Euler's φ function

Carl Pomerance
Dartmouth College

Euler's φ function: $\varphi(n)$ is the number of integers $m \in [1, n]$ with m coprime to n.

Or, it is the order of the unit group of the ring $\mathbb{Z}/n\mathbb{Z}$.

Euler: If a is coprime to n, then

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

Euler's theorem is the basis of the RSA Cryptosystem:

If integers E, D satisfy $ED \equiv 1 \pmod{\varphi(n)}$, then

$$a^{ED} \equiv a \pmod{n}$$

for every integer a coprime to n. (In fact, this holds for all integers a if n is squarefree, such as the product of two different large primes.)

Encrypt message "a": $b = a^E \pmod{n}$.

Decrypt: $a = b^D \pmod{n}$.

To encrypt, one should know E, n. To decrypt, D as well.

Note that it is easy to compute $a^E \pmod{n}$ given a, E, n and similarly it is easy to compute $b^D \pmod{n}$.

Further, given $\varphi(n)$, it is easy to come up with pairs E, D with $ED \equiv 1 \pmod{\varphi(n)}$. Indeed, keep choosing random numbers D until one is found that is coprime to $\varphi(n)$, and then use Euclid's algorithm to find E.

As a public-key system, E, n are released to the public, but D is kept secret. Then anyone can send you encrypted messages that only you can read.

The security of the RSA Cryptosystem is connected to our ability to compute $\varphi(n)$:

For p prime, $\varphi(p) = p - 1$; more generally, $\varphi(p^k) = p^k - p^{k-1} = p^k(1 - 1/p)$.

By the **Chinese Remainder Theorem**,

$$\varphi(n) = n \prod_{\substack{p \text{ prime} \\ p|n}} \left(1 - \frac{1}{p}\right).$$

So, knowing the prime factorization of n, one can compute $\varphi(n)$ rapidly—in deterministic polynomial time.

What about the converse? Given n and $\varphi(n)$ can one compute the prime factorization of n in deterministic polynomial time?

Yes, if $n = pq$, where p, q are different primes, since $\varphi(n) = (p-1)(q-1)$, so that $n - 1 - \varphi(n) = p + q$.

In general, the Extended Riemann Hypothesis implies that there is a deterministic, polynomial time algorithm to compute the prime factorization of n, given n and $\varphi(n)$.

A random polynomial time algorithm to get a nontrivial factorization:

We may assume $\varphi(n) < n - 1$ and that n and $\varphi(n)$ are coprime.

Write $\varphi(n) = 2^s m$, where m is odd.

Choose a at random from $[1, n-1]$. We may assume a and n are coprime.

Note that

$$a^{\varphi(n)} - 1 = (a^m - 1)(a^m + 1)(a^{2m} + 1) \cdots (a^{2^{s-1}m} + 1).$$

Fact: n divides the product, but the chance that n divides a factor is at most 1/2.

Some natural questions to ask about a function from $\mathbb{N}$ to $\mathbb{N}$:

1. What is $\varphi(n)$ on average? That is, what can be said about
$$\sum_{n\le x}\varphi(n)$$
as x grows?

2. What is typically true about the size of $\varphi(n)$?

3. What about extremes for $\varphi(n)$?

4. What is true on average or typically about $\varphi(n)$ arithmetically?

Euler's function on average

The chance that two random integers are both divisible by the prime p is $1/p^2$. So, the chance that no prime p divides both should be

$$\alpha := \prod_{p \text{ prime}} \left(1 - \frac{1}{p^2}\right).$$

We have

$$1 - \frac{1}{p^2} = \left(\frac{p^2}{p^2 - 1}\right)^{-1} = \left(1 + \frac{1}{p^2} + \frac{1}{p^4} + \cdots\right)^{-1},$$

so that

$$\alpha = \left(\sum_{n=1}^{\infty} \frac{1}{n^2}\right)^{-1} = \frac{1}{\zeta(2)} = \frac{6}{\pi^2}.$$

Thus, the probability that two random integers are coprime is $6/\pi^2$.
Another interpretation: Choose a lattice point (m, n) at random; the probability that it is “visible” is $6/\pi^2$.

Using these thoughts it is easy to see that

$$\sum_{n \le x} \varphi(n) \sim \frac{3}{\pi^2} x^2$$

as $x \to \infty$.

Extreme values of $\varphi(n)$ are also fairly easy:

$$\limsup \frac{\varphi(n)}{n} = 1,$$

$$\liminf \frac{\varphi(n)}{n} = 0,$$

in fact,

$$\liminf \frac{\varphi(n)}{n/\log\log n} = e^{-\gamma}.$$

Clearly $\varphi(n)/n$ jumps around a bit: if n has only large prime factors, the ratio is close to 1, but if n has many small prime factors, it is close to 0.

One can ask for a “distribution function”. That is, let u be a real variable in $[0,1]$ and consider

$$\{n : \varphi(n)/n \leq u\}.$$

Does this set have an asymptotic density $D(u)$, and if so, how does $D(u)$ vary with u?

