Euler's Phi Function and Theorem

Ben Hughes

In this paper I hope to give a brief overview of the number theory involved with Euler's Phi-Function and Theorem, along with several important results. The mathematics involved has many uses in solving systems of congruence, has an inherent relationship to prime numbers, and offers different tools to prove other theorems, such as the Chinese Remainder Theorem. Applications extend into cryptography, such as RSA encryption.

1 Preliminaries

In this section I will provide a basic outline of content required to understand this topic; many proofs and examples will be omitted, many of which are more appropriate to an introductory course in number theory or modern algebra.

Definition 1.0.1. *For $a, b \in \mathbb{Z}$ we say that a divides b if and only if there exists a $c \in \mathbb{Z}$ such that $ac = b$. If a divides b, then we write $a|b$, else we write $a \nmid b$; Similarly we say a is a divisor of b and b is a multiple of a.*

Definition 1.0.2. *An integer p is prime if $p > 1$ and $\pm 1, \pm p$ are the only divisors of p. Any positive integer which is not prime or one is a composite number.*

Lemma 1.0.1 (Euclid's Lemma)**.** *If p is prime and $p|ab$ then either $p|a$ or $p|b$.*

Theorem 1.1 (Unique Factorization Theorem (UFT))**.** *For all $n \in \mathbb{Z}^+$, n is either 1 or $n = p_1^{m_1} p_2^{m_2} \cdots p_r^{m_r}$, where p_i is prime and $m_i \in \mathbb{Z}^+$. What's more, this expression is unique up to order, and the standard (or canonical) form of n can be written when $p_1 < p_2 < ... < p_r$.*

Theorem 1.2 (Quotient Remainder Theorem)**.** *For integers x and y where $y > 0$ there exists unique integers q and r such that*

$$x = yq + r, 0 \leq r < y$$

By way of example if x = 61 and y = 8 then 61 = 8(7) + 5.

Definition 1.2.1. *We define the greatest common denominator d of two integers a and b (where at least one of them is nonzero) as follows:*
(a) $d \in \mathbb{Z}^+$
(b) $d|a$ and $d|b$
(c) if $c|a$ and $c|b$ then $c|d$
What's more, d can be written as a linear combination of a and b, namely

gcd(a,b) = gcd (b,a) = d = am + bn, $m, n \in \mathbb{Z}$. Lastly, d is smallest positive integer which may be written in this form.

Often times when the context is clear the gcd of two numbers a and b may be written either as gcd(a,b) or simply (a,b). Here we will use them interchangeably.

To give one example, gcd(27, 18) = 9, since $27 = 3^3$ and $18 = 3^2 \cdot 2$. One other way of thinking about the gcd of two numbers is as follows; suppose one knows the canonical prime factorizations of a and b, we can rewrite them so that $a = p_1^{m_1} p_2^{m_2} \cdots p_r^{m_r}$ and $b = p_1^{n_1} p_2^{n_2} \cdots p_r^{n_r}$, where $m_i, n_i \in \mathbb{Z}^+ \cup \{0\}$. Then
gcd(a, b) $= p_1^{min(m_1,n_1)} p_2^{min(m_2,n_2)} \cdots p_r^{min(m_r,n_r)}$.
Applying this to our example we do indeed have that gcd(27, 18) $= 2^{min(0,1)} 3^{min(3,2)} = 9$.

