Probability, primes, and mods

Jacob Richey and Carl de Marcken

University of Washington 2nd year Math Circle

4/9/2020

Probability

Let's recall some basic probability. Suppose N is a uniformly chosen random integer between 1 and 100: this means that every integer has equal probability of being chosen,

$$\mathbb{P}(N=1)=\mathbb{P}(N=2)=\mathbb{P}(N=3)=\cdots=\mathbb{P}(N=100)=\frac{1}{100}.$$

The expected or average value of N is

$$\begin{aligned}\mathbb{E}N &= 1\cdot\mathbb{P}(N=1)+2\cdot(N=2)+\cdots+100\cdot\mathbb{P}(N=100)\\ &= \frac{100\cdot 101}{2\cdot 100}\\ &= 50.5\end{aligned}$$

Random integers

Question: Can you pick a uniformly random integer from *all* the integers $1, 2, 3, \ldots$? Why or why not?

Random integers

Question: Can you pick a uniformly random integer from *all* the integers $1, 2, 3, \ldots$? Why or why not?

No! If all the probabilities were equal, they would all have to be 0!

Random integers

Question: Can you pick a uniformly random integer from *all* the integers $1, 2, 3, \ldots$? Why or why not?

No! If all the probabilities were equal, they would all have to be 0!

For today, when we pick a 'random' integer, it means: pick a uniformly random integer between 1 and 100, or 1 and 1000, or...

Divisibility

Question: What is the probability that a random integer N between 1 and 100 is divisible by 2? Divisible by 3? Divisible by n?

Divisibility

Question: What is the probability that a random integer N between 1 and 100 is divisible by 2? Divisible by 3? Divisible by n?

Answer: Same as asking $\mathbb{P}(N = 2, 4, 6 \ldots, 98, 100) \approx 1/2$, or $\mathbb{P}(N = 3, 6, \ldots, 99) \approx 1/3$.

Divisibility

Question: What is the probability that a random integer N between 1 and 100 is divisible by 2? Divisible by 3? Divisible by n?

Answer: Same as asking $\mathbb{P}(N = 2, 4, 6 \ldots, 98, 100) \approx 1/2$, or $\mathbb{P}(N = 3, 6, \ldots, 99) \approx 1/3$.

Question: What is the probability of a number being divisible by *both* 2 and 3? By both 3 and 6? By both 6 and 8?

Divisibility

Question: What is the probability that a random integer N between 1 and 100 is divisible by 2? Divisible by 3? Divisible by n?

Answer: Same as asking $\mathbb{P}(N = 2, 4, 6 \ldots, 98, 100) \approx 1/2$, or $\mathbb{P}(N = 3, 6, \ldots, 99) \approx 1/3$.

Question: What is the probability of a number being divisible by *both* 2 and 3? By both 3 and 6? By both 6 and 8?

Discuss!

Divisibility

Answer: If a and b are relatively prime, then $\mathbb{P}(a, b \text{ both divide } N) \approx \frac{1}{ab}$.

Divisibility

Answer: If a and b are relatively prime, then $\mathbb{P}(a, b \text{ both divide } N) \approx \frac{1}{ab}$.
In general,

$$\mathbb{P}(a, b \text{ both divide } N) \approx \frac{1}{\operatorname{lcm}(a, b)}.$$

Divisibility

Answer: If a and b are relatively prime, then $\mathbb{P}(a, b \text{ both divide } N) \approx \frac{1}{ab}$. In general,

$$\mathbb{P}(a, b \text{ both divide } N) \approx \frac{1}{\operatorname{lcm}(a, b)}.$$

Why? The numbers that are divisible by both a and b are the same as the numbers divisible by $\operatorname{lcm}(a, b)$!

Divisibility

Answer: If a and b are relatively prime, then $\mathbb{P}(a, b \text{ both divide } N) \approx \frac{1}{ab}$. In general,

$$\mathbb{P}(a, b \text{ both divide } N) \approx \frac{1}{\operatorname{lcm}(a, b)}.$$

Why? The numbers that are divisible by both a and b are the same as the numbers divisible by $\operatorname{lcm}(a, b)$!

Interpretation: Divisibility by distinct primes are **independent events**. For distinct primes p and q,

$$\mathbb{P}(p \text{ and } q \text{ divide } N) = \mathbb{P}(p|N) \cdot \mathbb{P}(q|N)$$

Relatively prime

Question: What is the probability that two independent random numbers N and M are relatively prime?

Relatively prime

Question: What is the probability that two independent random numbers N and M are relatively prime?

