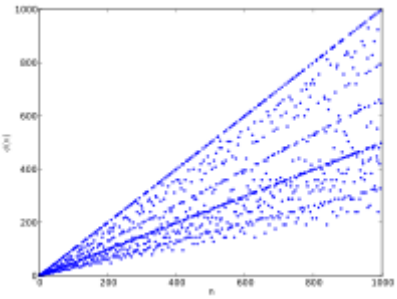
Euler's totient function

In number theory, **Euler's totient function** counts the positive integers up to a given integer n that are relatively prime to n. It is written using the Greek letter phi as $\varphi(n)$ or $\phi(n)$, and may also be called **Euler's phi function**. It can be defined more formally as the number of integers k in the range $1 \le k \le n$ for which the greatest common divisor $\gcd(n, k)$ is equal to 1.[2][3] The integers k of this form are sometimes referred to as totatives of n.



The first thousand values of $\varphi(n)$. The points on the top line represent $\varphi(p)$ when p is a prime number, which is $p - 1$.[1]

For example, the totatives of $n = 9$ are the six numbers 1, 2, 4, 5, 7 and 8. They are all relatively prime to 9, but the other three numbers in this range, 3, 6, and 9 are not, because $\gcd(9, 3) = \gcd(9, 6) = 3$ and $\gcd(9, 9) = 9$. Therefore, $\varphi(9) = 6$. As another example, $\varphi(1) = 1$ since for $n = 1$ the only integer in the range from 1 to n is 1 itself, and $\gcd(1, 1) = 1$.

Euler's totient function is a multiplicative function, meaning that if two numbers m and n are relatively prime, then $\varphi(mn) = \varphi(m)\varphi(n)$.[4][5] This function gives the order of the multiplicative group of integers modulo n (the group of units of the ring $\mathbb{Z}/n\mathbb{Z}$).[6] It also plays a key role in the definition of the RSA encryption system

Contents

History, terminology, and notation

Leonhard Euler introduced the function in 1763.[7][8][9] However, he did not at that time choose any specific symbol to denote it. In a 1784 publication, Euler studied the function further, choosing the Greek letter π to denote it: he wrote πD for "the multitude of numbers less than D, and which have no common divisor with it".[10] This definition varies from the current definition for the totient function at $D = 1$ but is otherwise the same. The now-standard notation[8][11] $\varphi(A)$ comes from Gauss's 1801 treatise *Disquisitiones Arithmeticae*.[12] although Gauss didn't use parentheses around the argument and wrote φA. Thus, it is often called **Euler's phi function** or simply the **phi function**.

In 1879, J. J. Sylvester coined the term **totient** for this function,[13][14] so it is also referred to as **Euler's totient function**, the **Euler totient**, or **Euler's totient**. Jordan's totient is a generalization of Euler's.

The **cototient** of n is defined as $n - \varphi(n)$. It counts the number of positive integers less than or equal to n that have at least one prime factor in common with n.

Computing Euler's totient function

There are several formulas for computing $\varphi(n)$.

Euler's product formula

It states

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

where the product is over the distinct prime numbers dividing n. (The notation is described in the article Arithmetical function)

The proof of Euler's product formula depends on two important facts.

The function is multiplicative

This means that if $\gcd(m, n) = 1$, then $\varphi(mn) = \varphi(m)\,\varphi(n)$. (*Outline of proof*: let A, B, C be the sets of nonnegative integers, which are, respectively, coprime to and less than m, n, and mn; then there is a bijection between $A \times B$ and C, by the Chinese remainder theorem)

Value for a prime power argument

If p is prime and $k \geq 1$, then

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

Proof: since p is a prime number the only possible values of $\gcd(p^k, m)$ are $1, p, p^2, ..., p^k$, and the only way for $\gcd(p^k, m)$ to not equal 1 is for m to be a multiple of p. The multiples of p that are less than or equal to p^k are $p, 2p, 3p, ..., p^{k-1}p = p^k$, and there are p^{k-1} of them. Therefore, the other $p^k - p^{k-1}$ numbers are all relatively prime to p^k.

Proof of Euler's product formula

The fundamental theorem of arithmetic states that if $n > 1$ there is a unique expression for n,

$$n = p_1^{k_1} \cdots p_r^{k_r},$$

where $p_1 < p_2 < ... < p_r$ are prime numbers and each $k_i \geq 1$. (The case $n = 1$ corresponds to the empty product.)

Repeatedly using the multiplicative property of φ and the formula for $\varphi(p^k)$ gives

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

This is Euler's product formula.