Definition 1.2.2. *For integers a and b, we say that a and b are relatively prime if (a,b) = 1.*

Definition 1.2.3. *The least common multiple m or lcm of two integers a and b (where at least one of them is nonzero) is defined as follows:*
(a) $m \in \mathbb{Z}^+$
(b) $a|m$ *and* $b|m$
(c) if $a|c$ *and* $b|c$ *then* $c|m$

Written either as lcm(a,b) or [a,b], the lcm may be thought of as taking the max instead of the min as in our previous example. So lcm(27, 18) $= 2^{max(0,1)} \cdot 3^{max(3,2)} = 2 \cdot 3^3 = 54$.
We note here without formal proof that for two nonzero integers a and b

$$ab = gcd(a, b) \cdot lcm(a, b)$$

Definition 1.2.4. *For $n \in \mathbb{Z}^+ \backslash \{1\}$, integers x and y are congruent modulo n if and only if $n|x - y$. This may be written as:*

$$x \equiv y \pmod{n}$$

For example, $8 \equiv 3 \pmod 5$ and $4 \equiv 49 \pmod 9$.

Theorem 1.3 (Properties of Modulo Congruence)**.** *Let a, b, c, d, x, $\in \mathbb{Z}$. Then*

(a) Congruence modulo n is an equivalence relation on $\mathbb{Z}$, so
(i) $a \equiv a \pmod n$
(ii) $a \equiv b \pmod n \Leftrightarrow b \equiv a \pmod n$
(iii) if $a \equiv b \pmod n$ *and* $b \equiv c \pmod n$ *then* $a \equiv c \pmod n$

(b) $a \equiv b \pmod n \Rightarrow a + x \equiv b + x \pmod n$ *and* $ax \equiv bx \pmod n$

(c) $a \equiv b \pmod n$ *and* $c \equiv d \pmod n \Rightarrow$
$a + c \equiv b + d \pmod n$ *and* $ac \equiv bd \pmod n$

(d) if $xa \equiv xb \pmod n$ *and (x,n) = 1 then* $a \equiv b \pmod n$

Theorem 1.4 (Inclusion-Exclusion Principle). † *Let $A_1, A_2, ..., A_n$ be finite sets, then*

$$|\bigcup_{i=1}^{n} A_i| = \sum_{i=1}^{n} |A_i| - \sum_{1\le i<j\le n} |A_i \cap A_j| + \sum_{1\le i<j<k\le n} |A_i \cap A_j \cap A_k| - ... + (-1)^{n-1} |\bigcup_{i=1}^{n} A_i|$$

For example, consider the finite sets A, B, and C. We have from the Inclusion-Exclusion Principle that

$$|A \cup B \cup C| = |A| + |B| + |C| - |A \cap B| - |B \cap C| - |A \cap C| + |A \cap B \cap C|$$

Lastly, we will establish some Lemmas which will prove useful later on.

Lemma 1.4.1. *$a \equiv b \pmod n$ if and only if gcd(a,n) = gcd(b,n). Similarly, for integers $q, r \in \mathbb{Z}$, gcd(qn + r, n) = gcd(r, n).*

Proof. $a \equiv b \pmod n \Leftrightarrow n|a-b \Leftrightarrow a = b + nq, q \in \mathbb{Z}$. Now this reduces the problem to showing that (b + nq, n) = (b, n).
gcd(b + nq, n) = (b + nq)l + nm $(l, m \in \mathbb{Z})$ = bl + n(m + ql). Since gcd(b,n) divides b and n gcd(b,n)|gcd(a,n).
Likewise, gcd(b,n) = bk + nj $(k, j \in \mathbb{Z})$ = bk + nj + nqk - nqk = (b + nq)k + n(j - qk). Since gcd(a, n) divides b + nq and n gcd(a,n)|gcd(b,n).
But before we can conclude what we sent out to prove, another short proof: $\forall x, y \in \mathbb{Z}^+$, if $x|y$ and $y|x$, then xk = y and yq = x, for some $k, q \in \mathbb{Z}^+$ (otherwise the LHS would be negative or zero if $k, q \in \mathbb{Z}\backslash\mathbb{Z}^+$). So y = $\frac{x}{q}$ and xk = $\frac{x}{q}$ ⇒ xkq = x ⇒ kq = 1, so k = q = 1. So x = y.
Therefore we can conclude gcd(a,n) = gcd(b + nq, n) = gcd(b,n) (since the gcd is always positive). □

