1. ---

You toss a coin, independently from toss to toss, whose probability of heads is p and of tails $q = 1 - p$. Find the expected number of tosses required to get the first head.

Solution.

Let X_i be the outcome (H or T) at the i-th toss. Let N be the number of tosses required to get the first head. Then

$$N > k \iff X_1 = X_2 = \cdots = X_k = T.$$

Therefore

$$P(N > k) = P(X_1 = T)P(X_2 = T) \cdots P(X_k = T) = (1 - p)^k.$$

Notice that

$$\begin{aligned}\sum_{k=0}^{\infty} P(N > k) &= \sum_{k=0}^{\infty} E\mathbf{1}(N > k) = E\sum_{k=0}^{\infty} \mathbf{1}(N > k) \\ &= E\sum_{k=0}^{N-1} 1 = E(\underbrace{1 + 1 + \cdots + 1}_{N \text{ times}}) = EN.\end{aligned}$$

Therefore,

$$\begin{aligned}EN = \sum_{k=0}^{\infty} P(N > k) &= \sum_{k=0}^{\infty} q^k \\ &= 1 + q + q^2 + q^3 + \cdots \\ &= 1 + q(1 + q + q^2 + \cdots) \\ &= 1 + qEN.\end{aligned}$$

Thus, EN satisfies $EN = 1 + qEN$, whence $(1 - q)EN = 1$, i.e. $pEN = 1$, and so $EN = 1/p$.

2. ---

Consider a box containing n balls, out of which m are red and $n - m$ blue. Start picking the balls one by one until you see a red one. What is the average number of picks required?

Assume, in particular, that n is large and that $m/n \to p$ as $n \to \infty$. Compare your result with the one of the previous problem.

Solution.

Let X_i be the colour of the i-th ball picked. (Use the symbol 1 for red and the symbol 0 for blue.) Let N be the number of picks required to get the first red ball. It is well-known that $1+1=2$, $1+1+1=3$, $1+1+1+1=4$, and so on. In general,

$$N = \underbrace{1+1+\cdots+1}_{N \text{ times}}.$$

Therefore,

$$N = 1 + \sum_{k=1}^{N-1} 1 = 1 + \sum_{k=1}^{\infty} \mathbf{1}(N > k).$$

(Recall that $x < y$ means that x is smaller but not equal to y, whereas $x \le y$ means that x is smallr or, perhaps, equal to y.) Hence

$$\begin{aligned} EN = 1 + E\sum_{k=1}^{\infty} \mathbf{1}(N > k) &= 1 + \sum_{k=1}^{\infty} P(N > k) \\ &= 1 + \sum_{k=1}^{\infty} P(X_1 = \cdots = X_k = 0). \\ &= 1 + \sum_{k=1}^{\infty} \tfrac{n-m}{n} \, \tfrac{n-m-1}{n-1} \, \cdots \, \tfrac{n-m-k+1}{n-k+1} \end{aligned}$$

The sum contains only finitely many terms because, for k large enough, the term inside the summation is zero. Be it as it may, it is not obvious what the sum is. So let's forget the last line of the display and think differently.

Consider the box and add an extra red ball. Now the box has $n+1$ balls, out of which $m+1$ are red. Pick a ball. Call its colour Y_0. Continue picking the balls until exhuastion, and let $Y_1, \ldots, Y_n$ be the colours of the balls, in the order they are picked. If it so happens that $Y_0 = 1$ (=red) then $(Y_1, \ldots, Y_n)$ *obviously* behaves as if it was coming from the original urn. So, in particular,

$$P(Y_1 = \cdots = Y_k = 0 | Y_0 = 1) = P(X_1 = \cdots = X_k = 0).$$

We can write this as

$$P(Y_0 = 1, Y_1 = \cdots = Y_k = 0 | Y_0 = 1) = P(X_1 = \cdots = X_k = 0).$$

Therefore,

$$EN = 1 + \sum_{k=1}^{\infty} P(Y_0 = 1, Y_1 = \cdots = Y_k = 0 | Y_0 = 1).$$

Since

$$P(Y_0 = 1 | Y_0 = 1) = 1,$$

we can also write the above as

$$\begin{aligned} EN &= \sum_{k=0}^{\infty} P(Y_0 = 1, Y_1 = \cdots = Y_k = 0 | Y_0 = 1) \\ &= \sum_{k=0}^{\infty} \frac{P(Y_0 = 1, Y_1 = \cdots = Y_k = 0)}{P(Y_0 = 1)}. \end{aligned}$$

But, since Y_0 is the colour of the first ball picked in an urn with $m+1$ red balls, we have

$$P(Y_0 = 1) = \frac{m+1}{n+1}.$$

On the other hand (explain this!),

$$P(Y_0 = 1, Y_1 = \cdots = Y_k = 0) = P(Y_1 = \cdots = Y_{k-1} = 0, Y_k = 1).$$

Hence

$$EN = \frac{n+1}{m+1} \sum_{k=0}^{\infty} P(Y_1 = \cdots = Y_{k-1} = 0, Y_k = 1).$$

But the latter sum is the probability of the event that, at some point of time, a red ball will be picked; clearly, this is 1. Hence

$$EN = \frac{n+1}{m+1}.$$

If $m/n \to p$ then $EN \to 1/p$, as in the coin-tossing case.

3.

Explain what division of an integer n by a positive integer m means.

Divide the number 56793 by 382.

Solution.