Example

$$\varphi(36) = \varphi\left(2^2 3^2\right) = 36\left(1-\tfrac{1}{2}\right)\left(1-\tfrac{1}{3}\right) = 36 \cdot \tfrac{1}{2} \cdot \tfrac{2}{3} = 12.$$

In words, this says that the distinct prime factors of 36 are 2 and 3; half of the thirty-six integers from 1 to 36 are divisible by 2, leaving eighteen; a third of those are divisible by 3, leaving twelve numbers that are coprime to 36. And indeed there are twelve positive integers that are coprime with 36 and lower than 36: 1, 5, 7, 11, 13, 17, 19, 23, 25, 29, 31, and 35.

Fourier transform

The totient is the discrete Fourier transform of the gcd, evaluated at 1.[15] Let

$$\mathcal{F}\{\mathbf{x}\}[m] = \sum_{k=1}^{n} x_k \cdot e^{-2\pi i \frac{mk}{n}}$$

where $x_k = \gcd(k,n)$ for $k \in \{1, \ldots, n\}$. Then

$$\varphi(n) = \mathcal{F}\{\mathbf{x}\}[1] = \sum_{k=1}^{n} \gcd(k,n) e^{-2\pi i \frac{k}{n}}.$$

The real part of this formula is

$$\varphi(n) = \sum_{k=1}^{n} \gcd(k,n) \cos 2\pi \frac{k}{n}.$$

Note that unlike the other two formulae (the Euler product and the divisor sum) this one does not require knowing the factors of n. However, it does involve the calculation of the greatest common divisor of n and every positive integer less than n, which suffices to provide the factorization anyway

Divisor sum

The property established by Gauss,[16] that

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

where the sum is over all positive divisors d of n, can be proven in several ways. (see Arithmetical function for notational conventions.)

One way is to note that $\varphi(d)$ is also equal to the number of possible generators of the cyclic group C_d; specifically, if $C_d = \langle g \rangle$, then g^k is a generator for every k coprime to d. Since every element of C_n generates a cyclic subgroup, and all subgroups of $C_d \leq C_n$ are generated by some element of C_n, the formula follows.[17] In the article Root of unity Euler's formula is derived by using this argument in the special case of the multiplicative group of the nth roots of unity.

This formula can also be derived in a more concrete manner.[18] Let $n = 20$ and consider the fractions between 0 and 1 with denominator 20:

$$\frac{1}{20}, \frac{2}{20}, \frac{3}{20}, \frac{4}{20}, \frac{5}{20}, \frac{6}{20}, \frac{7}{20}, \frac{8}{20}, \frac{9}{20}, \frac{10}{20}, \frac{11}{20}, \frac{12}{20}, \frac{13}{20}, \frac{14}{20}, \frac{15}{20}, \frac{16}{20}, \frac{17}{20}, \frac{18}{20}, \frac{19}{20}, \frac{20}{20}$$

Put them into lowest terms:

$$\frac{1}{20}, \frac{1}{10}, \frac{3}{20}, \frac{1}{5}, \frac{1}{4}, \frac{3}{10}, \frac{7}{20}, \frac{2}{5}, \frac{9}{20}, \frac{1}{2}, \frac{11}{20}, \frac{3}{5}, \frac{13}{20}, \frac{7}{10}, \frac{3}{4}, \frac{4}{5}, \frac{17}{20}, \frac{9}{10}, \frac{19}{20}, \frac{1}{1}$$

First note that all the divisors of 20 are denominators. And second, note that there are 20 fractions. Which fractions have 20 as denominator? The ones whose numerators are relatively prime to 20 ($\frac{1}{20}$, $\frac{3}{20}$, $\frac{7}{20}$, $\frac{9}{20}$, $\frac{11}{20}$, $\frac{13}{20}$, $\frac{17}{20}$, $\frac{19}{20}$). By definition this is $\varphi(20)$ fractions. Similarly, there are $\varphi(10) = 4$ fractions with denominator 10 ($\frac{1}{10}$, $\frac{3}{10}$, $\frac{7}{10}$, $\frac{9}{10}$), $\varphi(5) = 4$ fractions with denominator 5 ($\frac{1}{5}$, $\frac{2}{5}$, $\frac{3}{5}$, $\frac{4}{5}$), and so on.

In detail, we are considering the fractions of the form $\frac{k}{n}$ where k is an integer from 1 to n inclusive. Upon reducing these to lowest terms, each fraction will have as its denominator some divisor of n. We can group the fractions together by denominator, and we must show that for a given divisor d of n, the number of such fractions with denominator d is $\varphi(d)$.