Lemma 1.4.2. *For integers a, b, and c, gcd(a, bc) = 1 ⇔ gcd(a,b) = gcd(a,c) = 1.*

Proof. ("⇒"): Assume (a, bc) = 1 and let d = (a, b); by definition $d|a$ and $d|b$, so $d|bc$. Therefore d ≤ (a, bc) = 1, and since d must be a positive integer d = 1. The argument is similar to prove (a, c) = 1.
("⇐"): Assume (a, b) = (b, c) = 1. By way of contradiction assume (a, bc) = d > 1. Then $\exists p \in \mathbb{Z}^+$ such that p is prime and $p|d$ (by UFT) which implies that since $p|bc$ and $p|a$. By Euclid's Lemma $p|b$ or $p|c$. If $p|b$ then (a,b) ≥ p, a contradiction. Similarly we get a contradiction if $p|c$. Therefore (a, bc) = 1. □

†In general, if $f : S \to \mathbb{R}$ where S is an algebra of sets (a ring of sets with unit) and f is an additive function then this principle may be similarly applied. Here, our f is the cardinality function.

2 Euler's Phi-Function and Product Formula

Euler's Phi-Function (also known as indicator or totient function), denoted $\varphi(n)$ for some n $\in \mathbb{N}$ is a mapping $\varphi : \mathbb{N} \to \mathbb{N}$ associating n with the number of positive integers which are relatively prime to n, i.e. the cardinality of the set S where
S = $\{m \in \mathbb{N} | 1 \leq m < n; gcd(m, n) = 1\}$.
For example, if n = 24, the numbers 1,5,7,11,13,17,19,23 are all relatively prime and less than 24, so $\varphi(24) = 8$.
$\varphi(1) = 1$, $\varphi(2) = 1$, $\varphi(3) = 2$, $\varphi(5) = 4$, $\varphi(8) = 4$, $\varphi(11) = 10$, ...
Immediately we might notice a special relationship between any prime number p and $\varphi(p)$, since by definition p is relatively prime to all positive integers less than p. Therefore,

$$\text{If p is prime, then } \varphi(p) = p - 1$$

Indeed, this relation goes both ways, since if n is a composite number, then there must exist some divisor m such that 1 < m < n, so m and n are not relatively prime and therefore $\varphi(n) \leq n - 2$.
We would like to extend this finding to p^k, as then we might be able to use the Prime Factorization Theorem to generalize for all n. This is given in the following theorem.

Theorem 2.1. *If p is prime and $k \in \mathbb{N}$, then*

$$\varphi(p^k) = p^k - p^{k-1} = p^k\left(1 - \frac{1}{p}\right)$$

Proof. For some positive integer $1 < n \leq p^k$ - 1, gcd(n, p^k) = 1 if and only if p$\nmid$n, i.e. n's prime factorization does not include some power of p. However, since $p|p$, $p|2p$, ..., $(p^{k-1} - 1)p|p^k$, there are exactly p^{k-1} numbers *not* relatively prime to p^k, and thus the statement holds (since the rest are relatively prime, we have $p^k - p^{k-1}$). □

One tactic to generalize for all n is to show that φ is a multiplicative function, i.e. $\varphi(m)\varphi(n) = \varphi(mn)$ when gcd(m,n) = 1, and then to induct on i, where $n = p_1^{k_1}p_2^{k_2}\cdots p_i^{k_i}$. A more direct route is to argue by the Principle of Inclusion-Exclusion by finding an expression for all the integers that are not relatively prime to n and subtracting that from n. Here I will take the latter approach, and prove afterwards that φ is indeed multiplicative.

