# Dice and divisors

Valentin Rousselet

June 14, 2023

**Problem.** Rolling two 100-sided dice, what are the odds of getting numbers that share exactly three divisors?

Let $N \geq 1$ be the dice number and $k > 0$ the number of shared factors. How many pairs $P_k(N)$ of integers $1 \leq n \leq N$ share exactly $k$ factors?

**Preliminaries** In the following discussion, a number's divisors include 1 and itself. For example, the factors of 6 are 1,2,3, and 6. For this reason, any two numbers will always have at least 1 as a common divisor.
For any number $N$ we denote by $s_k(N)$ how many integers $1 \leq n \leq N$ share k factors with $N$. For example for $N = 10$ and $k = 2$: 10 shares factors $(1,2)$ wih four integers (2,4,6, and 8) and shares factors (1,5) with 5. Any other odd integer will not share any factor other than 1 with 10, and 10 itself shares four with itself $(1,2,5, \text{and } 10)$. Thus $\sigma(10, 2) = 5$
When studying common factors in pairs of integers, a useful number is their their greatest common divisor (GCD) and its divisors.

**Lemma 1.** Let $x$ and $y \in \mathbb{N}$. $x$ and $y$ share exactly $k$ factors if and only if their GCD has exactly $k$ factors.

*Proof.* This comes directly from the fact that any common divisor of $x$ and $y$ must be a divisor of $\gcd(x, y)$. □

In the following, we will prove formulas for $k = 1, 2, 3$, by induction on $N$. Making use of the idea that when going from $N - 1$ to $N$, we must add to the previous count $P(N - 1, k)$ the pairs of the form $(x, N)$ and $(N, y)$ for any $x, y \leq N$, of which there are $s(N, k)$ However, if $(N, N)$ is a valid pair, then we must substract 1. We thus derive the following recurrence relation:

**Lemma 2.** Let $N > 1$ and $1 \leq k < N$.

$$P_k(N) = P_k(N-1) + 2\,s_k(N) - \begin{cases} 1 & \text{if } (N, N) \text{ shares } k \text{ factors} \\ 0 & \text{otherwise} \end{cases}$$

## Case $k = 1$

In this case, $x$ and $y$ share exactly one factor: 1. By using Lemma 1, this is equivalent to $\gcd(x, y) = 1$: in other words $x$ and $y$ share one factor if and only if they are coprime.
We introduce $\phi$, Euler's totient function, where $\phi(n)$ counts coprimes less than or equal to $n$. yielding immediately:

$$s_1(N) = \phi(N)$$

We can then state the result for $k = 1$:

**Theorem 1.**

$$P_1(N) = 2\left(\sum_{n=1}^{N} \phi(n)\right) - 1$$

*Proof.* We prove this theorem by induction.
Firstly, we check that $P_1(1) = 1$, that is the formula is true for $N = 1$, as there is exactly one pair of coprime numbers: $(1, 1)$ and $\phi(1) = 1$

Next, assume the formula holds for $N-1$, $N > 1$. Using lemma 2, to count the additional pairs, we have

$$P_1(N) = P_1(N-1) + 2\phi(N)$$

Note that the pair $(N, N)$ is never counted twice, since $N > 1$ cannot be coprime with itself. Therefore, substituting $P_1(N-1)$ from our inductive hypothesis

$$P_1(N) = 2\left(\sum_{n=1}^{N} \phi(n)\right) - 1$$

$\square$

## Case $k = 2$

**Lemma 3.** Let $x$ and $y$ be two positive integers. $x$ and $y$ share exactly two divisors if and only if their GCD $p$ is prime and $\gcd(\frac{x}{p}, \frac{y}{p}) = 1$

*Proof.* Suppose $x$ and $y$ share exactly two divisors: 1 and $p$. By lemma 1, this means that $\gcd(x, y) = p$ has exactly two divisors, so $p$ is a prime number.
If we denote $a = \frac{x}{p}$ and $b = \frac{y}{p}$, we show that $a$ and $b$ must be coprime. Since $\gcd(a, b) \mid a$ and $a \mid x$ then $\gcd(a, b) \mid x$; similarly $\gcd(a, b) \mid y$. Therefore $\gcd(a, b)$ is a common factor of $x$ and $y$, and thus is either 1 or $p$. However it cannot be $p$; otherwise, $p^2$ would divide $x$ and $y$.
Conversely, if $p$ is a prime and $a$ and $b$ are two coprime positive integers, $pa$ and $pb$ share exactly two factors, 1 and $p$. Suppose there is a third common factor $q \neq 1$. Since $p$ is prime then $q \mid a$ and $q \mid b$, so $q \mid \gcd(a, b)$, which is contradicts $a$ and $b$ being coprime. $\square$

Denoting $\pi(n)$ as the function counting the number of primes less than $n$, we can write the formula for $P_2$

**Theorem 2.**

$$P_2(N) = 2\left(\sum_{n=1}^{N} \sum_{p|n} \phi(\frac{n}{p})\right) - \pi(N)$$

where $\sum_{p|n}$ means summing over all primes that divide $n$

*Proof.* Similarly to the previous section, we prove this formula by induction. For $N = 1$ there are no pairs that share two factors since $(1, 1)$ has only one factor. Thus $P_2(1) = 0$.
Next, we assume the formula holds for $N-1$ with $N > 1$. To use the recurrence of lemma 2 we must express $s_2(N)$
By lemma 3 $(x, N)$ share two factors if their GCD is a prime number $p$, thus $p$ must be a prime factor of $N$.
The numbers $x$ sharing factors $(1, p)$ with $N$ are numbers of the form $p \times a$ where $a$ must be coprime with $\frac{N}{p}$. For a given prime divisor $p$ of $N$ there are exactly $\phi(\frac{N}{p})$ numbers coprime with the quotient.

$$s_2(N) = \sum_{p|N} \phi(\frac{N}{p})$$

To apply the recurrence relation we must check the pair $(N, N)$. It shares two factors if and only if $\gcd(N, N) = N$ is a prime number. It follows that we doubled counted $(N, N)$ if and only if $N$ is prime.
We distinguish the two cases:

- if $N$ is not prime, then $(N, N)$ shares more than two factors, so this pair will not be double-counted; and we have

$$P_2(N) = P_2(N-1) + 2\sum_{p|N} \phi(\frac{N}{p})$$

  Since in this case, $\pi(N) = \pi(N-1)$ the formula holds.

