Chapter 2
The Asymptotic Density of Relatively Prime Pairs and of Square-Free Numbers

Pick a positive integer at random. What is the probability of it being even? As stated, this question is not well posed, because there is no uniform probability measure on the set $\mathbb{N}$ of positive integers. However, what one can do is fix a positive integer n, and choose a number uniformly at random from the finite set $[n] = \{1, \ldots, n\}$. Letting ρ_n denote the probability that the chosen number was even, we have $\lim_{n\to\infty} \rho_n = \frac{1}{2}$, and we say that the *asymptotic density* of even numbers is equal to $\frac{1}{2}$.

In this spirit, we ask: *if one selects two positive integers at random, what is the probability that they are relatively prime?* Fixing n, we choose two positive integers uniformly at random from $[n]$. Of course, there are two natural ways to interpret this. Do we choose a number uniformly at random from $[n]$ and then choose a second number uniformly at random from the remaining $n - 1$ integers, or, alternatively, do we select the second number again from $[n]$, thereby allowing for doubles? The answer is that it doesn't matter, because under the second alternative the probability of getting doubles is only $\frac{1}{n}$, and this doesn't affect the asymptotic probability. Here is the theorem we will prove.

Theorem 2.1. *Choose two integers uniformly at random from* $[n]$. *As* $n \to \infty$, *the asymptotic probability that they are relatively prime is* $\frac{6}{\pi^2} \approx 0.6079$.

We will give two very different proofs of Theorem 2.1: one completely number theoretic and one completely probabilistic. The number theoretic proof is elegant even a little magical. However, it does require the preparation of some basic number theoretic tools, and it provides little intuition. The number theoretic proof gives the asymptotic probability as $(\sum_{n=1}^{\infty} \frac{1}{n^2})^{-1}$. The well-known fact that $\sum_{n=1}^{\infty} \frac{1}{n^2} = \frac{\pi^2}{6}$ is proved in Appendix D. The probabilistic proof requires very little preparation; it is enough to know just the most rudimentary notions from discrete probability theory: probability space, event, and independence. A heuristic, non-rigorous version of the probabilistic proof provides a lot of intuition, some of which the reader might find obscured in the rigorous proof. The probabilistic proof gives the asymptotic probability as $\prod_{k=1}^{\infty}(1 - \frac{1}{p_k^2})$, where $\{p_k\}_{k=1}^{\infty}$ is an enumeration of the primes. One

R.G. Pinsky, *Problems from the Discrete to the Continuous*, Universitext,
DOI 10.1007/978-3-319-07965-3_2,

then must use the Euler product formula to show that this is equal to $(\sum_{n=1}^{\infty} \frac{1}{n^2})^{-1}$. We will first give the number theoretic proof and then give the heuristic and the rigorous probabilistic proofs.

The number theoretic ideas we develop along the way to our first proof of Theorem 2.1 will bring us close to proving another result, which we now describe. Every positive integer $n \geq 2$ can be factored uniquely as $n = p_1^{k_1} \cdots p_m^{k_m}$, where $m \geq 1$, $\{p_j\}_{j=1}^m$ are distinct primes, and $k_j \in \mathbb{N}$, for $j \in [m]$. If in this factorization, one has $k_j = 1$, for all $j \in [m]$, then we say that n is *square-free*. Thus, an integer $n \geq 2$ is square-free if and only if it is of the form $n = p_1 \cdots p_m$, where $m \geq 1$ and $\{p_j\}_{j=1}^m$ are distinct primes. The integer 1 is also called square-free. There are 61 square-free positive integers that are no greater than 100:
1,2,3,5,6,7,10,11,13,14,15,17,19,21,22,23,26,29,30,31,33,34,35,37,38,39,41,42,43,
46,47,51,53,55,57,58,59,61,62,65,66,67,69,70,71,73,74,77,78,79,82,83,85,86,
87,89,91,93,94,95,97.

Let $C_n = \{k : 1 \leq k \leq n,\ k \text{ is square-free}\}$. If $\lim_{n\to\infty} \frac{|C_n|}{n}$ exists, we call this limit the asymptotic density of square-free numbers. After giving the number theoretic proof of Theorem 2.1, we will prove the following theorem.

Theorem 2.2. *The asymptotic density of square-free integers is* $\frac{6}{\pi^2} \approx 0.6079$.