Answer: Being relatively prime means they share no common prime factors. So for any prime p, they can't *both* be divisible by p:

$$\mathbb{P}(p \text{ doesn't divide both } N, M) = 1 - \mathbb{P}(p \text{ divides both } N, M) \approx 1 - \frac{1}{p^2}.$$

Relatively prime

Question: What is the probability that two independent random numbers N and M are relatively prime?

Answer: Being relatively prime means they share no common prime factors. So for any prime p, they can't *both* be divisible by p:

$$\mathbb{P}(p \text{ doesn't divide both } N, M) = 1 - \mathbb{P}(p \text{ divides both } N, M) \approx 1 - \frac{1}{p^2}.$$

This has to happen for every prime! Using the independence for different primes,

$$\mathbb{P}(N, M \text{ relatively prime}) \approx \left(1 - \frac{1}{2^2}\right)\left(1 - \frac{1}{3^2}\right)\left(1 - \frac{1}{5^2}\right)\cdots.$$

Relatively prime

$$\mathbb{P}(N, M \text{ relatively prime}) \approx \left(1 - \frac{1}{2^2}\right)\left(1 - \frac{1}{3^2}\right)\left(1 - \frac{1}{5^2}\right)\cdots.$$

This product can be written in a nicer form. First let's re-write all the terms: for any p,

$$1 - \frac{1}{p^2} = \left(\frac{1}{1 - 1/p^2}\right)^{-1} = \left(1 + \frac{1}{p^2} + \frac{1}{p^4} + \frac{1}{p^6} + \cdots\right)^{-1}$$

Relatively prime

$$\mathbb{P}(N, M \text{ relatively prime}) \approx \left(1 - \frac{1}{2^2}\right)\left(1 - \frac{1}{3^2}\right)\left(1 - \frac{1}{5^2}\right)\cdots.$$

This product can be written in a nicer form. First let's re-write all the terms: for any p,

$$1 - \frac{1}{p^2} = \left(\frac{1}{1 - 1/p^2}\right)^{-1} = \left(1 + \frac{1}{p^2} + \frac{1}{p^4} + \frac{1}{p^6} + \cdots\right)^{-1}$$

So the product becomes

$$\left[\left(1 + \frac{1}{2^2} + \frac{1}{2^4} + \cdots\right)\left(1 + \frac{1}{3^2} + \frac{1}{3^4} + \cdots\right)\left(1 + \frac{1}{5^2} + \frac{1}{5^4} + \cdots\right)\cdots\right]^{-1}$$

Relatively prime

$$\left[\left(1+\frac{1}{2^2}+\frac{1}{2^4}+\cdots\right)\left(1+\frac{1}{3^2}+\frac{1}{3^4}+\cdots\right)\left(1+\frac{1}{5^2}+\frac{1}{5^4}+\cdots\right)\cdots\right]^{-1}$$

Relatively prime

$$\left[\left(1+\frac{1}{2^2}+\frac{1}{2^4}+\cdots\right)\left(1+\frac{1}{3^2}+\frac{1}{3^4}+\cdots\right)\left(1+\frac{1}{5^2}+\frac{1}{5^4}+\cdots\right)\cdots\right]^{-1}$$

Think about which terms appear in this sum when you multiply it out: any number n that can be written as a product of squares of prime numbers appears exactly once in the denominator. But those are just the square numbers! So

Relatively prime

$$\left[\left(1+\frac{1}{2^2}+\frac{1}{2^4}+\cdots\right)\left(1+\frac{1}{3^2}+\frac{1}{3^4}+\cdots\right)\left(1+\frac{1}{5^2}+\frac{1}{5^4}+\cdots\right)\cdots\right]^{-1}$$

Think about which terms appear in this sum when you multiply it out: any number n that can be written as a product of squares of prime numbers appears exactly once in the denominator. But those are just the square numbers! So

$$\mathbb{P}(N, M \text{ relatively prime}) = \left[1+\frac{1}{2^2}+\frac{1}{3^2}+\frac{1}{4^2}+\frac{1}{5^2}+\cdots\right]^{-1}$$

Relatively prime

$$\left[\left(1+\frac{1}{2^2}+\frac{1}{2^4}+\cdots\right)\left(1+\frac{1}{3^2}+\frac{1}{3^4}+\cdots\right)\left(1+\frac{1}{5^2}+\frac{1}{5^4}+\cdots\right)\cdots\right]^{-1}$$

Think about which terms appear in this sum when you multiply it out: any number n that can be written as a product of squares of prime numbers appears exactly once in the denominator. But those are just the square numbers! So

$$\mathbb{P}(N, M \text{ relatively prime}) = \left[1+\frac{1}{2^2}+\frac{1}{3^2}+\frac{1}{4^2}+\frac{1}{5^2}+\cdots\right]^{-1} = \frac{6}{\pi^2}.$$

Factors

So this says that if N and M are uniform between 1 and 10^6,

$$\mathbb{P}(\gcd(N, M) = 1) \approx 6/\pi^2 \approx .601$$

N and M share *no* common factors with probability around 3/5.

