Some multiplicative arithmetical functions

an invitation to number theory

K. N. Raghavan

`http://www.imsc.res.in/~knr/`

IMSc, Chennai

August 2013

STANDARD FORM AS A PRODUCT OF PRIMES: GCD AND LCM

As we all know well, every positive integer is uniquely a product of primes. Given a positive integer n, we can write:

$$n = p^r q^s \cdots \qquad \text{or, alternatively,} \qquad n = p_1^{r_1} \cdots p_k^{r_k}$$

Here we assume tacitly that $p, q, \ldots$ are distinct primes and that $r, s, \ldots$ are positive (sometimes only non-negative) integers; in the latter case, that $p_1, p_2, \ldots$ are distinct primes and that $r_1, r_2, \ldots$ are positive (sometimes only non-negative) integers.

Such an expression for n is said to be in *standard form*.

If $m = p^r q^s \cdots$ and $n = p^{r'} q^{s'} \cdots$ are in standard form—where the exponents are assumed to be non-negative—then the GCD or HCF of m and n, denoted (m, n), and the LCM of m and n are given by

$$(m, n) = \text{HCF of } m \text{ and } n = p^{\min(r,r')} q^{\min(s,s')} \cdots$$
$$\text{LCM of } m \text{ and } n = p^{\max(r,r')} q^{\max(s,s')} \cdots$$

Since $\{r, r'\} = \{\min(r, r'), \max(r, r')\}$, $\{s, s'\} = \{\min(s, s'), \max(s, s')\}, \ldots,$ it follows that $m \cdot n = \text{their HCF} \cdot \text{their LCM}$.

THE FUNCTIONS $\tau(n)$ AND $\sigma(n)$

Let $n = p_1^{r_1} p_2^{r_2} \cdots$ be in standard form. Then

- the number of divisors $\tau(n)$ of n is $(r_1+1)(r_2+1)\cdots$, for the standard form of any divisor is $p_1^{r_1'} p_2^{r_2'} \cdots$ with $\quad 0 \le r_1' \le r_1, \quad 0 \le r_2' \le r_2, \quad \ldots,$ and there is a one-to-one correspondence between divisors and the choices $(r_1', r_2', \ldots)$.
- the sum of the divisors $\sigma(n)$ is $(1 + p_1 + \cdots + p_1^{r_1})(1 + p_2 + \cdots + p_2^{r_2}) \cdots =$

$$\frac{p_1^{r_1+1} - 1}{p_1 - 1} \cdot \frac{p_2^{r_2+1} - 1}{p_2 - 1} \cdots .$$

To justify the above formula, recall how to sum a geometric series. Writing $S = 1 + p + p^2 + \cdots + p^r$, we have:

$$\begin{aligned} p \cdot S &= \qquad p + p^2 + \cdots + p^{r-1} + p^r + p^{r+1} \\ S &= 1 + p + p^2 + \cdots + p^{r-1} + p^r \end{aligned}$$

so that $pS - S = -1 + p^{r+1}$ and $S = (p^{r+1} - 1)/(p-1)$.

MULTIPLICATIVE ARITHMETICAL FUNCTIONS

We've just seen that if $n = p_1^{r_1} p_2^{r_2} \cdots$ is in standard form, then

$$\tau(n) = (r_1 + 1)(r_2 + 1) \cdots \qquad \sigma(n) = \frac{p_1^{r_1+1} - 1}{p_1 - 1} \cdot \frac{p_2^{r_2+1} - 1}{p_2 - 1} \cdots$$

A function (say, taking real values) on positive integers is called an *arithmetical* function; an arithmetical function f is called *multiplicative* if $f(mn) = f(m)f(n)$ whenever m and n are coprime (i.e., relatively prime).

The functions τ and σ just defined are multiplicative arithmetical functions. Indeed, if $m = p_1^{r_1} p_2^{r_2} \cdots$ and $n = q_1^{s_1} q_2^{s_2} \cdots$ are the standard forms for coprime integers m and n, then $p_1^{r_1} p_2^{r_2} \cdots q_1^{s_1} q_2^{s_2} \cdots$ is the standard form of mn.

Perfect numbers

A positive integer n is called *perfect* if the sum $\sigma(n)$ of its divisors equals $2n$. For example, 6 $(1+2+3+6=12)$ and 28 $(1+2+4+7+14+28=56)$.