For the number theoretic proof of Theorem 2.1, the first alternative suggested above in the second paragraph of this chapter will be more convenient. In fact, once we have chosen the two distinct integers, it will be convenient to order them by size; thus, we may consider the set B_n of all possible (and equally likely) outcomes to be

$$B_n = \{(j,k) : 1 \leq j < k \leq n\}.$$

Let $A_n \subset B_n$ denote those pairs which are relatively prime:

$$A_n = \{(j,k) : 1 \leq j < k \leq n,\ \gcd(j,k) = 1\}.$$

Then the probability q_n that the two selected integers are relatively prime is

$$q_n = \frac{|A_n|}{|B_n|} = \frac{2|A_n|}{n(n-1)}. \tag{2.1}$$

We proceed to develop a circle of ideas that will facilitate the calculation of $\lim_{n\to\infty} q_n$ and thus give a proof of Theorem 2.1. A function $a : \mathbb{N} \to \mathbb{R}$ is called an *arithmetic* function. The *Möbius function* μ is the arithmetic function defined by

$$\mu(n) = \begin{cases} 1, \text{ if } n = 1; \\ (-1)^m, \text{ if } n = \prod_{j=1}^m p_j, \text{ where } \{p_j\}_{j=1}^m \text{ are distinct primes;} \\ 0, \text{ otherwise.} \end{cases}$$

Thus, for example, we have $\mu(3) = -1, \mu(15) = 1$, and $\mu(12) = 0$.

Given arithmetic functions a and b, we define their *convolution* $a * b$ to be the arithmetic function satisfying

$$(a * b)(n) = \sum_{d|n} a(d)b(\frac{n}{d}),\ n \in \mathbb{N}.$$

Clearly, $a * b = b * a$. The convolution arises naturally in the following context. Define formally

$$f(x) = \sum_{n=1}^{\infty} \frac{a(n)}{n^x} \tag{2.2}$$

and

$$g(x) = \sum_{n=1}^{\infty} \frac{b(n)}{n^x}. \tag{2.3}$$

When we say "formally," what we mean is that we ignore questions of convergence and manipulate these infinite series according to the laws of addition, subtraction, multiplication, and division, which are valid for series with a finite number of terms and for absolutely convergent infinite series. Their formal product is given by

$$f(x)g(x) = \Big(\sum_{d=1}^{\infty} \frac{a(d)}{d^x}\Big)\Big(\sum_{k=1}^{\infty} \frac{b(k)}{k^x}\Big) = \sum_{d,k=1}^{\infty} \frac{a(d)b(k)}{(dk)^x} = \sum_{n=1}^{\infty} \frac{1}{n^x} \sum_{d,k\,:\,dk=n} a(d)b(k)$$

$$= \sum_{n=1}^{\infty} \frac{1}{n^x} \sum_{d|n} a(d)b(\frac{n}{d}) = \sum_{n=1}^{\infty} \frac{(a * b)(n)}{n^x}. \tag{2.4}$$

If the series on the right hand side of (2.2) and (2.3) are in fact absolutely convergent, then the series on the right hand side of (2.4) is also absolutely convergent. In such case, the equality $\big(\sum_{d=1}^{\infty} \frac{a(d)}{d^x}\big)\big(\sum_{k=1}^{\infty} \frac{b(k)}{k^x}\big) = \sum_{n=1}^{\infty} \frac{(a*b)(n)}{n^x}$ is a rigorous statement in mathematical analysis.

An arithmetic function a is called *multiplicative* if $a(nm) = a(n)a(m)$ whenever $\gcd(n, m) = 1$. It follows that if $a \not\equiv 0$ is multiplicative, then $a(1) = 1$. If $a \not\equiv 0$ is multiplicative, then it is completely determined by its values on the prime powers; indeed, if $n = \prod_{j=1}^{m} p_j^{k_j}$ is the factorization of n into a product of distinct prime powers, then $a(n) = a(\prod_{j=1}^{m} p_j^{k_j}) = \prod_{j=1}^{m} a(p_j^{k_j})$.

It is trivial to verify that μ is multiplicative. For the first proposition below, the following lemma will be useful.

Lemma 2.1. *The arithmetic function* $\sum_{d|n} \mu(d)$ *is multiplicative.*

Proof. Let n and m be positive integers satisfying $\gcd(n, m) = 1$. We have

$$\sum_{d_1|n}\mu(d_1)\sum_{d_2|m}\mu(d_2)=\sum_{d_1|n,d_2|m}\mu(d_1)\mu(d_2)=\sum_{d_1|n,d_2|m}\mu(d_1d_2)=\sum_{d|nm}\mu(d),$$

where the second equality follows from the fact that μ is multiplicative and the fact that if $\gcd(n,m)=1$, $d_1|n$ and $d_2|m$, then $\gcd(d_1,d_2)=1$, while the final equality follows from the fact that if $\gcd(n,m)=1$ and $d|nm$, then d can be written as $d=d_1d_2$ for a unique pair d_1,d_2 satisfying $d_1|n$ and $d_2|m$. (The reader should verify these facts.) □

We introduce three more arithmetic functions that will be used in the sequel:

$$1(n)=1,\ \text{for all } n;\quad i(n)=n,\ \text{for all } n;\quad e(n)=\begin{cases}1, & \text{if } n=1;\\ 0, & \text{otherwise.}\end{cases}$$

Note that $a*e=a$, for all a, and that $(a*1)(n)=\sum_{d|n}a(d)$. A key result we need is the *Möbius inversion formula.*

Proposition 2.1. *Let a be an arithmetic function. Define $b=a*1$. Then $a=b*\mu$.*

Remark. Written out explicitly, the theorem asserts that if

$$b(n):=\sum_{d|n}a(d),$$

then $a(n)=\sum_{d|n}b(d)\mu(\frac{n}{d})$.

