On the probability that two integers are relatively prime*

by

Marcel K. Goh (Saigon, Vietnam)

26 July 2019

By the fundamental theorem of arithmetic, any integer $n > 1$ may be expressed as a product of primes

$$n = p_1^{e_1} p_2^{e_2} \cdots p_k^{e_k},$$

and this representation is unique up to the order of the factors. If none of the primes are repeated, i.e. each exponent e_i is at most 1, then we say that n is *square-free*. The *Möbius function* $\mu : \mathbf{N} \to \{0, \pm 1\}$ is given by

$$\mu(n) = \begin{cases} 1 & \text{if } n = 1 \text{ or } n \text{ is square-free and has an even number of prime factors;} \\ -1 & \text{if } n \text{ is square-free and has an odd number of prime factors; and} \\ 0 & \text{otherwise.} \end{cases}$$

If two integers u, v have no prime factors in common (i.e. $\gcd(u, v) = 1$), we say they are *relatively prime* and write $u \perp v$. For any positive integer n, let q_n denote the number of ordered pairs of integers (u, v) such that $1 \leq u, v \leq n$and $u \perp v$. Then the probability that any pair of integers u, v lying in the range $[1 \,..\, n]$ are relatively prime is q_n/n^2. Our goal is to find out what happens when u and v may be *any* positive integers. In other words, we will investigate the behaviour of q_n/n^2 as $n \to \infty$. We begin with the following lemma:

Lemma A. *For any positive integer n, we have*

$$q_n = \sum_{k \geq 1} \mu(k) \left\lfloor \frac{n}{k} \right\rfloor^2,$$

where the floor function $\lfloor x \rfloor$ returns the largest integer that is no larger than x.

Proof. Let X denote the set of all ordered pairs (u, v) in the range $1 \geq u, v \geq n$. Note that X contains n^2 elements. For each prime number p_i, let $S_{p_i} \subset X$ denote the set of pairs (u, v) such that p_i divides both u and v. Since $u \perp v$ if and only if no prime divides both u and v, the number of pairs (u, v) that lie in *none* of the sets S_{p_i} is exactly q_n. Thus

$$q_n = |X \setminus \bigcup_{p_i} S_{p_i}|.$$

By the inclusion-exclusion principle, we can expand this to get

$$q_n = |X| - \sum_{p_i} |S_{p_i}| + \sum_{p_i < p_j} |S_{p_i} \cap S_{p_j}| - \sum_{p_i < p_j < p_k} |S_{p_i} \cap S_{p_j} \cap S_{p_k}| + \cdots$$

$$q_n = n^2 - \sum_{p_i} \left\lfloor \frac{n}{p_i} \right\rfloor^2 + \sum_{p_i < p_j} \left\lfloor \frac{n}{p_i p_j} \right\rfloor^2 - \sum_{p_i < p_j < p_k} \left\lfloor \frac{n}{p_i p_j p_k} \right\rfloor^2 + \cdots$$

where the sums are taken over all prime numbers.

First, notice that although each sum is taken over all prime numbers, each sum is actually finite due to the floor function. From the uniqueness of prime decompositions, each positive integer $k \geq 1$ appears in the denominator of at most one term in the overall alternating sum. If k is not square-free, it does not appear at all, since no term contains a repeated prime in its denominator. If the prime decomposition of k consists of an odd number of distinct primes, then we see from the sum above that it contributes $-\lfloor n/k \rfloor^2$ to the sum. Finally, if $k = 1$ or k is the product of an even number of distinct primes, then it contributes $+\lfloor n/k \rfloor^2$

* This document functions as a complete solution to Exercise 4.5.2–10 of *The Art of Computer Programming* by D. E. Knuth.

to the sum. This corresponds to the definition of the Möbius function. So we have $q_n = \sum_{k\geq 1} \mu(k)\lfloor n/k \rfloor^2$, as we had hoped. ∎

In the proof of the next result, we will employ notation that is useful when describing the asymptotic behaviour of a function. Let f and g be functions such that g is strictly positive for large enough values of n. We write $f(n) = O\big(g(n)\big)$ if and only if there exist positive real numbers c and n_0 such that $|f(n)| \leq c \cdot g(n)$ for $n \geq n_0$; and we write $f(n) = o\big(g(n)\big)$ if and only if for all choices of positive real ϵ, there exists a real $n_0 > 0$ such that $|f(n)| \leq \epsilon \cdot g(n)$ for any $n \geq n_0$. Intuitively, $f(n)$ being $O\big(g(n)\big)$ means that as n gets very large and omitting constant factors, $f(n)$ grows no faster than $g(n)$. The notation $f(n) = o\big(g(n)\big)$ makes a stronger statement, implying that as n gets very large, $f(n)$ becomes insignificant relative to $g(n)$.

Lemma B.

$$\lim_{n\to\infty} \frac{q_n}{n^2} = \sum_{k\geq 1} \frac{\mu(k)}{k^2}.$$

Proof. To prove this limit, we will investigate the difference

$$q_n - \sum_{k\geq 1} \mu(k) \left(\frac{n}{k}\right)^2 = \sum_{k\geq 1} \mu(k) \left\lfloor \frac{n}{k} \right\rfloor^2 - \sum_{k\geq 1} \mu(k) \left(\frac{n}{k}\right)^2.$$