Suppose n is an even perfect number. Write $n = 2^k m$ with m odd and $k \geq 1$. We have

$$\sigma(n) = \sigma(2^k)\sigma(m) = (2^{k+1}-1)\sigma(m)$$

Since $\sigma(n) = 2n$, we get: $\qquad (2^{k+1}-1)\sigma(m) = 2^{k+1}m.$

Thus $2^{k+1}-1$ divides m. Put $\ell := m/(2^{k+1}-1)$, so that

$$m = (2^{k+1}-1)\ell \quad \text{and} \quad \sigma(m) = 2^{k+1}\ell.$$

If $\ell > 1$, then m has at least 3 distinct divisors, 1, ℓ, and m; so

$$\begin{aligned} \sigma(m) \geq \quad 1 + m + l \quad &= \quad 1 + (2^{k+1}-1)\ell + \ell \quad = \quad 1 + 2^{k+1}\ell \\ &> \quad 2^{k+1}\ell \quad = \quad \sigma(m) \end{aligned}$$

But this is a contradiction. So $\ell = 1$, which means that $m = 2^{k+1}-1$ and $\sigma(m) = 2^{k+1}$; since $\sigma(m) = m+1$, we conclude that $m = 2^{k+1}-1$ is a prime.

Thus the even perfect numbers are precisely those of the form

$$n = 2^k(2^{k+1}-1) \qquad \text{with } 2^{k+1}-1 \text{ a prime}$$

EVEN PERFECT NUMBERS

We've just seen that the even perfect numbers are precisely those of type $n = 2^{p-1}(2^p - 1)$ with p an integer such that $2^p - 1$ a prime. The observation is due to the great mathematician Leonhard Euler (1707–1783).

For $2^p - 1$ to be a prime, it is necessary that p be prime: for, if $p = rs$, then

$$2^p - 1 = 2^{rs-1} = (2^r - 1)(2^{r(s-1)} + 2^{r(s-2)} + \cdots + 2^r + 1)$$

So to generate even perfect numbers, we must take p to be prime and check if $2^p - 1$ is prime. For the values 2, 3, 5, 7, 11, 13, 17, 19, 23, 29 of p, the respective values of $2^p - 1$ are:

$3,\ 7,\ 31,\ 127,\ 2047 = 23{\cdot}89,\ 8191,\ 131071,\ 524287,\ 47{\cdot}178481,\ 233{\cdot}1103{\cdot}2089$

Thus the first few even perfect numbers are: $2 \cdot 3 = 6$, $4 \cdot 7 = 28$, $2^4 \cdot 31 = 496$, $2^6 \cdot 127 = 8128$, $2^{12} \cdot 8191 = 33550336$.

MERSENNE PRIMES AND PERFECT NUMBERS

A prime number of the form $2^p - 1$ is called a *Mersenne prime* after a certain Frenchman Marin Mersenne who lived in the 17th Century.

As we just saw, in order that $2^p - 1$ be prime, it is necessary that p be prime. But the primality of p is by no means sufficient: $2^{11} - 1 = 2047 = 23 \cdot 89$, for example. We know precious little about Mersenne primes:

- It is not known if there are infinitely many Mersenne primes.
- The total number of known Mersenne primes is 48 (the latest being discovered in Janurary 2013! It has 17,425,170 digits!).
- It is not even known whether $2^p - 1$ is composite for infinitely many primes p.

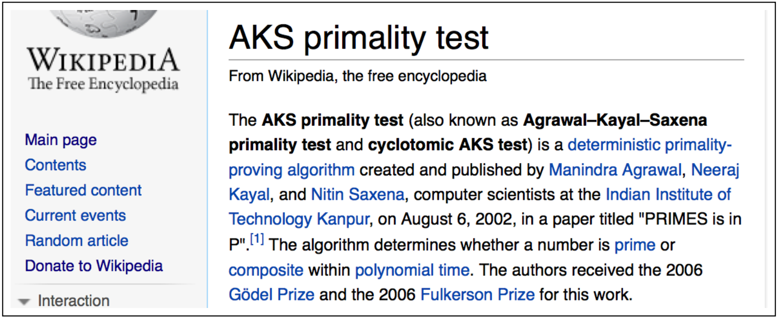
As to perfect numbers, our knowledge of them is equally thin:

- Since the known number of Mersenne primes is 48, it follows that the known number of even perfect numbers is also 48.
- We do not know even a single odd perfect number. Nor do we know that they do not exist.