Proof. To prove the proposition, it suffices to prove that

$$1*\mu=e. \tag{2.5}$$

Indeed, using this along with the easily verified associativity of the convolution, we have

$$b*\mu=(a*1)*\mu=a*(1*\mu)=a*e=a.$$

We now prove (2.5). We have

$$(1*\mu)(n)=(\mu*1)(n)=\sum_{d|n}\mu(d).$$

By Lemma 2.1, the function $\sum_{d|n}\mu(d)$ is multiplicative. Clearly, the function e is multiplicative. Obviously, $e(1)=1$ and $e(p^k)=0$, for any prime p and any positive integer k. We have $\sum_{d|1}\mu(d)=\mu(1)=1$. Thus, since a nonzero,

multiplicative, arithmetic function is completely determined by its values on prime powers, to complete the proof that $1 * \mu = e$, it suffices to show that $\sum_{d|p^k} \mu(d) = 0$. We have $\sum_{d|p^k} \mu(d) = \sum_{j=0}^{k} \mu(p^j) = \mu(1) + \mu(p) = 1 - 1 = 0$. □

We introduce one final arithmetic function—the well-known *Euler ϕ-function*:

$$\phi(n) = |\{j : 1 \le j \le n,\ \gcd(j,n) = 1\}|.$$

That is, $\phi(n)$ counts the number of positive integers less than or equal to n which are relatively prime to n. For our calculation of $\lim_{n\to\infty} q_n$, we will use a result that is a corollary of the following proposition.

Proposition 2.2. *$\phi * 1 = i$; that is,*

$$\sum_{d|n} \phi(d) = n.$$

From Proposition 2.2 and the Möbius inversion formula, the following corollary is immediate.

Corollary 2.1. *$\mu * i = \phi$; that is,*

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

Remark. For the proofs of Theorems 2.1 and 2.2, we do not need Proposition 2.2, but only Corollary 2.1. In Exercise 2.1, the reader is guided through a direct proof of the corollary. The proof also will reveal why the seemingly strange Möbius function has such nice properties.

Proof of Proposition 2.2. Let $d|n$. It is easy to see that $\phi(d)$ is equal to the number of $k \in [n]$ satisfying $\gcd(k,n) = \frac{n}{d}$. Indeed, $k \in [n]$ satisfies $\gcd(k,n) = \frac{n}{d}$ if and only if $k = j(\frac{n}{d})$, for some $j \in [d]$ satisfying $\gcd(d, j) = 1$. (The reader should verify this.) Also, clearly, every $k \in [n]$ satisfies $\gcd(k,n) = \frac{n}{d}$ for some $d|n$. The proposition follows from these facts. □

Remark. For an alternative proof of Proposition 2.2, exactly in the spirit of Lemma 2.1 and the proof of (2.5), see Exercise 2.2.

We are now in a position to prove Theorem 2.1.

Number Theoretic Proof of Theorem 2.1. For each $k \ge 2$, there are $\phi(k)$ integers j satisfying $1 \le j < k$ and $\gcd(j,k) = 1$. Thus,

$$|A_n| = |\{(j,k) : 1 \le j < k \le n,\ \gcd(j,k) = 1\}| = \sum_{k=2}^{n} \phi(k).$$

Therefore, from (2.1), we have

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

To calculate

$$\lim_{n\to\infty} q_n = \lim_{n\to\infty} \frac{2\sum_{k=2}^{n}\phi(k)}{n(n-1)}, \tag{2.6}$$

we analyze the behavior of the sum $\sum_{k=1}^{n}\phi(k)$ for large n.

Remark. The function ϕ can be written explicitly as

$$\phi(n) = n\prod_{p|n}(1-\frac{1}{p}),\ n \geq 2, \tag{2.7}$$

where $\prod_{p|n}$ indicates that the product is over all primes that divide n; see Exercise 2.3. However, this formula is of no help whatsoever for analyzing the above sum.