Schoenberg, 1928: $D(u)$ exists, it is strictly monotone, and varies continuously with u. It has an infinite one-sided derivative on a dense subset of $[0,1]$.

Let $\omega(n)$ denote the number of primes p with $p \mid n$.
For example, $\omega(1) = 0$, $\omega(100) = 2$, $\omega(1001) = 3$.

Hardy and Ramanujan, 1917: Normally $\omega(n) \approx \log\log n$. That is, for each $\epsilon > 0$, the set of n with

$$(1 - \epsilon)\log\log n < \omega(n) < (1 + \epsilon)\log\log n$$

has asymptotic density 1.

Erdős and Kac, 1939 : For each real number u, the set

$$\{n : \omega(n) \le \log\log n + u\sqrt{\log\log n}\}$$

has asymptotic density

$$\frac{1}{\sqrt{2\pi}}\int_{-\infty}^{u} e^{-x^2/2}\,dx,$$

the Gaussian normal distribution.

What can be said about $\omega(\varphi(n))$?

Erdős and P, 1985: For each real number u, the set

$$\left\{n : \omega(\varphi(n)) \le \frac{1}{2}(\log\log n)^2 + \frac{u}{\sqrt{3}}(\log\log n)^{3/2}\right\}$$

has asymptotic density $G(u)$.

Euler's function and groups

Burnside, Dickson, Szele: There is exactly one isomorphism class for groups of order n precisely when n and $\varphi(n)$ are coprime.

Erdős, 1948: The number of integers n in $[1, x]$ with n coprime to $\varphi(n)$ is

$$\left(e^{-\gamma} + o(1)\right) \frac{x}{\log\log\log x}$$

as $x \to \infty$.

Carmichael's conjecture

R. D. Carmichael conjectured that φ is never 1 to 1. That is, for each n there is some $m \neq n$ with $\varphi(m) = \varphi(n)$.

For example: If n is odd, let $\varphi(2n) = \varphi(n)$. Or if $2\|n$, then $\varphi(n/2) = \varphi(n)$. If $4 \mid n$, then $3 \mid n$, since otherwise $\varphi(3n/2) = \varphi(n)$. And if $3\|n$, then $\varphi(2n/3) = \varphi(n)$. Etc.

An elementary theorem: *If n has the property that $p^2 \mid n$ for each prime p with $p - 1 \mid n$, then n is a counterexample to Carmichael's conjecture.*

A challenge: prove no number n satisfies the hypothesis!

Let $V(x)$ denote the number of integers in $[1, x]$ that are values of φ.

Elementary thoughts: 1 is the only odd value of φ.
14 is the first even number that's not a value.
The next is 26.

Do we expect $V(x) \sim \frac{1}{2}x$? Or $V(x) \sim cx$? Or $V(x) = o(x)$?

Idea: Most numbers have many different prime factors, so most values of φ are divisible by a large power of 2. But most numbers are not divisible by a large power of 2. So $V(x) = o(x)$ as $x \to \infty$.

Pillai, 1929: There is some $c > 0$ such that $V(x) \le x/(\log x)^c$ for all large x.

Erdős, 1935: $V(x) = x/(\log x)^{1+o(1)}$ as $x \to \infty$.

Erdős and Hall, 1973, 1976: There are $c_1, c_2 > 0$ such that for all large x,

$$\frac{x}{\log x} \exp\left(c_1(\log\log\log x)^2\right) \le V(x) \le \frac{x}{\log x} \exp\left(c_2(\log\log x)^{1/2}\right).$$

Maier and P, 1988: There is a number $c > 0$ such that as $x \to \infty$,

$$V(x) = \frac{x}{\log x} \exp\left((c + o(1))(\log\log\log x)^2\right).$$

Ford, 1998: Found secondary factors so as to have the correct order of magnitude of $V(x)$.

We still don't have an asymptotic formula for $V(x)$, nor do we know even that $V(2x) \sim 2V(x)$ as $x \to \infty$.

Sierpiński's conjecture

For each integer $k \geq 2$ there is some number v such that $\varphi(n) = v$ has exactly k solutions n.

Ford, 1999: Yes. In fact, a positive proportion of φ values satisfy this. (The proportion depends on k.)

Ford went on to prove in the case $k = 1$ (Carmichael's conjecture), that if there is just one value v with a unique pre-image, than a positive proportion of all values have a unique pre-image.

So, we've seen that most numbers are not values of φ, maybe no number is a value exactly once, and for each $k \geq 2$ there are numbers v which are a value exactly k times.

How large can k be as a function of v?

Erdős, 1935: There is some $\alpha > 0$ such that for infinitely many numbers v, the equation $\varphi(n) = v$ has at least v^{α} solutions.

Idea of proof: There is some $c > 0$ such that a positive proportion of the primes $p \leq y^{1+c}$ have all prime factors of $p - 1$ at most y. (Uses Brun's sieve method.) Now take subsets of these primes with product below e^y. If n is one of these products, then $\varphi(n)$ has prime factors all below y. There are many such n's, but not many numbers below e^y with all prime factors below y. So, some value is inordinately popular.