Because $\lfloor n/k \rfloor = 0$ for $k > n$, the first summation on the right-hand side need only range up to $k = n$, and we can reorganise the summations as follows:

$$\sum_{k\geq 1} \mu(k) \left\lfloor \frac{n}{k} \right\rfloor^2 - \sum_{k\geq 1} \mu(k) \left(\frac{n}{k}\right)^2 = \sum_{k=1}^{n} \mu(k) \left\lfloor \frac{n}{k} \right\rfloor^2 - \sum_{k=1}^{n} \mu(k) \left(\frac{n}{k}\right)^2 - \sum_{k>n} \mu(k) \left(\frac{n}{k}\right)^2$$

$$q_n - \sum_{k\geq 1} \mu(k) \left(\frac{n}{k}\right)^2 = \sum_{k=1}^{n} \mu(k) \left(\left\lfloor \frac{n}{k} \right\rfloor^2 - \left(\frac{n}{k}\right)^2 \right) - \sum_{k>n} \mu(k) \left(\frac{n}{k}\right)^2 \tag{1}$$

We will want to put asymptotic bounds on these rearranged sums. First, note that for all positive real x,

$$x^2 - \lfloor x \rfloor^2 = O(x). \tag{2}$$

For $x^2 - \lfloor x \rfloor^2$ can be rewritten $(x + \lfloor x \rfloor)(x - \lfloor x \rfloor)$, which is at most $2x \cdot x = 3x$. Next, we use standard formulas to analyse the asymptotic behaviour of the series $\sum_{k>n}(n/k)^2$:

$$\begin{aligned} \sum_{k>n} \left(\frac{n}{k}\right)^2 &= \sum_{k\geq 1} \left(\frac{n}{k}\right)^2 - \sum_{k=1}^{n} \left(\frac{n}{k}\right)^2 \\ &= \frac{n^2\pi^2}{6} - n^2 \left(\frac{\pi^2}{6} - \frac{1}{n} + O(n^{-2}) \right) \\ &= n - O(1) \\ &= O(n) \end{aligned} \tag{3}$$

Since $\mu(k) \leq 1$, we can discard this factor when applying Eqs. (2) and (3) to get the asymptotic behaviour of Eq. (1); this yields

$$\begin{aligned} q_n - \sum_{k\geq 1} \mu(k) \left(\frac{n}{k}\right)^2 &= \sum_{k=1}^{n} O(n/k) - O(n) \\ &= O(nH_n) - O(n), \end{aligned}$$

where $H_n = \sum_{k=1}^{n} 1/k$ denotes the n-th harmonic number. Because both $O(nH_n)$ and $O(n)$ are $o(n^2)$, we can replace these terms by $o(n^2)$ and divide by n^2 to arrive at

$$\frac{q_n}{n^2} - \sum_{k\geq 1} \frac{\mu(k)}{k^2} = o(1).$$

This means that for any real $\epsilon > 0$, we can find a number n_0 such that for all $n \geq n_0$ the difference $|q_n - \sum_{k\geq 1} \mu(k)/k^2| \leq \epsilon$; the sequence q_n/n^2 converges exactly as stated by the lemma. ∎

We now know that q_n/n^2 tends to the mysterious summation $\sum_{k\geq 1} \mu(k)/k^2$ as n approaches infinity. Before we may compute the value of this summation, we need the following theorem, whose proof is simple enough that it may be included as well.

Theorem M. *The sum $\sum_{d\backslash n} \mu(d)$, taken over all integers d that divide n, equals 1 when $n = 1$ and equals 0 for all integers $n > 1$.*

Proof. The case $n = 1$ is obviously true, so let $n > 1$. By the fundamental theorem of arithmetic, $n = p_1^{e_1} p_2^{e_2} \cdots p_k^{e_k}$. Only square-free divisors contribute to the sum $\sum_{d\backslash n} \mu(d)$, so we have

$$\sum_{d\backslash n} \mu(d) = \mu(1) + \sum_{1\leq i\leq k} \mu(p_i) + \sum_{1\leq i<j\leq k} \mu(p_i p_j) + \cdots + \mu(p_1 \cdots p_k).$$

Since the magnitude of $\mu(d)$ is 1 (whenever d is square-free) and the sign of $\mu(d)$ depends on the number of primes that make up d, this can be re-expressed as the alternating sum of binomial coefficients

$$\sum_{d\backslash n} \mu(d) = \binom{k}{0} - \binom{k}{1} + \binom{k}{2} - \cdots + (-1)^k \binom{k}{k}.$$

which equals 0. (We will not prove this claim, but one may be convinced of this fact by trying it out on a couple of rows of Pascal's Triangle.) ∎

We are now ready for the final lemma.

Lemma C.

$$\left(\sum_{k\geq 1} \frac{\mu(k)}{k^2}\right)\left(\sum_{m\geq 1} \frac{1}{m^2}\right) = 1$$

.

Proof. Both series in the product are absolutely convergent, so we may make use of the identity

$$\left(\sum_{k\geq 1} \frac{a_k}{k^z}\right)\left(\sum_{m\geq 1} \frac{b_m}{m^z}\right) = \sum_{n\geq 1} \left(\sum_{d\backslash n} a_d b_{n/d}\right) \Big/ n^z,$$

setting $a_k = \mu(k)$, $b_m = 1$, and $z = 2$. This yields

$$\left(\sum_{k\geq 1} \frac{\mu(k)}{k^2}\right)\left(\sum_{m\geq 1} \frac{1}{m^2}\right) = \sum_{n\geq 1} \left(\sum_{d\backslash n} \mu(d) \cdot 1\right) \Big/ n^2.$$

As a result of Theorem M, the only non-zero term in the sum on the right-hand side occurs when $n = 1$, so the product simplifies to $\mu(1)/1^2 = 1$. ∎

Since $\sum_{m\geq 1} 1/m^2 = \pi^2/6$, we must have

$$\sum_{k\geq 1} \frac{\mu(k)}{k^2} = \frac{6}{\pi^2} \approx 60.8\%,$$

and this is the probability that two random integers are relatively prime.