We will use Corollary 2.1 to analyze $\sum_{k=1}^{n}\phi(k)$. From Corollary 2.1, we have

$$\sum_{k=1}^{n}\phi(k) = \sum_{k=1}^{n}(\mu * i)(k) = \sum_{k=1}^{n}\sum_{d|k}\mu(d)\frac{k}{d} =$$

$$\sum_{k=1}^{n}\sum_{dd'=k} d'\mu(d) = \sum_{d=1}^{n}\mu(d)\sum_{d'\leq\frac{n}{d}} d'.$$

Since $\sum_{j=1}^{m} j = \frac{1}{2}m(m+1)$, we have

$$\sum_{k=1}^{n}\phi(k) = \sum_{d=1}^{n}\mu(d)\sum_{d'\leq\frac{n}{d}} d' = \frac{1}{2}\sum_{d=1}^{n}\mu(d)[\frac{n}{d}]([\frac{n}{d}]+1). \tag{2.8}$$

We have $[\frac{n}{d}]([\frac{n}{d}]+1) \leq \frac{n}{d}(\frac{n}{d}+1) = (\frac{n}{d})^2 + \frac{n}{d}$, and $[\frac{n}{d}]([\frac{n}{d}]+1) \geq (\frac{n}{d}-1)\frac{n}{d} = (\frac{n}{d})^2 - \frac{n}{d}$; thus,

$$(\frac{n}{d})^2 - \frac{n}{d} \leq [\frac{n}{d}]([\frac{n}{d}]+1) \leq (\frac{n}{d})^2 + \frac{n}{d}.$$

Substituting this two-sided inequality in (2.8), we obtain

$$\frac{n^2}{2}\sum_{d=1}^{n}\frac{\mu(d)}{d^2} - \frac{n}{2}\sum_{d=1}^{n}\frac{\mu(d)}{d} \leq \sum_{k=1}^{n}\phi(k) \leq \frac{n^2}{2}\sum_{d=1}^{n}\frac{\mu(d)}{d^2} + \frac{n}{2}\sum_{d=1}^{n}\frac{\mu(d)}{d}. \tag{2.9}$$

Now

$$|\sum_{d=1}^{n} \frac{\mu(d)}{d}| \leq \sum_{d=1}^{n} \frac{1}{d} = 1 + \sum_{d=2}^{n} \frac{1}{d} \leq 1 + \log n, \tag{2.10}$$

since the final sum is a lower Riemann sum for $\int_1^n \frac{1}{x}\, dx$. From (2.9) and (2.10), we obtain

$$\lim_{n\to\infty} \frac{\sum_{k=2}^{n} \phi(k)}{n(n-1)} = \frac{1}{2} \sum_{d=1}^{\infty} \frac{\mu(d)}{d^2}. \tag{2.11}$$

It remains to evaluate $\sum_{d=1}^{\infty} \frac{\mu(d)}{d^2}$. On the face of it, from the definition of μ, it would seem very difficult to evaluate this explicitly. However, Möbius inversion saves the day. Consider (2.2)–(2.4) with $a = 1$ and $b = \mu$ and with $x = 2$. With these choices, the right hand sides of (2.2) and (2.3) are absolutely convergent. By (2.5), we have $1 * \mu = e$; that is, $a * b = e$. Therefore, we conclude from (2.2)–(2.4) that

$$\left(\sum_{d=1}^{\infty} \frac{1}{d^2}\right)\left(\sum_{d=1}^{\infty} \frac{\mu(d)}{d^2}\right) = 1. \tag{2.12}$$

Recall the well-known formula

$$\sum_{n=1}^{\infty} \frac{1}{n^2} = \frac{\pi^2}{6}. \tag{2.13}$$

We give a completely elementary proof of this fact in Appendix D. From (2.12) and (2.13) we obtain

$$\sum_{d=1}^{\infty} \frac{\mu(d)}{d^2} = \frac{6}{\pi^2}. \tag{2.14}$$

Using (2.14) with (2.11) and (2.6) gives

$$\lim_{n\to\infty} q_n = \frac{6}{\pi^2},$$

completing the proof of the theorem. □

Remark. If a is an arithmetic function and f is a nondecreasing function, we say that the function f is the *average order* of the arithmetic function a if $\frac{1}{n}\sum_{k=1}^{n} a(k) = f(n) + o(f(n))$. Of course this doesn't uniquely define f; we usually choose a particular such f which has a simple form. From (2.11) and (2.14), it follows that the average order of the Euler ϕ-function is $\frac{3n}{\pi^2}$.

We now turn to Theorem 2.2.

Proof of Theorem 2.2. From the definition of the Möbius function, it follows that

$$\mu^2(n) = \begin{cases} 1, & \text{if } n \text{ is square-free;} \\ 0, & \text{otherwise.} \end{cases} \tag{2.15}$$

Thus, letting

$$A_n = \{j \in [n] : j \text{ is square-free}\},$$

we have

$$|A_n| = \sum_{j=1}^{n} \mu^2(j). \tag{2.16}$$

To prove the theorem, we need to show that

$$\lim_{n\to\infty} \frac{|A_n|}{n} = \frac{6}{\pi^2}. \tag{2.17}$$

We need the following lemma.