PRIMALITY TESTING: THE AKS TEST

As you can see, it would help, in the search for Mersenne primes, to be able to tell "quickly" whether a given large number (with thousands of digits or even larger) is prime. This question of whether there is a quick test for primality is a fundamental one and was open for a long time (although efficient algorithms were known to check primality of numbers of the form $2^p - 1$ with p prime).

Screenshot of Wikipedia page:



AKS primality test

From Wikipedia, the free encyclopedia

The **AKS primality test** (also known as **Agrawal–Kayal–Saxena primality test** and **cyclotomic AKS test**) is a deterministic primality-proving algorithm created and published by Manindra Agrawal, Neeraj Kayal, and Nitin Saxena, computer scientists at the Indian Institute of Technology Kanpur, on August 6, 2002, in a paper titled "PRIMES is in P".[1] The algorithm determines whether a number is prime or composite within polynomial time. The authors received the 2006 Gödel Prize and the 2006 Fulkerson Prize for this work.

SOME OPEN PROBLEMS

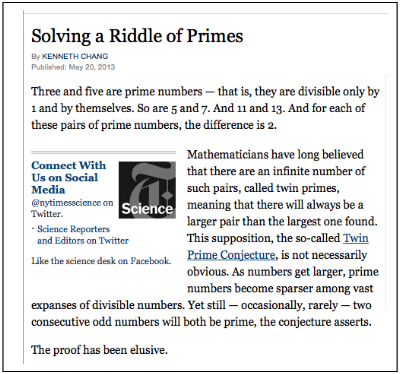
A similar test for whether or not a number is square-free (that is, whether the square of any prime divides it) is not known. For this and many other simply stated open problems in mathematics, one could see the video of a lecture by Joseph Oesterlé on **matsciencechannel–YouTube**:
Some simple open problems in Mathematics.

Whether there are infinitely many prime pairs that are 2 apart, like:

$$3,5 \quad 5,7 \quad 11,13 \quad 17,19 \quad 29,31 \quad \cdots$$

is a very famous problem called the *twin prime problem* which has been open for several hundred years and towards which there has been spectacular recent progress (by Yitang Zhang, April 2013).

from the NY times of May 20, 2013



Solving a Riddle of Primes

By KENNETH CHANG
Published: May 20, 2013

Three and five are prime numbers — that is, they are divisible only by 1 and by themselves. So are 5 and 7. And 11 and 13. And for each of these pairs of prime numbers, the difference is 2.

Connect With Us on Social Media
@nytimesscience on Twitter.
· Science Reporters and Editors on Twitter
Like the science desk on Facebook.

Mathematicians have long believed that there are an infinite number of such pairs, called twin primes, meaning that there will always be a larger pair than the largest one found. This supposition, the so-called Twin Prime Conjecture, is not necessarily obvious. As numbers get larger, prime numbers become sparser among vast expanses of divisible numbers. Yet still — occasionally, rarely — two consecutive odd numbers will both be prime, the conjecture asserts.

The proof has been elusive.

The Möbius function μ and the Euler totient function ϕ

The *Möbius function* $\mu(n)$ of a positive integer $n = p_1^{r_1} \cdots p_k^{r_k}$ in standard form with all exponents $r_1, \ldots, r_k$ assumed to be positive is defined to be

$$\begin{array}{cl} 0 & \text{if at least one of the exponents } r_1, \ldots r_k \text{ is } \geq 2 \\ (-1)^k & \text{otherwise (that is, if either } r_1 = \ldots = r_k = 1\text{, or if } k = 0\text{, i.e., } n = 1) \end{array}$$

It is easily seen to be multiplicative. Its usefulness will soon become clear.