Note that to reduce $\frac{k}{n}$ to lowest terms, we divide the numerator and denominator by $\gcd(k, n)$. The reduced fractions with denominator d are therefore precisely the ones originally of the form $\frac{k}{n}$ in which $\gcd(k, n) = \frac{n}{d}$. The question therefore becomes: how many k are there less than or equal to n which verify $\gcd(k, n) = \frac{n}{d}$? Any such k must clearly be a multiple of $\frac{n}{d}$, but it must also be coprime to d (if it had any common divisor s with d, then $\frac{sn}{d}$ would be a larger common divisor of n and k). Conversely, any multiple k of $\frac{n}{d}$ which is coprime to d will satisfy $\gcd(k, n) = \frac{n}{d}$. We can generate $\varphi(d)$ such numbers by taking the numbers less than d coprime to d and multiplying each one by $\frac{n}{d}$ (these products will of course each be smaller than n, as required). This in fact generates all such numbers, as if k is a multiple of $\frac{n}{d}$ coprime to d (and less than n), then $\frac{k}{n/d}$ will still be coprime to d, and must also be smaller than d, else k would be larger than n. Thus there are precisely $\varphi(d)$ values of k less than or equal to n such that $\gcd(k, n) = \frac{n}{d}$, which was to be demonstrated.

Möbius inversion gives

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

where μ is the Möbius function

This formula may also be derived from the product formula by multiplying out

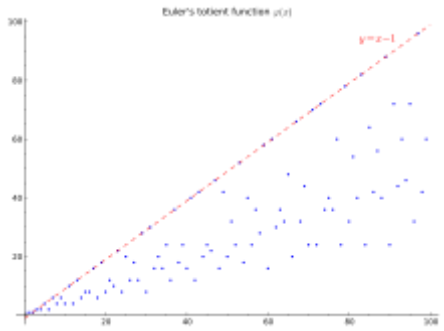
$$\prod_{p|n} \left(1 - \frac{1}{p}\right)$$

to get

$$\sum_{d|n} \frac{\mu(d)}{d}.$$

Some values of the function

The first 143 values (sequenceA000010 in the OEIS) are shown in the table and graph below.[19]



Graph of the first 100 values

$\varphi(n)$ for $1 \le n \le 143$

+	0	1	2	3	4	5	6	7	8	9	10	11
0	N/A	1	1	2	2	4	2	6	4	6	4	10
12	4	12	6	8	8	16	6	18	8	12	10	22
24	8	20	12	18	12	28	8	30	16	20	16	24
36	12	36	18	24	16	40	12	42	20	24	22	46
48	16	42	20	32	24	52	18	40	24	36	28	58
60	16	60	30	36	32	48	20	66	32	44	24	70
72	24	72	36	40	36	60	24	78	32	54	40	82
84	24	64	42	56	40	88	24	72	44	60	46	72
96	32	96	42	60	40	100	32	102	48	48	52	106
108	36	108	40	72	48	112	36	88	56	72	58	96
120	32	110	60	80	60	100	36	126	64	84	48	130
132	40	108	66	72	64	136	44	138	48	92	70	120

The top line in the graph, $y = n - 1$, is a true upper bound. It is attained whenever n is prime. There is no lower bound that is a straight line of positive slope; no matter how gentle the slope of a line is, there will eventually be points of the plot below the line. More precisely, the lower limit of the graph is proportional to $\frac{n}{\log \log n}$ rather than being linear.[20]

Euler's theorem

This states that if a and n are relatively prime then

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

The special case where n is prime is known as Fermat's little theorem.

This follows from Lagrange's theorem and the fact that $\varphi(n)$ is the order of the multiplicative group of integers modulo n.

The RSA cryptosystem is based on this theorem: it implies that the inverse of the function $a \mapsto a^e \mod n$, where e is the (public) encryption exponent, is the function $b \mapsto b^d \mod n$, where d, the (private) decryption exponent, is the multiplicative inverse of e modulo $\varphi(n)$. The difficulty of computing $\varphi(n)$ without knowing the factorization of n is thus the difficulty of computing d: this is known as the RSA problem which can be solved by factoring n. The owner of the private key knows the factorization, since an RSA private key is constructed by choosing n as the product of two (randomly chosen) large primes p and q. Only n is publicly disclosed, and given the difficulty to factor large numbers we have the guarantee that no-one else knows the factorization.

Other formulae

- $a \mid b \implies \varphi(a) \mid \varphi(b)$
- $n \mid \varphi(a^n - 1) \quad \text{for } a, n > 1$
- $\varphi(mn) = \varphi(m)\varphi(n) \cdot \frac{d}{\varphi(d)} \quad \text{where } d = \gcd(m, n)$

  Note the special cases

  - $\varphi(2m) = \begin{cases} 2\varphi(m) & \text{if } m \text{ is even} \\ \varphi(m) & \text{if } m \text{ is odd} \end{cases}$
  - $\varphi(n^m) = n^{m-1}\varphi(n)$
- $\varphi(\operatorname{lcm}(m, n)) \cdot \varphi(\gcd(m, n)) = \varphi(m) \cdot \varphi(n)$

  Compare this to the formula

  - $\operatorname{lcm}(m, n) \cdot \gcd(m, n) = m \cdot n$

  (See least common multiple.)