Lemma 2.2.

$$\mu^2(n) = \sum_{k^2|n} \mu(k).$$

Proof. Let $\Lambda(n) := \sum_{k^2|n} \mu(k)$. If n is square-free, then the only integer k that satisfies $k^2|n$ is $k = 1$. Thus, since $\mu(1) = 1$, we have $\Lambda(n) = 1$. On the other hand, if n is not square-free, then n can be written in the form $n = m^2 l$, where $m > 1$ and l is square-free. Now $k^2|m^2 l$ if and only if $k|m$. (The reader should verify this.) Thus, we have

$$\Lambda(n) = \sum_{k^2|n} \mu(k) = \sum_{k^2|m^2 l} \mu(k) = \sum_{k|m} \mu(k) = (\mu * 1)(m) = 0,$$

where the last equality follows from (2.5). The lemma now follows from (2.15). □

Using Lemma 2.2, we have

$$\sum_{j=1}^{n} \mu^2(j) = \sum_{j=1}^{n} \sum_{k^2|j} \mu(k). \tag{2.18}$$

If $k^2 > n$, then $\mu(k)$ will not appear on the right hand side of (2.18). If $k^2 \le n$, then $\mu(k)$ will appear on the right hand side of (2.18) $[\frac{n}{k^2}]$ times, namely, when $j = k^2, 2k^2, \ldots, [\frac{n}{k^2}]k^2$. Thus, we have

$$\sum_{j=1}^{n} \mu^2(j) = \sum_{j=1}^{n} \sum_{k^2|j} \mu(k) = \sum_{k^2 \le n} [\frac{n}{k^2}]\, \mu(k) = \sum_{k \le [n^{\frac{1}{2}}]} [\frac{n}{k^2}]\, \mu(k) =$$

$$n \sum_{k \le [n^{\frac{1}{2}}]} \frac{\mu(k)}{k^2} + \sum_{k \le [n^{\frac{1}{2}}]} \Big([\frac{n}{k^2}] - \frac{n}{k^2}\Big)\mu(k). \tag{2.19}$$

Since each summand in the second term on the right hand side of (2.19) is bounded in absolute value by 1, we have

$$|\sum_{k \le [n^{\frac{1}{2}}]} \Big([\frac{n}{k^2}] - \frac{n}{k^2}\Big)\mu(k)| \le n^{\frac{1}{2}}. \tag{2.20}$$

It follows from (2.16), (2.19), and (2.20) that

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

Using this with (2.14) gives (2.17) and completes the proof of the theorem. □

We now give a heuristic probabilistic proof and a rigorous probabilistic proof of Theorem 2.1. In the heuristic proof, we put quotation marks around the steps that are not rigorous.

Heuristic Probabilistic Proof of Theorem 2.1. Let $\{p_k\}_{k=1}^{\infty}$ be an enumeration of the primes. In the spirit described in the first paragraph of the chapter, if we pick a positive integer "at random," then the "probability" of it being divisible by the prime number p_k is $\frac{1}{p_k}$. (Of course, this is true also with p_k replaced by an arbitrary positive integer.) If we pick two positive integers "independently," then the "probability" that they are both divisible by p_k is $\frac{1}{p_k}\frac{1}{p_k} = \frac{1}{p_k^2}$, by "independence." So the "probability" that at least one of them is not divisible by p_k is $1 - \frac{1}{p_k^2}$. The "probability" that a "randomly" selected positive integer is divisible by the two distinct primes, p_j and p_k, is $\frac{1}{p_j p_k} = \frac{1}{p_j}\frac{1}{p_k}$. (The reader should check that this "holds" more generally if p_j and p_k are replaced by an arbitrary pair of relatively prime positive integers, but not otherwise.) Thus, the events of *being divisible by* p_j and *being divisible by* p_k are "independent." Now two "randomly" selected positive integers are relatively prime if and only if, for every k, at least one of the integers is not divisible by p_k. But since the "probability" that at least one of them is not divisible by p_k is $1 - \frac{1}{p_k^2}$, and since being divisible by a prime p_j and being divisible

by a different prime p_k are "independent" events, the "probability" that the two "randomly" selected positive integers are such that, for every k, at least one of them is not divisible by p_k is $\prod_{k=1}^{\infty}(1-\frac{1}{p_k^2})$. Thus, this should be the "probability" that two "randomly" selected positive integers are relatively prime. □