The *Euler totient function* $\phi(n)$ of a positive integer n is the number of integers among $1, \ldots, n$ that are coprime to n. We take $\phi(1) = 1$ (by definition, if you wish). We will presently show that for $n = p_1^{r_1} \cdots p_k^{r_k}$ in standard form with $r_1, \ldots, r_k$ all > 0,

$$\boxed{\phi(n) = n \cdot (1 - \frac{1}{p_1}) \cdots (1 - \frac{1}{p_k})}$$

In other words,

$$\phi(n) = n \cdot \frac{p_1 - 1}{p_1} \cdot \ \cdots \ \cdot \frac{p_k - 1}{p_k} = (p_1 - 1)p_1^{r_1 - 1} \cdots (p_k - 1)p_k^{r_k - 1}$$

It follows immediately from the formula above for ϕ that it is multiplicative.

PROOF BY INCLUSION-EXCLUSION OF THE FORMULA FOR ϕ

If $d|n$, then there are n/d integers from among $1, \ldots, n$ that divisible by d: namely, $d, 2d, 3d, \ldots, (n/d)d = n$.

Suppose that $n = p^k$ is a prime power. To compute $\phi(n)$ we need only delete all multiples of p from $1, \ldots, n$, and count how many remain. Since the number of these multiples is $n/p = p^{k-1}$, we get

$$\phi(p^k) = p^k - p^{k-1} = p^{k-1}(p-1) = p^k(1 - \frac{1}{p})$$

Now suppose $n = p_1^{r_1} p_2^{r_2}$ has two prime divisors p_1 and p_2. To compute $\phi(n)$, we must now delete all multiples of p_1 and also all multiples of p_2 from $1, \ldots, n$, and count how many remain. The number of multiples of p_1 here is n/p_1; the number of multiples of p_2 is n/p_2. Are there numbers that are multiples of both p_1 and p_2? Yes, of course. They are precisely those that are multiples of $p_1 p_2$, and their number is $n/p_1 p_2$. We therefore get

$$\begin{aligned}\phi(n) = \phi(p_1^{r_1} p_2^{r_2}) &= n - \frac{n}{p_1} - \frac{n}{p_2} + \frac{n}{p_1 p_2} \\ &= n(1 - \frac{1}{p_1} - \frac{1}{p_2} + \frac{1}{p_1 p_2}) = n(1 - \frac{1}{p_1})(1 - \frac{1}{p_2})\end{aligned}$$

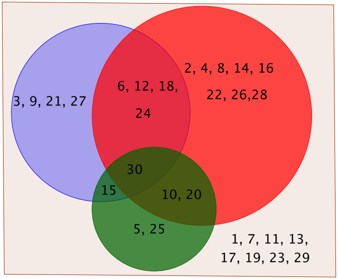
PROOF BY INCLUSION-EXCLUSION (CONTINUED)

Now suppose $n = 30 = 2 \cdot 3 \cdot 5$.

The red, blue, and green circles in the picture consist respectively of the multiples of 2, 3, and 5.

Those integers from $1, \ldots, 30$ that are relatively prime to 30 lie outside all three circles.

Thus $\phi(30) = 8$.



The priniciple of "inclusion exclusion": let $S = S_0$ be a set, and $S_1, \ldots, S_k$ be subsets. Then the cardinality of the complement of the union of the subsets is:

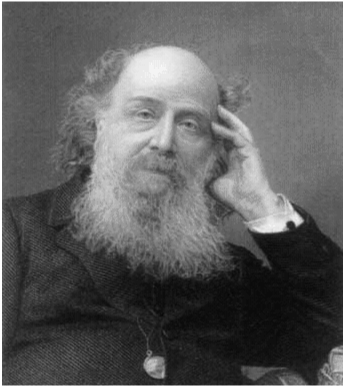
$$|\,(S \setminus (S_1 \cup \cdots \cup S_k))\,| = \sum_{j=0}^{k} (-1)^j \left(\sum_{1 \le i_1 < \ldots < i_j \le k} |S_{i_1} \cap \ldots \cap S_{i_j}| \right)$$

In case $k = 3$, for example, we get:

$$|S \setminus (S_1 \cup S_2 \cup S_3)| = |S| - (|S_1| + |S_2| + |S_3|) + (|S_1 \cap S_2| + |S_1 \cap S_3| + |S_2 \cap S_3|) - |S_1 \cap S_2 \cap S_3|$$

Proof of the inclusion-exclusion principle

J. J. Sylvester (1814–1897)



The justification for the principle of inclusion exclusion is this. Consider the contribution of a given element, say s, of the set S to the expression on the right hand side. If s does not belong to any of the subsets $S_1, \ldots, S_k$, then it contributes only to $|S|$ and to nothing else, so its total contribution is 1.

