7-26-1998

# Euler's Theorem

**Question:** How can you generalize the little Fermat theorem to the case where the modulus is composite?

**Idea:** The key point of the proof of Fermat's theorem was that if $p$ is prime, $\{1, 2, \ldots, p-1\}$ are relatively prime to $p$.

This suggests that in the general case, it might be useful to look at the numbers less than the modulus $n$ which are relatively prime to $n$. This motivates the following definition.

**Definition.** The **Euler $\phi$-function** is the function on positive integers defined by

$$\phi(n) = (\text{the number of integers in } \{1, 2, \ldots, n-1\} \text{ which are relatively prime to } n).$$

---

**Example.** $\phi(24) = 8$, because there are eight positive integers less than 24 which are relatively prime to 24:

$$1, 5, 7, 11, 13, 17, 19, 23$$

On the other hand, $\phi(11) = 10$, because all of the numbers in $\{1, \ldots, 10\}$ are relatively prime to 11.

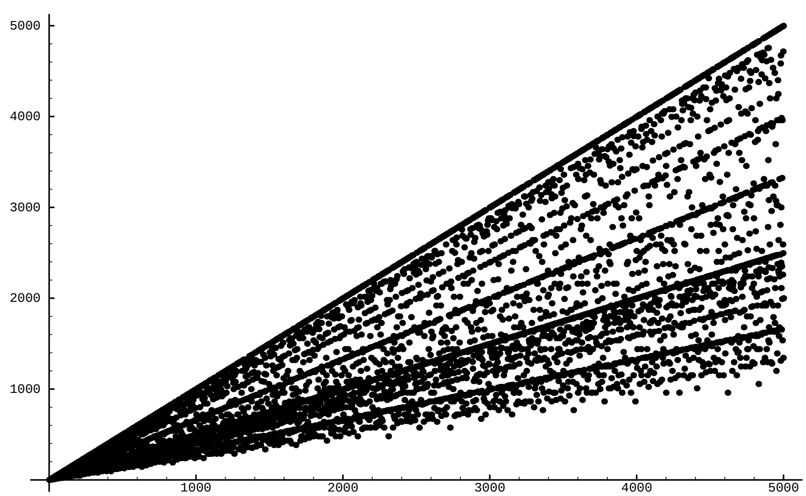
Here is *Mathematica* computing $\phi(20!)$:

```
EulerPhi[20!]

    416084687585280000
```

Next, I had *Mathematica* plot $(n, \phi(n))$ for $1 \le n \le 5000$.

```
ListPlot[Table[EulerPhi[n], {n, 1, 5000}]]
```




You can see that the function jumps around a little, but the data points are bounded above by the line $y = x$. A point will be nearly on this line whenever $n$ is prime, and since there are infinitely many primes, there will always be points near it.

Later, I'll derive a formula for computing $\phi(n)$ in terms of the prime factorization of $n$. $\square$

---

**Remarks.**

1. If $p$ is prime, $\phi(p) = p - 1$.

   This is clear, because all of the numbers $\{1, \ldots, p-1\}$ are relatively prime to $p$.

2. $\phi(n)$ counts the elements in $\{1, 2, \ldots, n-1\}$ which are invertible mod $n$.

   For $(a, n) = 1$ if and only if $ax = 1 \pmod{n}$ for some $x$. (For people who know some abstract algebra, $\phi(n)$ is the order of the group of units $\mathbb{Z}_n^*$.)

**Definition.** A **reduced residue system mod** $n$ is a set of numbers

$$a_1, a_2, \ldots, a_{\phi(n)}$$

such that:

(a) If $i \neq j$, then $a_i \neq a_j \pmod{n}$. That is, the $a$'s are distinct mod $n$.

(b) For each $i$, $(a_i, n) = 1$. That is, all the $a$'s are relatively prime to $n$.

Thus, a reduced residue system contains exactly one representative for each number relatively prime to $n$. Compare this to a **complete residue system mod** $n$, which contains exactly one representative to every number mod $n$.

---

**Example.** $\{1, 5, 7, 11\}$ is a reduced residue system mod 12. So if $\{-11, 17, 31, -1\}$.

On the other hand, $\{0, 1, 2, 3, 4, 5, 6, 7, 8, 9, 10, 11\}$ is a complete residue system mod 12. $\square$

---

**Lemma.** Let $\phi(n) = k$, and let $\{a_1, \ldots, a_k\}$ be a reduced residue system mod $n$.

(a) For all $m$, $\{a_1 + mn, \ldots, a_k + mn\}$ is a reduced residue system mod $n$.