Rigorous Probabilistic Proof of Theorem 2.1. For the probabilistic proof, the second alternative suggested in the second paragraph of the chapter will be more convenient. Thus, we choose an integer from $[n]$ uniformly at random and then choose a second integer from $[n]$ uniformly at random. Let $\Omega_n = [n]$. The appropriate probability space on which to analyze the model described above is the space $(\Omega_n \times \Omega_n, P_n)$, where the probability measure P_n on $\Omega_n \times \Omega_n$ is the uniform measure; that is, $P_n(A) = \frac{|A|}{n^2}$, for any $A \subset \Omega_n \times \Omega_n$. The point $(i, j) \in \Omega_n \times \Omega_n$ indicates that the integer i was chosen the first time and the integer j was chosen the second time. Let C_n denote the event that the two selected integers are relatively prime; that is,

$$C_n = \{(i, j) \in \Omega_n \times \Omega_n : \gcd(i, j) = 1\}.$$

Then the probability q_n that the two selected integers are relatively prime is

$$q_n = P_n(C_n) = \frac{|C_n|}{n^2}.$$

Let $\{p_k\}_{k=1}^{\infty}$ denote the prime numbers arranged in increasing order. (Any enumeration of the primes would do, but for the proof it is more convenient to choose the increasing enumeration.) For each $k \in \mathbb{N}$, let $B_{n;k}^1$ denote the event that the first integer chosen is divisible by p_k and let $B_{n;k}^2$ denote the event that the second integer chosen is divisible by p_k. That is,

$$B_{n;k}^1 = \{(i, j) \in \Omega_n \times \Omega_n : p_k | i\}, \quad B_{n;k}^2 = \{(i, j) \in \Omega_n \times \Omega_n : p_k | j\}.$$

Note of course that the above sets are empty if $p_k > n$. The event $B_{n;k}^1 \cap B_{n;k}^2 = \{(i, j) \in \Omega_n \times \Omega_n : p_k | i \text{ and } p_k | j\}$ is the event that both selected integers have p_k as a factor. There are $[\frac{n}{p_k}]$ integers in Ω_n that are divisible by p_k, namely, $p_k, 2p_k, \cdots, [\frac{n}{p_k}]p_k$. Thus, there are $[\frac{n}{p_k}]^2$ pairs $(i, j) \in \Omega_n \times \Omega_n$ for which both coordinates are divisible by p_k; therefore,

$$P_n(B_{n;k}^1 \cap B_{n;k}^2) = \frac{[\frac{n}{p_k}]^2}{n^2}. \tag{2.21}$$

Note that $\cup_{k=1}^{\infty}(B_{n;k}^1 \cap B_{n;k}^2) = \cup_{k=1}^{n}(B_{n;k}^1 \cap B_{n;k}^2)$ is the event that the two selected integers have at least one common prime factor. (The equality above follows from the fact that $B_{n;k}^1$ and $B_{n;k}^2$ are clearly empty for $k > n$.) Consequently, C_n can be expressed as

$$C_n = \big(\cup_{k=1}^n (B_{n;k}^1 \cap B_{n;k}^2)\big)^c = \cap_{k=1}^n (B_{n;k}^1 \cap B_{n;k}^2)^c,$$

where $A^c := \Omega_n \times \Omega_n - A$ denotes the complement of an event $A \subset \Omega_n \times \Omega_n$. Thus,

$$P_n(C_n) = P_n\big(\cap_{k=1}^n (B_{n;k}^1 \cap B_{n;k}^2)^c\big). \tag{2.22}$$

Let $R < n$ be a positive integer. We have

$$\cap_{k=1}^n (B_{n;k}^1 \cap B_{n;k}^2)^c = \cap_{k=1}^R (B_{n;k}^1 \cap B_{n;k}^2)^c - \cup_{k=R+1}^n (B_{n;k}^1 \cap B_{n;k}^2)$$

and, of course, $\cap_{k=1}^n (B_{n;k}^1 \cap B_{n;k}^2)^c \subset \cap_{k=1}^R (B_{n;k}^1 \cap B_{n;k}^2)^c$. Thus,

$$\begin{aligned} &P_n\big(\cap_{k=1}^R (B_{n;k}^1 \cap B_{n;k}^2)^c\big) - P_n\big(\cup_{k=R+1}^n (B_{n;k}^1 \cap B_{n;k}^2)\big) \le \\ &P_n\big(\cap_{k=1}^n (B_{n;k}^1 \cap B_{n;k}^2)^c\big) \le P_n\big(\cap_{k=1}^R (B_{n;k}^1 \cap B_{n;k}^2)^c\big). \end{aligned} \tag{2.23}$$

Using the sub-additivity property of probability measures for the first inequality below, and using (2.21) for the equality below, we have

$$P_n\big(\cup_{k=R+1}^n (B_{n;k}^1 \cap B_{n;k}^2)\big) \le \sum_{k=R+1}^n P_n\big(B_{n;k}^1 \cap B_{n;k}^2\big) = \sum_{k=R+1}^n \frac{[\frac{n}{p_k}]^2}{n^2} \le \sum_{k=R+1}^\infty \frac{1}{p_k^2}. \tag{2.24}$$