Theorem 2.2 (Euler's Product Formula)**.** $\varphi(1) = 1$. *For $n \in \mathbb{N}$, $n > 1$ and $n = p_1^{k_1}p_2^{k_2}\cdots p_r^{k_r}$:*

$$\begin{aligned}
\varphi(n) &= \left(p_1^{k_1} - p_1^{k_1-1}\right)\left(p_2^{k_2} - p_2^{k_2-1}\right)\cdots\left(p_i^{k_i} - p_r^{k_r-1}\right) \\
&= n\left(1 - \frac{1}{p_1}\right)\left(1 - \frac{1}{p_2}\right)\cdots\left(1 - \frac{1}{p_r}\right) \\
&= n\prod_{i=1}^{r}\left(1 - \frac{1}{p_i}\right)
\end{aligned}$$

Proof. It's trivial that $\varphi(1) = 1$, so we assume n > 1, and $n = p_1^{k_1} p_2^{k_2} \cdots p_r^{k_r}$. We are looking for the sum of integers less than n which are NOT relatively prime to n, i.e. the complement to subtract from n. Let $P = p_1 p_2 \cdots p_j$. It is clear that gcd(m,n) > 1 if and only if gcd(m, P) > 1; likewise, for some p which satisfies this condition, there are exactly (n/p) multiples of p which are less than n, which are $1 \cdot p, 2 \cdot p, ..., (n/p) \cdot p$. So adding how many multiples of $p_i \in \{p_1, p_2, ..., p_r\}$ for every p_i, we obtain

$$\frac{n}{p_1} + \frac{n}{p_2} + ... + \frac{n}{p_j} = \sum_{i=1}^{r} \frac{n}{p_i}$$

However, consider the sets of integers less than n which are divisible by $p_{i_1}, p_{i_2} \in \{p_1, p_2, ..., p_r\}$ - we are clearly over-counting. So we subtract $\sum_{1 \le i_1 < i_2 \le j} \frac{n}{p_{i1} p_{i2}}$. However, now we must add back the number of integers divisible by three primes and so on, so by the principle of inclusion-exclusion we have:

$$\begin{aligned}
\varphi(n) &= n - \left(\sum_{1 \le i_1 \le r} \frac{n}{p_i} + \sum_{1 \le i_1 < i_2 \le r} \frac{n}{p_{i_1} p_{i_2}} + ... + (-1)^{r+1} \frac{n}{p_1 p_2 \cdots p_r} \right) \\
&= n \left(1 - \sum_{1 \le i_1 \le r} \frac{1}{p_i} + \sum_{1 \le i_1 < i_2 \le r} \frac{1}{p_{i_1} p_{i_2}} + ... + (-1)^{r+1} \frac{1}{p_1 p_2 \cdots p_r} \right) \\
&= n \left(1 - \frac{1}{p_1} \right) \left(1 - \frac{1}{p_2} \right) \cdots \left(1 - \frac{1}{p_r} \right) \\
&= n \prod_{i=1}^{r} \left(1 - \frac{1}{p_i} \right)
\end{aligned}$$

□

Example. Consider $\varphi(1078)$. $1078 = 2 \cdot 7^2 \cdot 11$. Therefore,

$$\varphi(1078) = 1078 \left(1 - \frac{1}{2} \right) \left(1 - \frac{1}{7} \right) \left(1 - \frac{1}{11} \right) = 1708 \cdot \frac{1}{2} \cdot \frac{6}{7} \cdot \frac{10}{11} = 420.$$

Also notice that $\varphi(49)\varphi(22) = 42 \cdot 10 = \varphi(49 \cdot 22) = \varphi(1078)$, which leads us to the following corollary.

