An interesting property of Euler's totient function

Moreno Borrallo, Juan

March 11, 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, and $q < p$, then to get the elements of S we need to substract from $\varphi(p)$ those numbers that are multiples of q; as there are only $\lfloor\frac{p}{q}\rfloor$ numbers less than p are relatively prime to p and not relatively prime to qp, we have that

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

As $q \nmid p$, we can affirm that

$$\lfloor\frac{p}{q}\rfloor \leq \frac{p-1}{q} = \frac{\varphi(p)}{q}$$

And subsequently we get that

$$\mid S \mid \geq \varphi(p) - \frac{\varphi(p)}{q}$$

Operating, we get that

$$\mid S \mid \geq \varphi(p)\left(1 - \frac{1}{q}\right)$$

$$\mid S \mid \geq \varphi(p)\left(\frac{q-1}{q}\right)$$

As $\gcd(q,p) = 1$, and applying the multiplicative properties of $\varphi(n)$, we get that

$$\varphi(p)\left(\frac{q-1}{q}\right) = \frac{\varphi(p)\,\varphi(q)}{q} = \frac{\varphi(qn)}{q}$$

Therefore, for n being some prime number,

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

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, the multiples of q and each prime factor of n could be double-excluded by $\varphi\left(n\right)$ and $\frac{n}{q}$, and therefore need to be added once if necessary. Therefore,

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

Where $\sum_{p|n} \left(\lfloor \frac{n}{qp} \rfloor \right)$ counts the common multiples of q and each prime factor of n, which already are double excluded by $\varphi\left(n\right)$ and $\frac{n}{q}$.

We have that

$$\lfloor \frac{n}{q} \rfloor \leq \frac{n-1}{q}$$

$$\sum_{p|n} \left(\lfloor \frac{n}{qp} \rfloor \right) \geq \sum_{p|n} \left(\frac{n-\left(q-1\right)p}{qp} \right)$$

As

$$\sum_{p|n} \left(\frac{n-\left(q-1\right)p}{qp} \right) = \sum_{p|n} \left(\frac{n}{qp} - 1 + \frac{1}{q} \right)$$

Thus, we can affirm that

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

Where $\omega\left(n\right)$ counts the number of distinct prime divisors of n.

Operating, we get that

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

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

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

Therefore,

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

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

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

Operating,

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

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

As $\gcd(q,n) = 1$, and applying the multiplicative properties of $\varphi(n)$, we have that

$$\varphi(qn) = \varphi(n)\varphi(q)$$

Thus,

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

As the rate of growth of $\omega(n)$ is much lesser than the rate of growth of $\frac{\varphi(n)}{2}$, then we can affirm that, excepting the cases $n = 6$ and $n = 15$, which can be verified manually to fulfill the theorem,

$$\omega(n) < \frac{\varphi(n)}{2}$$

Then we have that

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

And subsequently

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

Therefore, for n being some composite number,

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

And the theorem is proved.