Up until now, we have made no assumption on n. Now assume that $p_k | n$, for $k = 1, \cdots, R$; that is, assume that n is a multiple of $\prod_{k=1}^R p_k$. Denote the set of such n by D_R; that is,

$$D_R = \{n \in \mathbb{N} : p_k | n \text{ for } k = 1, \cdots, R\}.$$

Recall that the event $B_{n;k}^1 \cap B_{n;k}^2$ is the event that both selected integers are divisible by k. We claim that if $n \in D_R$, then the events $\{B_{n;k}^1 \cap B_{n;k}^2\}_{k=1}^R$ are independent. That is, for any subset $I \subset \{1, 2, \cdots, R\}$, one has

$$P_n\big(\cap_{k\in I} (B_{n;k}^1 \cap B_{n;k}^2)\big) = \prod_{k\in I} P_n(B_{n;k}^1 \cap B_{n;k}^2), \text{ if } n \in D_R. \tag{2.25}$$

The proof of (2.25) is a straightforward counting exercise and is left as Exercise 2.4. If events $\{A_k\}_{k=1}^R$ are independent, then the complementary events $\{A_k^c\}_{k=1}^R$ are also independent. See Exercise A.3 in Appendix A. Thus, we conclude that

$$P_n\big(\cap_{k=1}^R (B_{n;k}^1 \cap B_{n;k}^2)^c\big) = \prod_{k=1}^R P_n\big((B_{n;k}^1 \cap B_{n;k}^2)^c\big), \text{ if } n \in D_R. \tag{2.26}$$

By (2.21) we have $P_n\big((B^1_{n;k} \cap B^2_{n;k})^c\big) = 1 - P_n(B^1_{n;k} \cap B^2_{n;k}) = 1 - \frac{[\frac{n}{p_k}]^2}{n^2}$, for any n. Thus, from the definition of D_R, we have

$$P_n\big((B^1_{n;k} \cap B^2_{n;k})^c\big) = 1 - \frac{1}{p_k^2}, \text{ if } n \in D_R. \tag{2.27}$$

From (2.22) to (2.24), (2.26), and (2.27), we conclude that

$$\prod_{k=1}^{R}(1-\frac{1}{p_k^2}) - \sum_{k=R+1}^{\infty}\frac{1}{p_k^2} \le P_n(C_n) \le \prod_{k=1}^{R}(1-\frac{1}{p_k^2}), \text{ for } R \in \mathbb{N} \text{ and } n \in D_R. \tag{2.28}$$

We now use (2.28) to obtain an estimate on $P_n(C_n)$ for general n. Let $n \ge \prod_{k=1}^{R} p_k$. Let n' denote the largest integer in D_R which is smaller or equal to n, and let n'' denote the smallest integer in D_R which is larger or equal to n. Since D_R is the set of positive multiples of $\prod_{k=1}^{R} p_k$, we obviously have

$$n' > n - \prod_{k=1}^{R} p_k \quad \text{and} \quad n'' < n + \prod_{k=1}^{R} p_k. \tag{2.29}$$

For any n, note that $n^2 P_n(C_n) = |C_n|$ is the number of pairs $(i, j) \in \Omega_n \times \Omega_n$ that are relatively prime. Obviously, the number of such pairs is increasing in n. Thus $(n')^2 P_{n'}(C_{n'}) \le n^2 P_n(C_n) \le (n'')^2 P_{n''}(C_{n''})$, or equivalently,

$$(\frac{n'}{n})^2 P_{n'}(C_{n'}) \le P_n(C_n) \le (\frac{n''}{n})^2 P_{n''}(C_{n''}). \tag{2.30}$$

Since $n', n'' \in D_R$, we conclude from (2.28)–(2.30) that

$$(\frac{n-\prod_{k=1}^{R} p_k}{n})^2 (\prod_{k=1}^{R}(1-\frac{1}{p_k^2}) - \sum_{k=R+1}^{\infty}\frac{1}{p_k^2}) < P_n(C_n) < (\frac{n+\prod_{k=1}^{R} p_k}{n})^2 \prod_{k=1}^{R}(1-\frac{1}{p_k^2}). \tag{2.31}$$

Letting $n \to \infty$ in (2.31), we obtain

$$\prod_{k=1}^{R}(1-\frac{1}{p_k^2}) - \sum_{k=R+1}^{\infty}\frac{1}{p_k^2} \le \liminf_{n\to\infty} P_n(C_n) \le \limsup_{n\to\infty} P_n(C_n) \le \prod_{k=1}^{R}(1-\frac{1}{p_k^2}). \tag{2.32}$$