Let n, m be positive integers. Consider the multiples

$$0 \cdot m,\ 1 \cdot m,\ 2 \cdot m,\ 3 \cdot m,\ \ldots$$

of m. There is a large enough multiple which exceeds n. So there is a last multiple, call it $q \cdot m$ such that $q \cdot m \le n$. In other words,

$$r := n - q \cdot m$$

is nonnegative. Also, it is strictly smaller than m. (If not, then we can replace q by $q+1$ and this violates the definition of $q \cdot m$ as the last multiple of m not exceeding n.) By **division** of n by m we mean precisely this: there exists a unique integer q (the quotient) such that

$$n = qm + r$$

where r (the remainder) satisfies

$$0 \le r < m.$$

To divide $n = 56793$ by $m = 382$, we follow a process (=algorithm) called long division.

The first step is as follows. Look at the multiples

$$100m,\ 200m, \dots$$

of m and try to find the one that is as close as possible to n. This is not hard, becase we can immediately observe that $100m = 38200 < n$, but $200m > n$. So q is a number whose first digit is 1.

In the second step, we replace n by $n_2 := n - 100m = 18593$. Since n_2 exceeds m we continue. Look at the multiples

$$10m,\ 20m, \dots$$

of m and try to find the one that is as close as possible to n_2. We see that $40m = 15280 < n_2$, but $50m > n_2$. So q is a number whose first digit is 1 and second digit 4.

In the third step, we replace n_2 by $n_3 := n_2 - 40m = 3313$. Since n_3 exceeds m we continue. Look at the multiples

$$m,\ 2m, \dots$$

of m and try to find the one that is as close as possible to n_3. We see that $8m = 3438 < n_3$, but $9m > n_3$. So the third digit of q is 8.

Next, see that $n_4 := n_3 - 8m = 257$ is strictly smaller than m, so stop and declare that $r := 257$, whereas $q = 148$.

I'm pretty sure you can arrange this process neatly in a table. I will skip this cosmetic (albeit important) element.

4. ____

Find the greatest common divisor between 56793 and 382.

Solution.

Observation: If d is the greatest common divisor between n and m then d is also the greatest common divisor between n and $n - m$.

Therefore: If d is the greatest common divisor between n and m then d is also the greatest common divisor between n and $n-2m$ and between n and $n-3m$, etc.

Therefore: If d is the greatest common divisor between n and m then d is also the greatest common divisor between n and $n-qm$ for any q, and, in particular, the quotient of the division of n by m.

Therefore: If d is the greatest common divisor between n and m then d is also the greatest common divisor between n and r where r is the remainder of the division of n by m.

So, in the particular case, where $n = 56793$ and $m = 382$, we found that $r = 257$, so $\gcd(56793, 382) = \gcd(382, 257)$.

Next, divide 382 by 257. We have

$$382 = 1 \cdot 257 + 125.$$

Hence $\gcd(382, 257) = \gcd(257, 125)$.

Next, divide 257 by 125:

$$257 = 2 \cdot 125 + 7.$$

Hence $\gcd(257, 125) = \gcd(125, 7)$.

Next, divide 125 by 7:

$$125 = 17 \cdot 7 + 6.$$

Hence $\gcd(125, 7) = \gcd(7, 6)$, and this is obviously equal to 1.

5. ____

Show that the greatest common divisor between two positive integers m and n is an integer d such that (i) d divides both m and n and (ii) if k divides m and n then k divides d.

Solution.

Consider all numbers of the form

$$an + bm,$$

where a, b are integers (of any sign), such that $an + bm \geq 1$. Let δ be the smallest of these numbers. We shall show that δ divides both m and n.

Indeed,

$$\delta = \alpha m + \beta n,$$

for some integers α, β. Divide m by δ to obtain

$$m = q\delta + r,$$

where $0 \leq r < \delta$. Hence

$$m = q(\alpha m + \beta n) + r,$$

and so

$$r = (1 - q\alpha)m + (-\beta n).$$

So r is of the form $am + bn$. If r is not zero, then we have a number of the form $am + bn$ which is strictly smaller than δ. This is impossible because δ was defined to be the smallest such number. So $r = 0$. This means that $m = q\delta$, i.e. δ divides m. Similarly, δ divides n.

We have shown that δ is a common divisor.

Now let k be any other common divisor between m and n. Since $\delta = \alpha m + \beta n$ we see that k divides δ.

This means that δ is the largest of all common divisors between m and n, i.e. the greatest common divisor. At the same time, we have shown that if k is any common divisor then k divides δ.

6.

Find the product AB of the matrices $A = \begin{pmatrix} 1 & 0 & 2 \\ 3 & 5 & 1 \end{pmatrix}$ and $B = \begin{pmatrix} 5 & 6 & 1 \\ 0 & 2 & 0 \\ 1 & 0 & -3 \end{pmatrix}$.

Recall that, in general, $(AB)_{ij} = \sum_k A_{ik} B_{kj}$.

Can you compute BA also?

Solution.

I shall compute $(AB)_{ij}$ for all i and j. For example,

$$(AB)_{21} = \sum_k A_{2k} B_{k1}.$$

The index k ranges between 1 and 3. (Notice that A has 3 columns and B has 3 rows; if the number of columns of A were not equal to the number of rows of B then we'd have a problem!) So

$$(AB)_{21} = \sum_{k=1}^{3} A_{2k} B_{k1} = A_{21}B_{11} + A_{22}B_{21} + A_{23}B_{31} = 3\cdot 5 + 5\cdot 0 + 1\cdot 1 = 15 + 0 + 1 = 16.$$

You can work out the remaining entries. I give you the answer:

$$AB = \begin{pmatrix} 7 & 6 & -5 \\ 16 & 28 & 0 \end{pmatrix}.$$

The product BA is not defined because the number of columns of B is not equal to the number of rows of A.