- if $N$ is prime, then it has only one prime factor, (which is $N$ itself).

$$\sum_{p|N} \phi(\frac{N}{p}) = \phi(1) = 1$$

in this case, $\pi(N) = \pi(N-1) + 1$ so we can write

$$\begin{aligned} P_2(N) &= P_2(N-1) + 1 \\ &= P_2(N-1, 2) + 2\sum_{p|N} \phi(\frac{N}{p}) - 1 \\ &= 2\left(\sum_{n=1}^{N} \sum_{p|n} \phi(\frac{n}{p})\right) - \pi(N-1) - 1 \\ &= 2\left(\sum_{n=1}^{N} \sum_{p|n} \phi(\frac{n}{p})\right) - \pi(N) \end{aligned}$$

□

## Case $k = 3$

**Lemma 4.** Let $(x, y)$ be two positive integers. They share exactly three divisors if and only if their GCD is the square of a prime $p$ and if $\frac{x}{p^2}$ and $\frac{y}{p^2}$ are coprime.

*Proof.* Suppose $x$ and $y$ share exactly three divisors. By lemma 1 their $gcd$ has exactly three divisors. This implies that $g = \gcd(x, y) > 1$, and therefore $x$ and $y$ are not coprime. Since $g > 1$ we already know two distinct divisors of $g$ : 1 and $g$ itself. This means there is a third divisor $p$ such that $1 < p < g$.
We then show that $p$ is prime. If $p$ was composite, then any non trivial divisor of $p$ would also divide $g$, which contradicts $g$ having only $\{1, p, g\}$ as divisors.
Since $p \mid g$, so does $\frac{g}{p}$; it must be one of the three divisors of $g$. It can neither be 1 or $g$, since $p \neq 1$ and $p \neq g$. Thus $\frac{g}{p} = p$ and $g = p^2$.
Similarly to the $k = 2$ case, we define the quotients $a = \frac{x}{p^2}$ and $b = \frac{y}{p^2}$. $x$ and $y$ are both divisible by $\gcd(a, b)$, therefore it also must be in $\{1, p, p^2\}$. But $p \nmid \gcd(a, b)$. If that was the case then $p^3$ would be a divisor of $x$ and $y$. So $\gcd(a, b)$ can neither be $p$ nor $p^2$, thus it must be 1, and $a$ and $b$ are coprime.
Conversely, if $p$ is a prime, and $a, b$ two coprime integers, $x = ap^2$ and $y = ap^2$ share three factors : 1 $p$, and $p^2$. □

**Corollary 1.** If an integer $x$ is squarefree (i.e. not divisible by any square of a prime), then there is no integer $y$ that shares exactly three divisors with $x$.

Denoting $Q(n)$ the number of squarefree integers between 1 and $n$, we get an expression for $P_3$.

**Theorem 3.**

$$P_3(N) = 2\left(\sum_{n=1}^{N} \sum_{p^2|n} \phi(\frac{n}{p^2})\right) - \pi(\sqrt{N})$$

where $\sum_{p^2|n}$ means summing over all primes whose square divide $n$. If $n$ is squarefree, this sum is 0.

*Proof.* We first check the formula is valid for $N = 1$, as $P_3(1) = 0$; since no square of prime divides 1.
Next, we again assume the formula for $P_3$ is valid for $N - 1$ with $N > 1$. To apply lemma 2 we must compute $s_3(N)$. By lemma 4, $(x, N)$ share three factors if and only if their GCD is a square of prime. For each prime $p$ such as $p^2 \mid N$, the numbers $x$ sharing factors $(1, p, p^2)$ with n are of the form $p^{\times}a$ where $a$ must be coprime with $\frac{N}{p^2}$. For a given square of prime $p^2$ that divides $N$, there are exactly $\phi(\frac{N}{p^2})$ numbers coprime with the quotient. Thus

$$s_3(N) = \sum_{p^2|n} \phi(\frac{n}{p^2})$$

Now, we double-count the pair $(N, N)$ when $N$ has exactly three factors. In this case $N = p^2$ is the square of a prime. Since $\pi(\sqrt{N})$ increments only when $N$ is a square of a prime, this gives us the formula. □

## Probability and asymptotical value

To answer the original question, we must give a value for the probability of a pair sharing $k$ divisors drawn from two independent uniform distriutions: $\frac{P_k(N)}{N^2}$
The totient summatory function $\Phi(N) = \sum_{n=1}^{N} \phi(n)$ has an asymptotic equivalent [Wei]

$$\Phi(N) \frac{1}{2} \frac{1}{\zeta(2)} N^2 + O(N \log N)$$

where $\zeta$ is the Riemann zeta function. This immediately yields

$$\begin{aligned} \lim_{N \to \infty} \frac{P_1(N)}{N^2} &= \frac{1}{\zeta(2)} \\ &= \frac{6}{\pi^2} \\ &\approx 0.6079 \end{aligned}$$

## References


[Wei] Eric W. Weisstein. *Totient Summatory Function*. URL: https://mathworld.wolfram.com/TotientSummatoryFunction.html.