Now suppose that s belongs to some of the subsets, say m of them, namely $S_{\ell_1}, \ldots, S_{\ell_m}$. Then s contributes to 2^m terms on the right: those with $j \leq m$ and $i_1, \ldots, i_j$ chosen from $\ell_1, \ldots, \ell_m$. Since there are $\binom{m}{j}$ of such choices, the total contribution is $\sum_{j=0}^{k}(-1)^j\binom{m}{j} = (1-1)^m = 0$.

This finishes the justification.

Proof by inclusion-exclusion (continued)

We now give the formal proof of the following formula for $\phi(n)$, when $n = p_1^{r_1} \cdots p_k^{r_k}$ is in standard form with $r_1, \ldots, r_k$ all positive:

$$\phi(n) = \phi(p_1^{r_1} \cdots p_k^{r_k}) = n \cdot (1 - \frac{1}{p_1}) \cdots (1 - \frac{1}{P_k}) = (p_1 - 1)p_1^{r_1 - 1} \cdots (p_k - 1)p_k^{r_k - 1}$$

Apply the inclusion-exclusion priniciple with $S = \{1, \ldots, n\}$ and subsets $S_1, \ldots, S_k$, where S_j consists of all those elements of S that are multiples of p_j.

- If an element of S has a common factor with n, then at least one of the primes $p_1, \ldots, p_k$ divide it. Thus $\phi(n)$ counts the cardinality of the complement in S of the union $S_1 \cup \cdots \cup S_k$.
- The intersection $S_{i_1} \cap \cdots \cap S_{i_j}$ consists of simultaneous multiples of p_{i_1}, $\ldots, p_{i_j}$; since the p_i are mutually relatively prime, this intersection consists of precisely of the multiples of $p_{i_1} \cdots p_{i_j}$. The cardinality of $S_{i_1} \cap \cdots \cap S_{i_j}$ is thus $n/p_{i_1} \cdots p_{i_j}$.

Plugging this into the formula inclusion-exclusion formula, we get

$$\phi(n) = \sum_{j=0}^{k} (-1)^j \frac{n}{p_{i_1} \cdots p_{i_j}} = n \cdot (\sum_{j=0}^{k} (-1)^j \frac{1}{p_{i_1} \cdots p_{i_j}}) = n \cdot (1 - \frac{1}{p_1}) \cdot \cdots \cdot (1 - \frac{1}{p_j})$$

OTHER MULTIPLICATIVE FUNCTIONS

We have so far defined four multiplicative functions: τ, σ, μ, and ϕ. These are by no means all. In fact, there are infinitely many of them:

- for example, $n \mapsto n^\alpha$ for any real number α is mutliplicative;
- moreover, the value of a multiplicative function on prime powers determines it, but these values can be fixed arbitrarily without any restriction.

Given an arithmetical function f, we may define another one $\tilde{f}$ as follows: $\tilde{f}(n) = \sum_{d|n} f(d)$. If f is multiplicative, then so is $\tilde{f}$. Indeed, if m and n are coprime, and D, E, and F the sets of divisors respectively of m, n, and mn, then $D \times E \to F$ given by $(d, e) \mapsto de$ is a bijection. Thus

$$\tilde{f}(mn) = \sum_{d|mn} f(d) = \sum_{d_1|m} \sum_{d_2|n} f(d_1 d_2) = (\sum_{d_1|m} f(d_1)) \cdot (\sum_{d_2|n} f(d_2)) = \tilde{f}(m) \cdot \tilde{f}(n)$$

- If c_1 denotes the constant function with value 1 (that maps every positive integer to 1), then $\tilde{c_1}(n) = \sum_{d|n} c_1(d) = \sum_{d|n} 1 = \tau(n)$.
- If ι is the identity function (that maps every positive integer to itself), then $\tilde{\iota}(n) = \sum_{d|n} \iota(d) = \sum_{d|n} d = \sigma(n)$.