(b) If $(m, n) = 1$, $\{ma_1, \ldots, ma_k\}$ is a reduced residue system mod $n$.

**Proof.** (a) This is clear, since $a_i = a_i + mn \pmod{n}$ for all $i$.

(b) Since $(m, n) = 1$, I may find $x$ such that $mx = 1 \pmod{n}$. Since $(a_i, n) = 1$, so I may find $b_i$ such that $a_i b_i = 1 \pmod{n}$. Then $(xb_i)(am_i) = (mx)(a_i b_i) = 1 \pmod{n}$, which proves that $am_i$ is invertible mod $n$. Hence, $(am_i, n) = 1$ — the $ma$'s are relatively prime to $n$.

Now if $ma_i = ma_j \pmod{n}$, then $xma_i = xma_j \pmod{n}$, or $a_i = a_j \pmod{n}$. Since the $a$'s were distinct mod $n$, this is only possible of $i = j$. Hence, the $ma$'s are also distinct mod $n$.

Therefore, $\{ma_1, \ldots, ma_k\}$ is a reduced residue system mod $n$. $\square$

**Corollary.** Let $\phi(n) = k$, and let $\{a_1, \ldots, a_k\}$ be a reduced residue system mod $n$. Suppose $(s, n) = 1$, and let $t$ be any integer. Then

$$\{sa_1 + tn, sa_2 + tn, \ldots, sa_k + tn\}$$

is a reduced residue system mod $n$. $\square$

---

**Example.** $\{1, 5\}$ is a reduced residue system mod 6. Adding $12 = 2 \cdot 6$ to each number, I get $\{13, 17\}$, another reduced residue system mod 6.

Since $(6, 25) = 1$, I may multiply the original system by 25 to obtain $\{25, 125\}$, another reduced residue system.

Finally, $\{25 + 12, 125 + 12\} = \{37, 137\}$ is yet another reduced residue system mod 12. $\square$

**Theorem.** (Euler) Let $n > 0$, $(a, n) = 1$. Then

$$a^{\phi(n)} = 1 \pmod{n}.$$

**Remark.** If $n$ is prime, then $\phi(n) = n - 1$, and Euler's theorem says $a^{n-1} = 1 \pmod{n}$: the little Fermat theorem.

**Proof.** Let $\phi(n) = k$, and let $\{a_1, \ldots, a_k\}$ be a reduced residue system mod $n$. I may assume that the $a_i$'s lie in the range $\{1, \ldots, n-1\}$.

Since $(a, n) = 1$, $\{aa_1, \ldots, aa_k\}$ is another reduced residue system mod $n$. Since this is the same set of numbers mod $n$ as the original system, the two systems must have the same product mod $n$:

$$(aa_1) \cdots (aa_k) = a_1 \cdots a_k \pmod{n}, \quad a^k (a_1 \cdots a_k) = a_1 \cdots a_k \pmod{n}.$$

Now each $a_i$ is invertible mod $n$, so multiplying both sides by $a_1^{-1} \cdots a_k^{-1}$, I get

$$a^k = 1 \pmod{n}, \quad \text{or} \quad a^{\phi(n)} = 1 \pmod{n}. \quad \square$$

---

**Example.** $\phi(40) = 16$, and $(9, 40) = 1$. Hence, $9^{16} = 1 \pmod{40}$ — surely not an obvious fact!

Likewise, $21^{16} = 1 \pmod{40}$.

You can also use Euler's theorem to compute modular powers. Suppose I want to find $33^{100} \pmod{40}$. *Mathematica* tells me that $33^{100}$ is

71022178218665632296316329939654308627851037229926786264915627239769472510693096283702513561865297732677687859060633131423168375418697393542687445968001

I probably don't want to do this by hand!

Euler's theorem says that $33^{16} = 1 \pmod{40}$. So

$$33^{100} = 33^{96} \cdot 33^4 = (33^{16})^6 \cdot 1089^2 = 9^2 = 81 = 1 \pmod{40}. \quad \square$$

---

**Example.** Solve $15x = 7 \pmod{32}$.

Note that $(15, 32) = 1$ and $\phi(32) = 16$. Therefore, $15^{16} = 1 \pmod{32}$. Multiply the equation by $15^{15}$:

$$x = 7 \cdot 15^{15} \pmod{32}.$$

Now

$$7 \cdot 15^{15} = 105 \cdot 15^{14} = 105 \cdot (15^2)^7 = 105 \cdot 225^7 = 9 \cdot 1^7 = 9 \pmod{32}.$$

So the solution is $x = 9 \pmod{32}$. $\square$