Corollary 2.2.1. *φ is a multiplicative function.*

Proof. We need to show that $\varphi(m)\varphi(n) = \varphi(mn)$, where $m = p_1^{a_1} \cdots p_r^{a_r}$, $n = q_1^{b_1} \cdots q_t^{b_t}$ and gcd(m,n) = 1 (i.e. they do not share a common prime factor). We have

$$\begin{aligned}
\varphi(mn) &= mn \left(1 - \frac{1}{p_1} \right) \cdots \left(1 - \frac{1}{p_r} \right) \left(1 - \frac{1}{q_1} \right) \cdots \left(1 - \frac{1}{q_t} \right) \\
&= m \left(1 - \frac{1}{p_1} \right) \cdots \left(1 - \frac{1}{p_r} \right) n \left(1 - \frac{1}{q_1} \right) \cdots \left(1 - \frac{1}{q_t} \right)
\end{aligned}$$

$$= m \prod_{i=1}^{r} \left(1 - \frac{1}{p_i}\right) n \prod_{i=1}^{t} \left(1 - \frac{1}{q_i}\right) = \varphi(m)\varphi(n)$$

□

It's essential that gcd(m,n) = 1; $\varphi(8)\varphi(6) \neq \varphi(42)$, because the formula requires that there is only one instance of each prime in the prime factorization of any number.

Before moving on to Euler's Theorem we shall first make note of a few interesting properties of φ.

Theorem 2.3.

(a) For positive integer n > 2 $\varphi(n)$ is even
(b) (Gauss)

$$n = \sum_{d|n} \varphi(d)$$

(c) For positive integers m and n $\varphi(m)\varphi(n) = \varphi(gcd(m,n))\varphi(lcm(m,n))$

Proof. (a) Either n is a power of two or it is not.
Case I: n = 2^k, $k \geq 2$. Then $\varphi(n) = \varphi(2^k) = 2^k\left(1 - \frac{1}{2}\right) = 2^{k-1}$, and clearly $2|(2^{k-1})$.
Case II: n is not a power of two, so by the UFT n must be divisible by some odd prime p such that n = $p^k m$, where $m \in \mathbb{Z}^+$ and (p^k, m) = 1. Then $\varphi(n) = \varphi(p^k m) = \varphi(p^k)\varphi(n) = p^{k-1}(p-1)\varphi(m)$, and since p was odd $2|(p-1)$ so $2|n$.

(b) For all positive divisors of n, we put the numbers 1,2, ..., n into the distinct classes $S_d = \{m | 1 \leq m \leq n, gcd(m,n) = 1\}$. Note that each number is uniquely placed in a distinct class. Now gcd(m, n) = d if and only if gcd(m/d, n/d) = 1 (otherwise it wouldn't be the *greatest* common denominator), so $m \in S_d$ if and only if $m/d \leq n/d$ (since $m \leq n$ implies $m/d \leq n/d$) and m/d and n/d must be relatively prime. In other words, $|S_d| = \varphi(n/d)$, and since every integer $a \in \{1, 2, 3, ..., n\}$ lies uniquely in some class we have

$$n = \sum_{d|n} \varphi(\frac{n}{d})$$

Since as d goes from 1 to n $\frac{n}{d}$ goes from n to 1, which tells us that the above expression is equal to

$$n = \sum_{d|n} \varphi(d)$$

(c) When gcd(m, n) = 1 we have lcm(m, n) = mn since $gcd(m,n) \cdot lcm(m,n) = mn$, and $\varphi(m)\varphi(n) = \varphi(mn)$ is true since φ is multiplicative.
Assume then gcd(m,n) = d > 1. $d|m$ and gcd(d, m) = d so m/d $\in \mathbb{Z}^+$ and gcd(d, m/d) = 1. Lastly note that gcd(m/d, n) = 1 (since by definition they no longer have *any* common divisor greater than 1) so we have

$$\varphi(m)\varphi(n) = \varphi\left(\frac{m}{gcd(m,n)} \cdot gcd(m,n)\right)\varphi(n) = \varphi\left(\frac{m}{gcd(m,n)}\right)\varphi(gcd(m,n))\varphi(n)$$

$$= \varphi(gcd(m,n))\varphi(lcm(m,n,)) \Rightarrow \varphi\left(\frac{m}{gcd(m,n)}\right)\varphi(n) = \varphi(lcm(m,n))$$
$$\Rightarrow \varphi\left(\frac{mn}{gcd(m,n)}\right) = \varphi(lcm(m,n))$$