- $\varphi(n)$ is even for $n \geq 3$. Moreover, if n has r distinct odd prime factors, $2^r \mid \varphi(n)$
- For any $a > 1$ and $n > 6$ such that $4 \nmid n$ there exists an $l \geq 2n$ such that $l \mid \varphi(a^n - 1)$.
- $\frac{\varphi(n)}{n} = \frac{\varphi(\operatorname{rad}(n))}{\operatorname{rad}(n)}$

  where $\operatorname{rad}(n)$ is the radical of n.

- $\sum_{d \mid n} \frac{\mu^2(d)}{\varphi(d)} = \frac{n}{\varphi(n)}$ [21]
- $\sum_{\substack{1 \leq k \leq n \\ (k,n)=1}} k = \frac{1}{2} n\varphi(n) \quad \text{for } n > 1$

- $\sum_{k=1}^{n} \varphi(k) = \frac{1}{2}\left(1 + \sum_{k=1}^{n} \mu(k)\left\lfloor \frac{n}{k} \right\rfloor^2\right) = \frac{3}{\pi^2} n^2 + O\left(n (\log n)^{\frac{2}{3}} (\log\log n)^{\frac{4}{3}}\right)$ ([22] cited in [23])
- $\sum_{k=1}^{n} \frac{\varphi(k)}{k} = \sum_{k=1}^{n} \frac{\mu(k)}{k} \left\lfloor \frac{n}{k} \right\rfloor = \frac{6}{\pi^2} n + O\left((\log n)^{\frac{2}{3}} (\log\log n)^{\frac{4}{3}}\right)$ [22]
- $\sum_{k=1}^{n} \frac{k}{\varphi(k)} = \frac{315\,\zeta(3)}{2\pi^4} n - \frac{\log n}{2} + O\left((\log n)^{\frac{2}{3}}\right)$ [24]
- $\sum_{k=1}^{n} \frac{1}{\varphi(k)} = \frac{315\,\zeta(3)}{2\pi^4}\left(\log n + \gamma - \sum_{p \text{ prime}} \frac{\log p}{p^2 - p + 1}\right) + O\left(\frac{(\log n)^{\frac{2}{3}}}{n}\right)$ [24]

  (where γ is the Euler–Mascheroni constant).

- $\sum_{\substack{1 \le k \le n \\ \gcd(k,m)=1}} 1 = n \frac{\varphi(m)}{m} + O\left(2^{\omega(m)}\right)$

  where $m > 1$ is a positive integer and $\omega(m)$ is the number of distinct prime factors of m.[25]

Menon's identity

In 1965 P. Kesava Menon proved

$$\sum_{\substack{1 \le k \le n \\ \gcd(k,n)=1}} \gcd(k-1, n) = \varphi(n) d(n),$$

where $d(n) = \sigma_0(n)$ is the number of divisors of n.

Formulae involving the golden ratio

Schneider[26] found a pair of identities connecting the totient function, the golden ratio and the Möbius function $\mu(n)$. In this section $\varphi(n)$ is the totient function, and $\phi = \frac{1+\sqrt{5}}{2} = 1.618\ldots$ is the golden ratio.

They are:

$$\phi = -\sum_{k=1}^{\infty} \frac{\varphi(k)}{k} \log\left(1 - \frac{1}{\phi^k}\right)$$

and

$$\frac{1}{\phi} = -\sum_{k=1}^{\infty} \frac{\mu(k)}{k} \log\left(1 - \frac{1}{\phi^k}\right).$$

Subtracting them gives

$$\sum_{k=1}^{\infty} \frac{\mu(k) - \varphi(k)}{k} \log\left(1 - \frac{1}{\phi^k}\right) = 1.$$

Applying the exponential function to both sides of the preceding identity yields an infinite product formula for

$$e = \prod_{k=1}^{\infty} \left(1 - \frac{1}{\phi^k}\right)^{\frac{\mu(k)-\varphi(k)}{k}}.$$

The proof is based on the two formulae

$$\sum_{k=1}^{\infty} \frac{\varphi(k)}{k} \left(-\log\left(1-x^k\right)\right) = \frac{x}{1-x}$$
$$\text{and } \sum_{k=1}^{\infty} \frac{\mu(k)}{k} \left(-\log\left(1-x^k\right)\right) = x, \qquad \text{for } 0 < x < 1.$$

Generating functions

The Dirichlet series for $\varphi(n)$ may be written in terms of the Riemann zeta function as:[27]

$$\sum_{n=1}^{\infty} \frac{\varphi(n)}{n^s} = \frac{\zeta(s-1)}{\zeta(s)}.$$

The Lambert series generating function is[28]

$$\sum_{n=1}^{\infty} \frac{\varphi(n) q^n}{1-q^n} = \frac{q}{(1-q)^2}$$

which converges for $|q| < 1$.

