Euler's Theorem (generalization of Fermat's)

Euler Phi Function

First, let's define the Euler ϕ(phi) function:

$\phi(n)$ = the number of integers in the set {1, 2, ..., n-1} that are relatively prime to n.
$\phi(p) = p - 1$, for all prime numbers
$\phi(pq) = (p-1)(q-1)$, where p and q are distinct primes. Here is a derivation of that result:

We want to count all values in the set {1, 2, 3, ..., pq –1} that are relatively prime to pq. Instead, we could count all value in the set NOT relatively prime to pq. We can list these values:

p, 2p, 3p, ... , (q-1)p

q, 2q, 3q, ... (p-1)q

Note that each of these values are distinct. To notice this, see that no number of the first row is divisible by q and no number on the second row is divisible by p. This ensures that there are no repeats on both rows. since p and q are relatively prime, in order for q to be a factor of a number on the first row, it would have to divide evenly into either 1, 2, 3, ... q-1. But clearly, it does not. The same argument will show that none of the values on the second row are divisible by p.

Finally, we can count the number of values on this list. It's $(q-1) + (p-1) = p + q - 2$.
Now, in order to find $\phi(pq)$, we must subtract this value from $pq - 1$. So, we find:

$\phi(pq) = (pq - 1) - (p + q - 2) = pq - p - q + 1 = (p - 1)(q - 1)$.

Now, let's try to derive a more general result to calculate the ϕ for all positive integers.

First, we will extend our formula $\phi(p) = p - 1$, for all prime numbers, to numbers of the form $\phi(p^n)$. This extension is rather simple because for a number to NOT be relatively prime to p^n, it must be divisible by p. Looking at the list: 1, 2, 3, …, p, …, p^n-1, there are exactly $p^{n-1} - 1$ values on the list divisible by p. (These values are p, 2p, 3p, …, $(p^{n-2} - 1)p$.) Thus, we find that $\phi(p^n) = p^n - 1 - (p^{n-1} - 1) = p^n - p^{n-1}$.

Next, we generalize the result $\phi(pq) = (p - 1)(q - 1) = \phi(p)\phi(q)$ for two primes p and q to any number that is the product of relative prime values, m and n. This extension will take a bit more work. We must count the number of values in the set {1, 2, 3, …, mn – 1} that are relatively prime to mn. Let us write them out in a chart as follows:

1	2	3	4	…	m
m+1	m+2	m+3	m+4	…	2m
…					
(n-1)m+1	(n-1)m+2	(n-1)m+3	(n-1)m+4		nm

We must "cancel out" any term in this grid that is NOT relatively prime to either m or n.

First, let's cancel out the terms NOT relatively prime to m. Quickly note that if some value r is NOT relatively prime to m, then km+r is not either. Thus, if there is some value r in between 1 and m inclusive that shares a common factor with m, then EVERY value in its column shares a common factor with m. Thus, there will be $\phi(m)$ columns that not canceled out. The other columns are completely canceled out.

Now, consider the remaining columns. We need only to look for values that share a common factor with n in these columns. Each column takes the following form:

$r, m+r, 2m+r, 3m+r, \ldots, (n-1)m+r$.

Now, we will prove that each of these numbers is distinct mod n. Assume to the contrary, that two values on the list are equivalent mod n. Let these two values be

$im+r$ and $jm+r$, for $0 \le i < j < n$. Thus, we have:

$im + r \equiv jm + r \pmod{n}$
$jm - im \equiv 0 \pmod{n}$
$m(j - i) \equiv 0 \pmod{n}$

It follows that n divides evenly into $m(i - j)$. But, we are given that $\gcd(m,n) = 1$. This implies that $n \mid (i - j)$. But, this is impossible because $0 < j - i < n$. This is our contradiction. Thus, it follows that each of the n numbers on that list is not equivalent mod n. Thus, there is exactly 1 number for each residue class mod n in the list. It follows that EXACTLY $\phi(n)$ of these are divisible by n. Finally, if we take a look at the numbers not crossed out, there are exactly $\phi(m)\phi(n)$ of them. Here is a quick example with m = 8 and n = 15. All crossed out numbers are underlined. We have $\phi(8)$ = 4 columns of numbers not crossed out.

1	2	3	4	5	6	7	8
9	10	11	12	13	14	15	16
17	18	19	20	21	22	23	24
25	26	27	28	29	30	31	32
33	34	35	36	37	38	39	40
41	42	43	44	45	46	47	48
49	50	51	52	53	54	55	56
57	58	59	60	61	62	63	64
65	66	67	68	69	70	71	72
73	74	75	76	77	78	79	80
81	82	83	84	85	86	87	88
89	90	91	92	93	94	95	96
97	98	99	100	101	102	103	104
105	106	107	108	109	110	111	112
113	114	115	116	117	118	119	120

In each column there are $\phi(15)$ = 8 numbers not crossed out.

Now, given these two results, we can derive a formula for $\phi(n)$ for any positive integer n. Given n's prime factorization, one can simply calculate the phi function of each prime factor separately and multiply these all together.