Which is indeed true since $gcd(m,n) \cdot lcm(m,n) = mn \Rightarrow \frac{mn}{gcd(m,n)} = lcm(m,n)$

□

3 Euler's Theorem

Now we are equipped to tackle Euler's Theorem:
Theorem 3.1. *For a,n ∈ $\mathbb{Z}^+$, if n ≥ 1 and gcd(a,n) = 1 then*

$$a^{\varphi(n)} \equiv 1 \pmod{n}$$

Proof. First consider the set S = $\{a_1, a_2, ..., a_{\varphi(n)}\}$, where $\forall a_i \in S$ $1 \leq a_i < n$ and gcd(a_i, n) = 1. The elements in set aS = $\{aa_1, aa_2, ..., aa_{\varphi(n)}\}$ are also all relatively prime to n, as we know from Lemma 1.4.2 that because gcd(a,n) = 1 and gcd(a_i, n) = 1 for all i that gcd(aa_i,n) = 1. Likewise, there exists a unique b, where 0 ≤ b < n such that $aa_i \equiv b \pmod{n}$. Then gcd(b, n) = gcd(aa_i,n) = 1 and b = a_i', $a_i' \in S$. Therefore the elements of aS are congruent to the elements of S in some order. So we have

$$(aa_1)(aa_2)\cdots(aa_{\varphi(n)}) \equiv a_1a_2\cdots a_{\varphi(n)} \pmod{n}$$
$$a^{\varphi(n)}(a_1a_2\cdots a_{\varphi(n)}) \equiv a_1a_2\cdots a_{\varphi(n)} \pmod{n}$$

Since gcd(a_i, n) = 1 for every i, gcd($a_1a_2\cdots a_{\varphi(n)}$, n) = 1, so we can divide their product from both sides, leaving us with $a^{\varphi(n)} \equiv 1 \pmod{n}$. □

As an immediate corollary, we have
Corollary 3.1.1 (Fermat's Little Theorem)**.** *For $a, p \in \mathbb{Z}$ where p is prime and $p \nmid a$ we have*

$$a^{p-1} \equiv 1 \pmod{p}$$

Likewise, $\forall z \in \mathbb{Z}$ we have

$$a^p \equiv a \pmod{p}$$

Proof. The first part follows directly from Euler's Theorem since $\varphi(p) = p - 1$ and $p \nmid a \Rightarrow$ (a, p) = 1. If (a, p) = 1 multiplying both sides by a gives us $a^p \equiv a \pmod{p}$. If $p|a$ then $p|a^p$, so by the transitivity of congruence (both are congruent to zero) $a^p \equiv a \pmod{p}$ □

Example 3.1.1. As a practical application Euler's formula can come in handy for reducing numbers of large powers. Let's say we would like to know the last two digits of 17^{283} such that $0 \leq x < 100$. This is equivalent to solving for x in $17^{283} \equiv x \pmod{100}$. Since (17, 100) = 1 and $\varphi(100) = 40$, we have by Euler's Theorem that $17^{40} \equiv 1 \pmod{100}$. Then $17^{283} = 17^{7 \cdot 40+3} = (17^{40})^7 \cdot 17^3 \equiv 17^3 \equiv 13 \pmod{100}$, so x = 13.