The current record has $c > 2$, and there are infinitely many values v of φ with more than $v^{0.7}$ pre-images.

It is conjectured that c can be arbitrarily large and that the exponent 0.7 can be replaced with any number < 1.

Lehmer's question

If n is prime, then $\varphi(n) \mid n-1$. Can $\varphi(n)$ be a proper divisor of $n-1$?

Little is known. Though we've searched, we know no such number. Failing a proof that there are none, can we at least show there are few of them? Yes, but we don't know that they are eventually sparser than the set of squares!

Just in: Banks, Güloğlu, and Nevans have shown that the number of such n in $[1, x]$ is, for all large x, at most $x^{1/2}/(\log x)^{1/8}$.

Carmichael's function

Recall that $\varphi(n)$ is the order of the unit group of $\mathbb{Z}/n\mathbb{Z}$. Let $\lambda(n)$ denote the *exponent* of this group.

That is, $\lambda(n)$ is the least positive integer l such that

$$a^l \equiv 1 \pmod{n}$$

for every integer a coprime to n.

Since the unit group is cyclic when $n = p$ is a prime, we have $\lambda(p) = p - 1$. In general, $\lambda(p^a) = \varphi(p^a)$ except when $p = 2, a \geq 3$, when $\lambda(2^a) = \frac{1}{2}\varphi(2^a)$. And

$$n = p_1^{a_1} \dots p_k^{a_k} \text{ implies } \lambda(n) = \mathrm{lcm}[\lambda(p_1^{a_1}), \dots, \lambda(p_k^{a_k})].$$

One can ask, like with Lehmer's question: can $\lambda(n)$ divide $n-1$ for n composite? It is easy to see that if $\lambda(n) \mid n-1$, then

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

for every integer a.

For example, $n = 561$. It is $3 \times 11 \times 17$, and $\text{lcm}[2, 10, 16] = 80$, which is a divisor of 560.

Such composite numbers are called Carmichael numbers.

Alford, Granville, P, 1994: There are infinitely many Carmichael numbers.

Euler chains

Starting with n, consider the sequence

$$n,\ \varphi(n),\ \varphi(\varphi(n)), \dots\ .$$

Eventually you reach 1 and there the sequence becomes constant.
Let $k(n)$ be the number of steps to reach 1.
For example, $k(1) = 0$, $k(2) = 1$, $k(3) = 2$, $k(100) = 6$, etc.

Pillai, 1929 For all n, $k(n) \le \log n/\log 2$ and this is attained when n is a power of 2. Further, $k(2 \cdot 3^j) = j + 1$ and this gives the minimal order of $k(n)$, namely $\log n/\log 3$.

Let $K(n)$ be the totally additive function $(K(ab) = K(a) + K(b))$ such that $K(2) = 1$ and $K(p) = K(p-1)$ for each odd prime p. Then $K(n)$ is the number of even terms in the Euler chain for n, so $K(n) = k(n)$ or $k(n) - 1$. (Essentially, Shapiro, 1943.)

Erdős, Granville, P, Spiro, 1990. Conditionally on the Elliott–Halberstam conjecture, there is some $\alpha > 0$ such that $k(n) \sim \alpha \log n$ on a set of asymptotic density 1.

Here,

$$\alpha = \lim_{x\to\infty} \frac{1}{x} \sum_{p\le x} K(p),$$

but we do not know how to prove unconditionally that this limit exists.

Luca, P, 2007. The product of all of the distinct primes that divide some member of the Euler chain for n exceeds $n^{(1-\epsilon)\log\log n/\log\log\log n}$ for all large n in a set of asymptotic density 1.

This result can be used to show that for almost all n, the degree $D(n)$ of the smallest algebraic number field that contains the nth roots of unity and which can be reached by a sequence of prime-degree radical Galois extensions, has $D(n)$ greater than any fixed power of n.

We know very little about "Carmichael chains" where we iterate λ to get to 1.

Consider "reverse" Euler chains, where given n we try to find n_1 with $\varphi(n_1) = n$ and continue with this. There is an infinite such chain if and only if n is in the range of each iterate of φ.

Luca, P, 2008. The number n is in the range of each iterate of φ if and only if $n = 1$ or is of the form $2^a 3^b$ with $a > 0$.

It's possible to show that if $\lambda(n) \mid n$, then n is in the range of each iterate of λ. There are more than $x^{0.7}$ such numbers $n \le x$. Is $n = 10$ in the range of each iterate of λ?

Further problems

Consider the function U which sends n to the isomorphism class of the unit group of $\mathbb{Z}/n\mathbb{Z}$.

What about the range of this function? That is, how does the number of unit groups with order in $[1, x]$ compare with the total number of abelian groups with order in $[1, x]$?

Is Carmichael's conjecture true for $U(n)$? What about Sierpiński's conjecture?

These and other questions are addressed by Bayless, 2008.