TWO MORE COMPUTATIONS

- We claim that $\tilde{\mu} = \imath$, where $\imath(n)$ is zero for all n except $\imath(1) = 1$.
  Proof: Since μ is multiplicative, so is $\tilde{\mu}$. We clearly have $\tilde{\mu}(1) = \mu(1) = 1$ (from the definition of $\tilde{\mu}$). Thus we need only show that $\tilde{\mu}(p^k) = 0$ for every prime p with k positive.

  Again from the definition of $\tilde{\mu}$, we have $\tilde{\mu}(p^k) = \sum_{0 \leq j \leq k} \mu(p^j)$. But $\mu(p^j) \neq 0$ only when $j = 0$ and $j = 1$. In the former case it is 1 and in the latter it is -1. Thus $\tilde{\mu}(p^k) = 0$ when k is positive.
- Let us compute $\tilde{\phi}$. Since ϕ is multiplicative (by our formula), so is $\tilde{\phi}$.
  It is thus enough to compute $\tilde{\phi}$ on a prime power p^k.
  As is easily seen, $\phi(p^j) = p^j - p^{j-1}$ for $j > 0$. So

$$\begin{aligned} \tilde{\phi}(p^k) &= \phi(1) + \phi(p) + \phi(p^2) + \cdots + \phi(p^{k-1}) + \phi(p^k) \\ &= 1 + (p-1) + (p^2 - p) + \cdots + (p^k - p^{k-1}) \quad = \quad p^k. \end{aligned}$$

  This proves that $\tilde{\phi} = \iota$, the identity function.
- Summary of our computations: $\tilde{c_1} = \tau, \quad \tilde{\iota} = \sigma, \quad \tilde{\mu} = \imath, \quad \tilde{\phi} = \iota.$

THE MÖBIUS INVERSION FORMULA

The Möbius inversion formula gives an answer to the following natural question: suppose that f is an arithmetical function; given $\tilde{f}$, can you determine f? If so, how to do it? Answer:

$$\boxed{f(n) = \sum_{d|n} \tilde{f}(d)\mu(n/d) = \sum_{d|n} \mu(d)\tilde{f}(n/d) = \sum_{d_1 d_2 = n} \mu(d_1)\tilde{f}(d_2)}$$

For the proof, expand the right hand side by substituting for $\tilde{f}$:

$$\sum_{d|n} \mu(d)\tilde{f}(n/d) = \sum_{d|n} \mu(d)\Big(\sum_{e|(n/d)} f(e)\Big) = \sum_{e|n} f(e)\Big(\sum_{d|(n/e)} \mu(d)\Big) = \sum_{e|n} f(e)\tilde{\mu}(n/e)$$

But, as we just saw, $\tilde{\mu} = 1$, which means that $\tilde{\mu}(n/e)$ is non-zero only for $e = n$ in which case it is 1. Thus the last summation in the above display reduces to $f(n)$, and the Möbius inversion is proved.

Möbius inversion reorganized: convolution product

To better organize the idea of Möbius inversion, we introduce the following *convolution product* on arithmetical functions:

$$f * g\,(n) = \sum_{d|n} f(d)g(n/d) = \sum_{d_1 d_2 = n} f(d_1)g(d_2)$$

- $\tilde{f} = f * c_1$ (where c_1 is the function that takes value 1 everywhere). Indeed, $f * c_1(n) = \sum_{d|n} f(d)c_1(n/d) = \sum_{d|n} f(d) = \tilde{f}(n)$.
- The convolution product is commutative and associative. It admits an identity, namely the function $\mathbb{1}$ that takes value 1 at 1 and 0 elsewhere: $f * \mathbb{1} = \mathbb{1} * f = f$.
- (Routine exercise) If f and g are multiplicative, so is $f * g$.
- On the one hand, $\mu * c_1 = c_1 * \mu = \tilde{\mu}$ from the first item above; on the other, $\tilde{\mu} = 1$, as seen on an earlier slide. Thus c_1 and μ are inverses of each other with respect to convolution.
- The Möbius inversion formula can now be written as: $f = \tilde{f} * \mu$, and its proof as:

$$\tilde{f} * \mu = (f * c_1) * \mu = f * (c_1 * \mu) = f * \tilde{\mu} = f * \mathbb{1} = f$$