Euler's Theorem also helps us establish the following result:

Theorem 3.2. *For integers a,b ∈ ℤ if (a, n) = 1 then* $ax \equiv b \pmod{n}$ *has a solution; what's more, any solution will be equivalent modulo n (i.e. unique).*

Proof. Since (a,n) = 1 by Euler's Theorem $a^{\varphi(n)} \equiv 1 \pmod{n}$ so $a(a^{\varphi(n)-1}b) = a^{\varphi(n)}b \equiv b \pmod{n}$. So $x = a^{\varphi(n)-1}b$ is a solution.
Now suppose $ax \equiv b \pmod{n}$ and $ay \equiv b \pmod{n}$, then by transitivity of congruence $ax \equiv ay \pmod{n}$, and since (a, n) = 1 $x \equiv y \pmod{n}$, so any two solutions are congruent modulo n. □

We should note that this a sufficient but not a necessary condition. The next and last theorem will give us an even more general picture of when a solution exists. But first an example:

Example 3.2.1. Solve $3x \equiv 10 \pmod{16}$, $0 \leq x < 16$. (3, 16) = 1, so Theorem 3.2 applies. Since $\varphi(16) = 8$ we have $3^8 \equiv 1 \pmod{16}$ so $3(3^7 \cdot 10) \equiv 10 \pmod{16}$ and $3^7 \cdot 10$ is a solution. Since $3^3 = 27 \equiv 11 \pmod{16}$ and $3^4 = 3^3 \cdot 3 \equiv 11 \cdot 3 \equiv 1 \pmod{16}$ we have $3^7 \cdot 10 = 3^4 \cdot 3^3 \cdot 10 \equiv 11 \cdot 10 \equiv 14 \pmod{16}$, so x = 14.

Theorem 3.3. *Let (a, n) = d. There exists a solution x to* $ax \equiv b \pmod{n}$ *if and only if d|b; if solvable there are d incongruent solutions modulo n.*

Proof. If d = 1 then Theorem 3.2 applies. We assume then that d > 1.
Suppose $ax \equiv b \pmod{n}$, then $ax = b + nq$, $q \in \mathbb{Z} \Rightarrow ax + n(-q) = b$. Since $d|a$ and $d|n$ it follows that $d|b$.
Suppose $d|b$, then dk = b and by the definition of gcd dq = a and ds = n for k,q ∈ ℤ, $s \in \mathbb{Z}^+$
So
$ax \equiv b \pmod{n}$ ⇔ dqx - dk = tds ($t \in \mathbb{Z}$) ⇔ qx - k = ts ⇔ $qx \equiv k \pmod{s}$. gcd(a/d, n/d) = gcd(q, s) = 1 (see Theorem 2.3 (b)) so we know from Theorem 2.3 there exists a unique solution z modulo s to $qx \equiv k \pmod{s}$. If x is a solution then $x \equiv z \pmod{s} \Leftrightarrow x = z + y_1 s$, $y_1 \in \mathbb{Z}$. Now for any two solutions to be congruent modulo n we have
$x + y_1 s \equiv x + y_2 s \pmod{n} \Leftrightarrow n|s(y_1 - y_2) \Leftrightarrow d|(y_1 - y_2)$, since $n \nmid s$ (n > s) and so by Euclid's Lemma $n|(y_1 - y_2) \Leftrightarrow d|(y_1 - y_2)$ by the transitivity of division. Therefore, all solutions will be $z, z + s, z + 2s, ..., z + (d - 1)s$, i.e. exactly d of them. □

This was but one application of Euler's Theorem, and there are many others, too numerous to be contained in these small margins. For more reading materials see the sources below or contact the author directly at bch3jh@virginia.edu.

References

[1] Redmond, Don. *Number Theory: An Introduction* . Marcell Dekker, Inc., Carbondale, Illinois, 1996.

[2] Burton M., David. *Elementary Number Theory: Sixth Edition*. McGraw-Hill, New York City, New York, 2007.

[3] Conrad, Keith. *Euler's Theorem*
`https://www.math.uconn.edu/~kconrad/blurbs/ugradnumthy/eulerthm.pdf`

[4] *Inclusion-Exclusion Principle*. ProofWiki. 2015.
`https://proofwiki.org/wiki/Inclusion-Exclusion_Principle`