1-\frac{2n}{\varphi(n)}>0$; subsequently, we need to evaluate only this last expression.

As the minimum value of q is $q=2$, we could affirm that $q+1-\frac{2n}{\varphi(n)}>0$ for every value of q and n if $\frac{2n}{\varphi(n)}<3$.

As

$$\frac{2n}{\varphi(n)}=\frac{2n}{n-1}$$

And $\frac{2n}{n-1}<3$ for every n prime number greater than 3, we can affirm that, for every prime number $p>3$,

$$\frac{\varphi(pq)}{2q}<\varphi(p)-\frac{p}{q}<\mid S\mid$$

We can check manually that for $p = 2$ there exists no prime $q < p$ (and therefore, the theorem is not applicable); and for $p = 3$ there exists only one prime $q < p$ ($q = 2$). It could be checked that

$$\frac{\varphi(6)}{4} = \frac{1}{2}$$

$$\varphi(3) - \lfloor\frac{3}{2}\rfloor = 1$$

$$\frac{\varphi(6)}{4} < \varphi(3) - \lfloor\frac{3}{2}\rfloor = \mid S \mid$$

Subsequently, for every prime number $p \leq 3$, the theorem holds.

Therefore, for n being some prime number,

$$\mid S \mid > \frac{\varphi(qn)}{2q}$$

And the theorem is proved for this particular case.

1.2 Proof for n being some composite number

If n is some composite number, then less than $\lfloor\frac{n}{q}\rfloor$ numbers less than n are relatively prime to n and not relatively prime to qn; concretely,

$$\mid S \mid = \varphi(n) - \lfloor\frac{n}{q}\rfloor + \sum_{p \mid n}\left(\lfloor\frac{n}{qp}\rfloor\right)$$

Therefore, and noting that

$$\lfloor\frac{n}{q}\rfloor < \frac{n}{q}$$

$$\sum_{p \mid n}\left(\lfloor\frac{n}{qp}\rfloor\right) > \sum_{p \mid n}\left(\frac{n}{qp}\right) - \omega(n)$$

We can affirm that

$$\mid S \mid > \varphi(n) - \frac{n}{q} - \omega(n) + \sum_{p \mid n}\left(\frac{n}{qp}\right)$$

Where each $\frac{n}{qp}$ counts the common multiples of q and each prime factor of n, which are double excluded by $\varphi(n)$ and $\frac{n}{q}$, and therefore need to be added once; and $\omega(n)$ counts the number of distinct prime divisors of n, which need to be substracted when transforming $\lfloor \frac{n}{qp} \rfloor$ into $\frac{n}{qp}$ to avoid overestimation of the minimum value of $\mid S \mid$.

Operating, we get that

$$\mid S \mid > \varphi(n) - \frac{n}{q}\left(1 - \sum_{p|n}\left(\frac{1}{p}\right)\right) - \omega(n)$$

For $\omega(n) > 1$, it is easy to show that

$$\prod_{p|n}\left(\frac{p-1}{p}\right) > 1 - \sum_{p|n}\left(\frac{1}{p}\right)$$

Therefore,

$$\mid S \mid > \varphi(n) - \frac{n}{q}\left(\prod_{p|n}\left(\frac{p-1}{p}\right)\right) - \omega(n)$$

As $\varphi(n) = n\prod_{p|n}\left(\frac{p-1}{p}\right)$, we have that

$$\mid S \mid > \varphi(n) - \frac{\varphi(n)}{q} - \omega(n)$$

$$\mid S \mid > \varphi(n)\left(1 - \frac{1}{q}\right) - \omega(n)$$

As before, we have that

$$\frac{\varphi(qn)}{2q} = \frac{\varphi(n)}{2}\left(1 - \frac{1}{q}\right)$$

Thus, for proving the theorem for n being some composite number it suffices to show that

$$\varphi(n)\left(1 - \frac{1}{q}\right) - \omega(n) > \frac{\varphi(n)}{2}\left(1 - \frac{1}{q}\right)$$

Operating,

$$\varphi(n)\left(1 - \frac{1}{q}\right) - \omega(n) - \frac{\varphi(n)}{2}\left(1 - \frac{1}{q}\right) > 0$$

$$\frac{\varphi(n)}{2}\left(1 - \frac{1}{q}\right) - \omega(n) > 0$$

As $\frac{\varphi(qn)}{2q} = \frac{\varphi(n)}{2}\left(1-\frac{1}{q}\right)$, subtituting,

$$\frac{\varphi(qn)}{2q} - \omega(n) > 0$$

$$\frac{\varphi(qn)}{2q} > \omega(n)$$

By the definition of $\varphi(n)$, and as $\gcd(q,n)=1$, we have that

$$\frac{\varphi(qn)}{2q} = \frac{\varphi(n)\varphi(q)}{2q} = n\left(\prod_{p|n}\left(\frac{p-1}{p}\right)\right)\left(\frac{q-1}{2q}\right)$$

If n is composite, then $n = p_1^{\alpha_1}p_2^{\alpha_2}...p_n^{\alpha_n}$. Thus, we can affirm that

$$\frac{\varphi(qn)}{2q} = \left(p_1^{\alpha_1-1}p_2^{\alpha_2-1}...p_n^{\alpha_n-1}\right)\left(\prod_{p|n}(p-1)\right)\left(\frac{q-1}{2q}\right)$$

It can bee seen that an increase of one unit in $\omega(n)$ implies an increase of $p_k^{\alpha_k}(p-1)$ in $\frac{\varphi(qn)}{2q}$.

Thus, as $p_k^{\alpha_k}(p-1) > 1$ for every prime number, it follows that the rate of growth of $\omega(n)$ is much lesser than the rate of growth of $\frac{\varphi(qn)}{2q}$.

Looking for the minimum values of $\omega(n)$ and $\frac{\varphi(qn)}{2q}$ for n composite, we find only two cases where the inequality $\frac{\varphi(qn)}{2q} > \omega(n)$ does not hold:

- $n=6$ and $q=5$, as $\frac{\varphi(30)}{10} < \omega(6)$
- $n=15$ and $q=2$, as $\frac{\varphi(30)}{4} = \omega(15)$

However, checking manually, we find that

$$\frac{\varphi(30)}{4} = 2$$

$$\varphi(6) - \lfloor\frac{6}{5}\rfloor + \sum_{p|6}\left(\lfloor\frac{6}{2p}\rfloor\right) = 3$$

$$\varphi(15) - \lfloor\frac{15}{2}\rfloor + \sum_{p|15}\left(\lfloor\frac{15}{2p}\rfloor\right) = 4$$

Subsequently,

$$\frac{\varphi\left(30\right)}{4} < \varphi\left(6\right) - \lfloor\frac{6}{5}\rfloor + \sum_{p|6}\left(\lfloor\frac{6}{2p}\rfloor\right) =\mid S\mid$$

$$\frac{\varphi\left(30\right)}{4} < \varphi\left(15\right) - \lfloor\frac{15}{2}\rfloor + \sum_{p|15} =\mid S\mid$$

Therefore, for this two particular cases the theorem holds.

As the rate of growth of $\omega\left(n\right)$ is much lesser than the rate of growth of $\frac{\varphi(qn)}{2q}$, then we can affirm that the inequality $\frac{\varphi(qn)}{2q} > \omega\left(n\right)$ holds in the rest of the cases.

Therefore, for n being some composite number,

$$\mid S\mid > \frac{\varphi\left(qn\right)}{2q}$$

And the theorem is proved.