Both of these are proved by elementary series manipulations and the formulae for $\varphi(n)$.

Growth rate

In the words of Hardy & Wright, the order of $\varphi(n)$ is "always 'nearly n'."[29]

First[30]

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

but as n goes to infinity,[31] for all $\delta > 0$

$$\frac{\varphi(n)}{n^{1-\delta}} \to \infty.$$

These two formulae can be proved by using little more than the formulae for $\varphi(n)$ and the divisor sum function $\sigma(n)$.

In fact, during the proof of the second formula, the inequality

$$\frac{6}{\pi^2} < \frac{\varphi(n)\sigma(n)}{n^2} < 1,$$

true for $n > 1$, is proved.

We also have[20]

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

Here γ is Euler's constant, $\gamma = 0.577215665...$, so $e^{\gamma} = 1.7810724...$ and $e^{-\gamma} = 0.56145948...$.

Proving this does not quite require the prime number theorem.[32][33] Since $\log\log(n)$ goes to infinity, this formula shows that

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

In fact, more is true:[34][35][36]

$$\varphi(n) > \frac{n}{e^{\gamma}\ \log\log n + \frac{3}{\log\log n}} \quad \text{for } n > 2$$

and

$$\varphi(n) < \frac{n}{e^{\gamma} \log\log n} \quad \text{for infinitely many } n.$$

The second inequality was shown by Jean-Louis Nicolas. Ribenboim says "The method of proof is interesting, in that the inequality is shown first under the assumption that the Riemann hypothesis is true, secondly under the contrary assumption."[36]

For the average order, we have[22][37]

$$\varphi(1) + \varphi(2) + \cdots + \varphi(n) = \frac{3n^2}{\pi^2} + O\left(n(\log n)^{\frac{2}{3}} (\log\log n)^{\frac{4}{3}}\right) \quad \text{as } n \to \infty,$$

due to Arnold Walfisz, its proof exploiting estimates on exponential sums due to I. M. Vinogradov and N. M. Korobov (this is currently the best known estimate of this type). The "Big O" stands for a quantity that is bounded by a constant times the function of n inside the parentheses (which is small compared to n^2).

This result can be used to prove[38] that the probability of two randomly chosen numbers being relatively prime is $\frac{6}{\pi^2}$.

Ratio of consecutive values

In 1950 Somayajulu proved[39][40]

$$\liminf \frac{\varphi(n+1)}{\varphi(n)} = 0 \quad \text{and}$$

$$\limsup \frac{\varphi(n+1)}{\varphi(n)} = \infty.$$

In 1954 Schinzel and Sierpiński strengthened this, proving[39][40] that the set

$$\left\{ \frac{\varphi(n+1)}{\varphi(n)},\ \ n = 1, 2, \cdots \right\}$$

is dense in the positive real numbers. They also proved[39] that the set

$$\left\{ \frac{\varphi(n)}{n},\ \ n = 1, 2, \cdots \right\}$$

is dense in the interval (0,1).

Totient numbers

A **totient number** is a value of Euler's totient function: that is, an m for which there is at least one n for which $\varphi(n) = m$. The *valency* or *multiplicity* of a totient number m is the number of solutions to this equation.[41] A *nontotient* is a natural number which is not a totient number. Every odd integer exceeding 1 is trivially a nontotient. There are also infinitely many even nontotients,[42] and indeed every positive integer has a multiple which is an even nontotient.[43]

The number of totient numbers up to a given limit x is

$$\frac{x}{\log x} e^{\left(C+o(1)\right)(\log\log\log x)^2}$$

for a constant $C = 0.8178146\ldots$.[44]

If counted accordingly to multiplicity the number of totient numbers up to a given limit x is

$$\left|\{n : \phi(n) \leq x\}\right| = \frac{\zeta(2)\zeta(3)}{\zeta(6)} \cdot x + R(x)$$

where the error term R is of order at most $\frac{x}{(\log x)^k}$ for any positive k.[45]

It is known that the multiplicity of m exceeds m^{δ} infinitely often for any $\delta < 0.55655$.[46][47]

Ford's theorem

Ford (1999) proved that for every integer $k \geq 2$ there is a totient number m of multiplicity k: that is, for which the equation $\varphi(n) = m$ has exactly k solutions; this result had previously been conjectured by Wacław Sierpiński,[48] and it had been obtained as a consequence of Schinzel's hypothesis H.[44] Indeed, each multiplicity that occurs, does so infinitely often.[44][47]

However, no number m is known with multiplicity $k = 1$. Carmichael's totient function conjecture is the statement that there is no such m.[49]

Perfect totient numbers

Applications

Cyclotomy

In the last section of the *Disquisitiones*[50][51] Gauss proves[52] that a regular n-gon can be constructed with straightedge and compass if $\varphi(n)$ is a power of 2. If n is a power of an odd prime number the formula for the totient says its totient can be a power of two only if n is a first power and $n - 1$ is a power of 2. The primes that are one more than a power of 2 are called Fermat primes, and only five are known: 3, 5, 17, 257, and 65537. Fermat and Gauss knew of these. Nobody has been able to prove whether there ar any more.