Now (2.32) holds for arbitrary R; thus letting $R \to \infty$, we conclude that

$$\lim_{n\to\infty} P_n(C_n) = \prod_{k=1}^{\infty}(1-\frac{1}{p_k^2}). \tag{2.33}$$

The celebrated *Euler product formula* states that

$$\frac{1}{\prod_{k=1}^{\infty}(1-\frac{1}{p_k^r})} = \sum_{n=1}^{\infty}\frac{1}{n^r},\ r>1; \tag{2.34}$$

see Exercise 2.5. From (2.33), (2.34), and (2.13), we conclude that

$$\lim_{n\to\infty} q_n = \lim_{n\to\infty} P_n(C_n) = \frac{1}{\sum_{n=1}^{\infty}\frac{1}{n^2}} = \frac{6}{\pi^2}. \qquad \square$$

Exercise 2.1. Give a direct proof of Corollary 2.1. (Hint: The Euler ϕ-function $\phi(n)$ counts the number of positive integers that are less than or equal to n and relatively prime to n. We employ the *sieve method*, which from the point of view of set theory is the method of *inclusion–exclusion*. Start with a list of all n integers between 1 and n as potential members of the set of the $\phi(n)$ relatively prime integers to n. Let $\{p_j\}_{j=1}^m$ be the prime divisors of n. For any such p_j, the $\frac{n}{p_j}$ numbers $p_j, 2p_j, \ldots, \frac{n}{p_j}p_j$ are not relatively prime to n. So we should strike these numbers from our list. When we do this for each j, the remaining numbers on the list are those numbers that are relatively prime to n, and the size of the list is $\phi(n)$. Now we haven't necessarily reduced the size of our list to $N_1 := n - \sum_{j=1}^m \frac{n}{p_j}$, because some of the numbers we have deleted might be multiples of two different primes, p_i and p_j, in which case they were subtracted above twice. Thus we need to add back to N_1 all of the $\frac{n}{p_i p_j}$ multiples of $p_i p_j$, for $i \neq j$. That is, we now have $N_2 := N_1 + \sum_{i\neq j}\frac{n}{p_i p_j}$. Continue in this vein.

Exercise 2.2. This exercise presents an alternative proof to Proposition 2.2:

(a) Show that the arithmetic function $\sum_{d|n}\phi(d)$ is multiplicative. Use the fact that ϕ is multiplicative—see Exercise 2.3.
(b) Show that $\sum_{d|n}\phi(d) = n$, when n is a prime power.
(c) Conclude that Proposition 2.2 holds.

Exercise 2.3. The *Chinese remainder theorem* states that if n and m are relatively prime positive integers, and $a \in [n]$ and $b \in [m]$, then there exists a unique $c \in [nm]$ such that $c = a \bmod n$ and $c = b \bmod m$. (For a proof, see [27].) Use this to prove that the Euler ϕ-function is multiplicative. Then use the fact that ϕ is multiplicative to prove (2.7).

Exercise 2.4. Prove (2.25).

Exercise 2.5. Prove the Euler product formula (2.34). (Hint: Let N_ℓ denote the set of positive integers all of whose prime factors are in the set $\{p_k\}_{k=1}^{\ell}$. Using the fact that

$$\frac{1}{1-\frac{1}{p_k^r}} = \sum_{m=0}^{\infty}\frac{1}{p_k^{rm}},$$

for all $k \in \mathbb{N}$, first show that $\frac{1}{1-\frac{1}{p_1^r}} \frac{1}{1-\frac{1}{p_2^r}} = \sum_{n \in N_2} \frac{1}{n^r}$, and then show that $\prod_{k=1}^{\ell} \frac{1}{1-\frac{1}{p_k^r}} = \sum_{n \in N_\ell} \frac{1}{n^r}$, for any $\ell \in \mathbb{N}$.)

Exercise 2.6. Using Theorem 2.1, prove the following result: Let $2 \leq d \in \mathbb{N}$. Choose two integers uniformly at random from $[n]$. As $n \to \infty$, the asymptotic probability that their greatest common divisor is d is $\frac{6}{d^2\pi^2}$.

Exercise 2.7. Give a probabilistic proof of Theorem 2.2.

Chapter Notes

It seems that Theorem 2.1 was first proven by E. Cesàro in 1881. A good source for the results in this chapter is Nathanson's book [27]. See also the more advanced treatment of Tenenbaum [33], which contains many interesting and nontrivial exercises. The heuristic probabilistic proof of Theorem 2.1 is well known and can be found readily, including via a Google-search. I am unaware of a rigorous probabilistic proof in the literature.

http://www.springer.com/978-3-319-07964-6

Problems from the Discrete to the Continuous
Probability, Number Theory, Graph Theory, and Combinatorics

Pinsky, R.

2014, XIII, 154 p. 8 illus. in color., Softcover
ISBN: 978-3-319-07964-6