Factors

Let N be a uniform random number between 1 and 10^6.

Question: For any prime p, what's the biggest power of p that divides N?

Factors

Let N be a uniform random number between 1 and 10^6.

Question: For any prime p, what's the biggest power of p that divides N?

For example, suppose $p = 3$. What's the probability of being divisible by 3 but not by 9?

Factors

Let N be a uniform random number between 1 and 10^6.

Question: For any prime p, what's the biggest power of p that divides N?

For example, suppose $p = 3$. What's the probability of being divisible by 3 but not by 9?

$$\mathbb{P}(3|N, 9 \not| N) = \frac{1}{3}\left(1 - \frac{1}{3}\right) = \frac{2}{9}.$$

Factors

Let N be a uniform random number between 1 and 10^6.

Question: For any prime p, what's the biggest power of p that divides N?

For example, suppose $p = 3$. What's the probability of being divisible by 3 but not by 9?

$$\mathbb{P}(3|N, 9 \not| N) = \frac{1}{3}\left(1 - \frac{1}{3}\right) = \frac{2}{9}.$$

More in the exercises...

Primes

Question: What is the probability that N is prime?

It turns out that $\mathbb{P}(N \text{ is prime}) \approx 0(!)$ More precisely:

Theorem (Prime number theorem)

Let $\pi(x)$ denote the number of primes less than or equal to x. Then

$$\pi(x) \approx \frac{x}{\log x}$$

Thus, if N was chosen between 1 and 10^6, then

$$\mathbb{P}(N \text{ is prime}) \approx \frac{1}{\log 10^6} \approx \frac{1}{14}$$

Primes

The primes behave sort of 'uniformly random'. For example, the four possible last digits in base 10 of the primes are 1, 3, 7, and 9, and:

Theorem (Dirichlet, 1837)

The proportion of primes ending in 1, 3, 7 and 9 are all $\frac{1}{4}$.

This works in any base.

Primes

The primes behave sort of ‘uniformly random’. For example, the four possible last digits in base 10 of the primes are 1, 3, 7, and 9, and:

Theorem (Dirichlet, 1837)

The proportion of primes ending in 1, 3, 7 and 9 are all $\frac{1}{4}$.

This works in any base.

Theorem (Vinogradov, 1937)

All sufficiently large odd numbers can be written as a sum of three primes.

For many purposes, we can pretend that every number x was chosen to be prime with probability $\frac{1}{\log x}$.

Primes

God may not play dice with the universe, but something strange is going on with the prime numbers. - Paul Erdős

Coverings

Definition: A set of numbers and mods is a *covering* for the integers if every integer falls into one of those classes. The **score** of a covering is the sum of the reciprocals of the mods you use.

Coverings

Definition: A set of numbers and mods is a *covering* for the integers if every integer falls into one of those classes. The **score** of a covering is the sum of the reciprocals of the mods you use.

- Example 1: $0 \mod 2$ and $1 \mod 2$ is a covering, since every number is either even or odd. The score is $1/2 + 1/2 = 1$.
- Example 2: $0 \mod 2, 1 \mod 3, 3 \mod 6, 5 \mod 6$ is a covering, since all the congruence classes $\mod 6$ appear. The score is $1/2 + 1/3 + 1/6 + 1/6 = 7/6$.

Coverings

Definition: A set of numbers and mods is a *covering* for the integers if every integer falls into one of those classes. The **score** of a covering is the sum of the reciprocals of the mods you use.

- Example 1: $0 \mod 2$ and $1 \mod 2$ is a covering, since every number is either even or odd. The score is $1/2 + 1/2 = 1$.
- Example 2: $0 \mod 2, 1 \mod 3, 3 \mod 6, 5 \mod 6$ is a covering, since all the congruence classes $\mod 6$ appear. The score is $1/2 + 1/3 + 1/6 + 1/6 = 7/6$.

Your job: find coverings with **MINIMUM** possible score, and such that you don't use the LCM of your mods as one of the mods. (Neither of the above examples passes this test, since 2 is the LCM in example 1, and 6 is the LCM in example 2.)

(Bonus: can you construct coverings with arbitrarily big scores?)