Thus, a regular n-gon has a straightedge-and-compass construction if n is a product of distinct Fermat primes and any power of 2. The first few such n are[53]

2, 3, 4, 5, 6, 8, 10, 12, 15, 16, 17, 20, 24, 30, 32, 34, 40,... (sequence A003401 in the OEIS).

The RSA cryptosystem

Setting up an RSA system involves choosing large prime numbers p and q, computing $n = pq$ and $k = \varphi(n)$, and finding two numbers e and d such that $ed \equiv 1 \pmod{k}$. The numbers n and e (the "encryption key") are released to the public, and d (the "decryption key") is kept private.

A message, represented by an integer m, where $0 < m < n$, is encrypted by computing $S = m^e \pmod{n}$.

It is decrypted by computing $t = S^d \pmod{n}$. Euler's Theorem can be used to show that if $0 < t < n$, then $t = m$.

The security of an RSA system would be compromised if the number n could be factored or if $\varphi(n)$ could be computed without factoring n.

Unsolved problems

Lehmer's conjecture

If p is prime, then $\varphi(p) = p - 1$. In 1932 D. H. Lehmer asked if there are any composite numbers n such that $\varphi(n) \mid n - 1$. None are known.[54]

In 1933 he proved that if any such n exists, it must be odd, square-free, and divisible by at least seven primes (i.e. $\omega(n) \geq 7$). In 1980 Cohen and Hagis proved that $n > 10^{20}$ and that $\omega(n) \geq 14$.[55] Further, Hagis showed that if 3 divides n then $n > 10^{1937042}$ and $\omega(n) \geq 298848$.[56][57]

Carmichael's conjecture

This states that there is no number n with the property that for all other numbers m, $m \neq n$, $\varphi(m) \neq \varphi(n)$. See Ford's theorem above.

As stated in the main article, if there is a single counterexample to this conjecture, there must be infinitely many counterexamples, and the smallest one has at least ten billion digits in base 10.[41]

See also

- Carmichael function
- Duffin–Schaeffer conjecture
- Generalizations of Fermat's little theorem
- Highly composite number
- Multiplicative group of integers modulo n
- Ramanujan sum

Notes

1. "Euler's totient function" (https://www.khanacademy.org/computing/computer-science/cryptography/modern-crypt/v/euler-s-totient-function-phi-function) *Khan Academy*. Retrieved 2016-02-26.
2. Long (1972, p. 85)
3. Pettofrezzo & Byrkit (1970, p. 72)
4. Long (1972, p. 162)
5. Pettofrezzo & Byrkit (1970, p. 80)
6. See Euler's theorem.