For example, $\phi(2^5 x 3 x 7^2) = \phi(2^5)\phi(3)\phi(7^2) = (2^5 - 2^4)(3 - 1)(7^2 - 7) = 16(2)(42) = 1344$.

Euler's Theorem

Euler's Theorem: If gcd(a,n) = 1, then $a^{\phi(n)} \equiv 1$ (mod n).

Definition of a reduced residue system modulo n: A set of $\phi(n)$ numbers $r_1, r_2, r_3, \ldots r_{\phi(n)}$ such that $r_i \neq r_j$, for all $1 \leq i < j \leq \phi(n)$ with $\gcd(r_i, n) = 1$ for all $1 \leq i \leq \phi(n)$.

Theorem about reduced residue systems: If $r_1, r_2, r_3, \ldots r_{\phi(n)}$ is a reduced residue system modulo n, and gcd(a,n) = 1, then $ar_1, ar_2, ar_3, \ldots ar_{\phi(n)}$ is ALSO a reduced residue system modulo n.

Proof: We need to prove two things in order to verify the theorem above:

1) $ar_i \neq ar_j$, for all $1 \leq i < j \leq \phi(n)$
2) $\gcd(ar_i, n) = 1$ for all $1 \leq i \leq \phi(n)$

Proof of 1:

Assume to the contrary that there exist distinct integers i and j such that $ar_i \equiv ar_j$ (mod n). We can deduce the following:

$ar_i \equiv ar_j$ (mod n)
$(ar_i - ar_j) \equiv 0$(mod n).
$n \mid (a(r_i - r_j))$

We know that gcd(a,n) = 1. Thus, based on a theorem proved earlier, it follows that $n \mid (r_i - r_j)$. But, this infers that $r_i \equiv r_j$ (mod n). This contradicts our premise that $r_1, r_2, r_3, \ldots r_{\phi(n)}$ is a reduced residue system modulo n. Thus, we can conclude that $ar_i \neq ar_j$, for all $1 \leq i < j \leq \phi(n)$.

Proof of 2:

Since gcd(a,n)=1 and $\gcd(r_i,n)=1$, it follows that n shares no common factors with a or r_i. Thus, it shares no common factors with their product and we can conclude that $\gcd(ar_i, n) = 1$ for all $1 \leq i \leq \phi(n)$.

Now, we will use this theorem to prove Euler's theorem:

Let $r_1, r_2, r_3, \ldots r_{\phi(n)}$ be a reduced residue system modulo n, and gcd(a,n)=1. Then we have that $ar_1, ar_2, ar_3, \ldots ar_{\phi(n)}$ is a reduced residue system modulo n. Since both are reduced residue systems modulo n, we know that the their products are equivalent mod n:

$$\prod_{i=1}^{\phi(n)} ar_i \equiv \prod_{i=1}^{\phi(n)} r_i \text{ (mod n)}$$

$$\prod_{i=1}^{\phi(n)} ar_i - \prod_{i=1}^{\phi(n)} r_i \equiv 0 \text{ (mod n)}$$

$a^{\phi(n)} \prod_{i=1}^{\phi(n)} r_i - \prod_{i=1}^{\phi(n)} r_i \equiv 0 \pmod{n}$

$(\prod_{i=1}^{\phi(n)} r_i)(a^{\phi(n)} - 1) \equiv 0 \pmod{n}$

Thus, we have that n divides this product. But, we know that $\gcd(r_i, n) = 1$ for each value of i. Thus the first large product of $\phi(n)$ terms is relatively prime to n. It follows that n divides the last factor:

$n \mid (a^{\phi(n)} - 1)$
$a^{\phi(n)} \equiv 1 \pmod{n}$, proving Euler's Theorem.

Wilson's Theorem

The theorem follows rather simply from some of our following work:

$(p - 1)! \equiv -1 \pmod{p}$ for all primes p.

This result can be verified for p = 2. Now, let's consider all odd p. Since each value 1, 2, …, p – 1 is relatively prime to p, each has an inverse mod p. We know that the inverse of 1 is 1 and the inverse of p – 1 is p – 1. But, for each other value on the list, its inverse is different than itself.

To see this, let's directly set up an equation for a value k that is its own inverse mod p:

$k^2 \equiv 1 \pmod{p}$
$k^2 - 1 \equiv 0 \pmod{p}$
$(k - 1)(k + 1) \equiv 0 \pmod{p}$

This implies that $p \mid (k - 1)$ or $p \mid (k + 1)$. These are exactly the two values we have written above as having self inverses.

Now, consider the product

1 x 2 x 3 x 4 … x (p – 1)

1 x (p – 1) x (2 x 3 x 4 … x (p – 2))

Each of the terms in the second set of parentheses (there are an even number of them), have their inverses mod p in that set. We can pair up these values such that

1 x (p – 1) x (2 x 3 x 4 … x (p – 2)) $\equiv$ 1 x (p – 1) x 1 x 1 … x 1 (mod p)
$\equiv$ (p – 1) mod p
$\equiv$ -1 (mod p)