7. L. Euler "Theoremata arithmetica nova methodo demonstrata (http://eulerarchive.maa.org/pages/E271.html) (An arithmetic theorem proved by a new method), *Novi commentarii academiae scientiarum imperialis Petropolitanae* (New Memoirs of the Saint-Petersburg Imperial Academy of Sciences), **8** (1763), 74–104. (The work was presented at the Saint-Petersburg Academy on October 15, 1759. A work with the same title was presented at the Berlin Academy on June 8, 1758). Available on-line in: Ferdinand Rudio, ed., *Leonhardi Euleri Commentationes Arithmeticae*, volume 1, in: *Leonhardi Euleri Opera Omnia*, series 1, volume 2 (Leipzig, Germany: B. G. Teubner, 1915), pages 531–555 (http://gallica.bnf.fr/ark:/12148/bpt6k6952c/f571.image) On page 531, Euler defines *n* as the number of integers that are smaller than N and relatively prime to N (… aequalis sit multitudini numerorum ipso N minorum, qui simul ad eum sint primi, …), which is the phi function, φ(N).
8. Sandifer, p. 203
9. Graham et al. p. 133 note 111
10. L. Euler, *Speculationes circa quasdam insignes proprietates numerorum* (http://math.dartmouth.edu/~euler/docs/originals/E564.pdf), Acta Academiae Scientarum Imperialis Petropolitinae, vol. 4, (1784), pp. 18–30, or Opera Omnia, Series 1, volume 4, pp. 105–115. (The work was presented at the Saint-Petersburg Academy on October 9, 1775).
11. Both $\varphi(n)$ and $\phi(n)$ are seen in the literature. These are two forms of the lower-case Greek letter phi.
12. Gauss, *Disquisitiones Arithmeticae* article 38
13. J. J. Sylvester (1879) "On certain ternary cubic-form equations", *American Journal of Mathematics*, **2** : 357-393; Sylvester coins the term "totient" on page 361 (https://books.google.com/books?id=-AcPAAAAIAAJ&pg=PA361#v=onepage&q&f=false)
14. "totient". *Oxford English Dictionary* (2nd ed.). Oxford University Press 1989.
15. Schramm (2008)
16. Gauss, DA, art 39
17. Gauss, DA art. 39, arts. 52-54
18. Graham et al. pp. 134-135
19. The cell for $n = 0$ in the upper-left corner of the table is empty, as the function $\varphi(n)$ is commonly defined only for positive integers, so it is not defined for $n = 0$.
20. Hardy & Wright 1979, thm. 328
21. Dineva (in external refs), prop. 1
22. Walfisz, Arnold (1963). *Weylsche Exponentialsummen in der neueren Zahlentheorie*. Mathematische Forschungsberichte (in German). **16**. Berlin: VEB Deutscher Verlag der Wissenschaften. Zbl 0146.06003 (https://zbmath.org/?format=complete&q=an:0146.06003)
23. Lomadse, G., "The scientific work of Arnold Walfisz" (http://matwbn.icm.edu.pl/ksiazki/aa/aa10/aa10111.pdf) (PDF), *Acta Arithmetica*, **10** (3): 227–237
24. Sitaramachandrarao, R. (1985). "On an error term of Landau II". *Rocky Mountain J. Math* **15**: 579–588.
25. Bordellès in the external links
26. All formulae in the section are from Schneider (in the external links)
27. Hardy & Wright 1979, thm. 288
28. Hardy & Wright 1979, thm. 309
29. Hardy & Wright 1979, intro to § 18.4
30. Hardy & Wright 1979, thm. 326
31. Hardy & Wright 1979, thm. 327
32. In fact Chebyshev's theorem (Hardy & Wright 1979, thm.7) and Mertens' third theorem is all that is needed.
33. Hardy & Wright 1979, thm. 436
34. Theorem 15 of Rosser, J. Barkley; Schoenfeld, Lowell (1962). "Approximate formulas for some functions of prime numbers" (http://projecteuclid.org/euclid.ijm/1255631807). *Illinois J. Math.* **6** (1): 64–94.
35. Bach & Shallit, thm. 8.8.7
36. Ribenboim. *The Book of Prime Number Records*. Section 4.I.C.
37. Sándor, Mitrinović & Crstici (2006) pp.24–25
38. Hardy & Wright 1979, thm. 332
39. Ribenboim, p.38

40. Sándor, Mitrinović & Crstici (2006) p.16
41. Guy (2004) p.144
42. Sándor & Crstici (2004) p.230
43. Zhang, Mingzhi (1993). "On nontotients" *Journal of Number Theory* **43** (2): 168–172. doi:10.1006/jnth.1993.1014 (https://doi.org/10.1006/jnth.1993.1014) ISSN 0022-314X (https://www.worldcat.org/issn/0022-314X) Zbl 0772.11001 (https://zbmath.org/?format=complete&q=an:0772.11001)
44. Ford, Kevin (1998). "The distribution of totients" *Ramanujan J.* **2** (1–2): 67–151. arXiv:1104.3264 (https://arxiv.org/abs/1104.3264). doi:10.1007/978-1-4757-4507-8_8 (https://doi.org/10.1007/978-1-4757-4507-8_8) ISSN 1382-4090 (https://www.worldcat.org/issn/1382-4090) Zbl 0914.11053 (https://zbmath.org/?format=complete&q=an:0914.11053).
45. Sándor et al (2006) p.22
46. Sándor et al (2006) p.21
47. Guy (2004) p.145
48. Sándor & Crstici (2004) p.229
49. Sándor & Crstici (2004) p.228
50. Gauss, DA. The 7th § is arts. 336–366
51. Gauss proved if n satisfies certain conditions then the n-gon can be constructed. In 1837 Pierre Wantzel proved the converse, if the n-gon is constructible, then n must satisfy Gauss's conditions
52. Gauss, DA, art 366
53. Gauss, DA, art. 366. This list is the last sentence in the *Disquisitiones*
54. Ribenboim, pp. 36–37.
55. Cohen, Graeme L.; Hagis, Peter, Jr. (1980). "On the number of prime factors of n if $\varphi(n)$ divides $n - 1$". *Nieuw Arch. Wiskd., III. Ser.* **28**: 177–185. ISSN 0028-9825 (https://www.worldcat.org/issn/0028-9825) Zbl 0436.10002 (https://zbmath.org/?format=complete&q=an:0436.10002)
56. Hagis, Peter, Jr. (1988). "On the equation $M \cdot \varphi(n) = n - 1$". *Nieuw Arch. Wiskd., IV. Ser.* **6** (3): 255–261. ISSN 0028-9825 (https://www.worldcat.org/issn/0028-9825) Zbl 0668.10006 (https://zbmath.org/?format=complete&q=an:0668.10006).
57. Guy (2004) p.142

References

The *Disquisitiones Arithmeticae* has been translated from Latin into English and German. The German edition includes all of Gauss' papers on number theory: all the proofs of quadratic reciprocity, the determination of the sign of the Gauss sum, the investigations into biquadratic reciprocity, and unpublished notes.

References to the *Disquisitiones* are of the form Gauss, DA, art. *nnn*.

- Abramowitz, M.; Stegun, I. A. (1964), *Handbook of Mathematical Functions*, New York: Dover Publications, ISBN 0-486-61272-4. See paragraph 24.3.2.
- Bach, Eric; Shallit, Jeffrey (1996), *Algorithmic Number Theory (Vol I: Efficient Algorithms)*, MIT Press Series in the Foundations of Computing, Cambridge, MA: The MIT Press, ISBN 0-262-02405-5, Zbl 0873.11070
- Ford, Kevin (1999), "The number of solutions of $\varphi(x) = m$", *Annals of Mathematics*, **150** (1): 283–311, doi:10.2307/121103, ISSN 0003-486X, JSTOR 121103, MR 1715326, Zbl 0978.11053.
- Gauss, Carl Friedrich; Clarke, Arthur A. (translator into English) (1986), *Disquisitiones Arithmeticae (Second, corrected edition)*, New York: Springer, ISBN 0-387-96254-9
- Gauss, Carl Friedrich; Maser, H. (translator into German) (1965), *Untersuchungen uber hohere Arithmetik (Disquisitiones Arithmeticae & other papers on number theory) (Second edition)*, New York: Chelsea, ISBN 0-8284-0191-8
- Graham, Ronald; Knuth, Donald; Patashnik, Oren (1994), *Concrete Mathematics a foundation for computer science* (2nd ed.), Reading, MA: Addison-Wesley, ISBN 0-201-55802-5, Zbl 0836.00001

- Guy, Richard K. (2004), *Unsolved Problems in Number Theory* Problem Books in Mathematics (3rd ed.), New York, NY: Springer-Verlag, ISBN 0-387-20860-7, Zbl 1058.11001
- Hardy, G. H.; Wright, E. M. (1979), *An Introduction to the Theory of Numbers* (Fifth ed.), Oxford: Oxford University Press, ISBN 978-0-19-853171-5
- Long, Calvin T. (1972), *Elementary Introduction to Number Theory* (2nd ed.), Lexington: D. C. Heath and Company, LCCN 77-171950
- Pettofrezzo, Anthony J.; Byrkit, Donald R. (1970) *Elements of Number Theory*, Englewood Cliffs: Prentice Hall, LCCN 77-81766
- Ribenboim, Paulo (1996), *The New Book of Prime Number Records* (3rd ed.), New York: Springer, ISBN 0-387-94457-5, Zbl 0856.11001
- Sandifer, Charles (2007), *The early mathematics of Leonhard Euler*, MAA, ISBN 0-88385-559-3
- Sándor, József; Mitrinović, Dragoslav S.; Crstici, Borislav, eds. (2006), *Handbook of number theory I*, Dordrecht: Springer-Verlag, pp. 9–36, ISBN 1-4020-4215-9, Zbl 1151.11300
- Sándor, Jozsef; Crstici, Borislav (2004). *Handbook of number theory II* Dordrecht: Kluwer Academic. pp. 179–327. ISBN 1-4020-2546-7. Zbl 1079.11001.
- Schramm, Wolfgang (2008), "The Fourier transform of functions of the greatest common divisor", *Electronic Journal of Combinatorial Number Theory*, **A50** (8(1)).

External links

- Hazewinkel, Michiel, ed. (2001) [1994], "Totient function", *Encyclopedia of Mathematics*, Springer Science+Business Media B.V. / Kluwer Academic Publishers, ISBN 978-1-55608-010-4
- Euler's Phi Function and the Chinese Remainder Theorem — proof that $\phi(n)$ is multiplicative
- Euler's totient function calculator in JavaScript — up to 20 digits
- Dineva, Rosica, The Euler Totient, the Möbius, and the Divisor Functions
- Plytage, Loomis, Polhill Summing Up The Euler Phi Function