

Example 221. (terrible jokes, parental guidance advised)

There are 10 types of people... those who understand binary, and those who don't.

Of course, you knew that. How about:

There are 11 types of people... those who understand Roman numerals, and those who don't.

It's not getting any better:

There are 16 types of people... those who understand hexadecimal, F the rest...

Example 222. (yet another joke) Why do mathematicians confuse Halloween and Christmas?

Because 31 Oct = 25 Dec.

Get it? $(31)_8 = 1 + 3 \cdot 8 = 25$ equals $(25)_{10} = 25$.

Fun borrowed from: https://en.wikipedia.org/wiki/Mathematical_joke

The Riemann hypothesis: Another Millennium Prize Problem

The Riemann hypothesis is another one of the seven Millennium Prize Problems that is of importance to the underpinnings of cryptography. It is concerned with the distribution of primes.

Recall that we discussed the prime number theorem, which states that, up to x , there are about $x/\ln(x)$ many primes. The Riemann hypothesis gives very precise error estimates for an improved prime number theorem (using a function more complicated than the logarithm).

Example 223. (Riemann hypothesis) Consider the Riemann zeta function $\zeta(s) = \sum_{n \geq 1} \frac{1}{n^s}$. This series converges (for real s) if and only if $s > 1$.

The divergent series $\zeta(1)$ is the harmonic series, and $\zeta(p)$ is often called a p -series in Calculus II.

Comment. Euler achieved worldwide fame in 1734 by discovering and proving that $\zeta(2) = \frac{\pi^2}{6}$ (and similar formulas for $\zeta(4), \zeta(6), \dots$).

For complex values of $s \neq 1$, there is a unique way to “analytically continue” this function. It is then “easy” to see that $\zeta(-2) = 0, \zeta(-4) = 0, \dots$. The **Riemann hypothesis** claims that all other zeroes of $\zeta(s)$ lie on the line $s = \frac{1}{2} + a\sqrt{-1}$ ($a \in \mathbb{R}$). A proof of this conjecture (checked for the first 10,000,000,000 zeroes) is worth \$1,000,000.

<http://www.claymath.org/millennium-problems/riemann-hypothesis>

The connection to primes. Here's a vague indication that $\zeta(s)$ is intimately connected to prime numbers:

$$\begin{aligned} \zeta(s) &= \left(1 + \frac{1}{2^s} + \frac{1}{2^{2s}} + \dots\right) \left(1 + \frac{1}{3^s} + \frac{1}{3^{2s}} + \dots\right) \left(1 + \frac{1}{5^s} + \frac{1}{5^{2s}} + \dots\right) \dots \\ &= \frac{1}{1 - 2^{-s}} \frac{1}{1 - 3^{-s}} \frac{1}{1 - 5^{-s}} \dots \\ &= \prod_{p \text{ prime}} \frac{1}{1 - p^{-s}} \end{aligned}$$

This infinite product is called the Euler product for the zeta function. If the Riemann hypothesis was true, then we would be better able to estimate the number $\pi(x)$ of primes $p \leq x$.

More generally, certain statements about the zeta function can be translated to statements about primes. For instance, the (non-obvious!) fact that $\zeta(s)$ has no zeros for $\text{Re } s = 1$ implies the prime number theorem.

<http://www-users.math.umn.edu/~garrett/m/v/pnt.pdf>

Example 224. (combinatorial warm-up) A typical Amazon gift card code is of the form

6DAG-KJ2PZ5-3ATM.

Suppose that, at any time, say, one million gift cards are active. What are the odds that a random gift card code is a valid one? Is this a security issue?

Solution. It seems that each of the $4 + 6 + 4 = 14$ letters is either a capital letter or a digit, meaning there are $26 + 10 = 36$ possibilities for each (though, in actuality, for instance, a letter like O might not be used because of possible confusion with 0). In total, there are $36^{14} \approx 6.14 \cdot 10^{21}$ many possible such codes.

If 10^6 codes are valid, then the odds are $10^6 / (6.14 \cdot 10^{21}) \approx 1.63 \cdot 10^{-16}$.

If you were able to go through one million random codes per second, then it would still take about 195 years on average until you ran into a valid code.

Variation. A typical Netflix gift card is of the form LEQGXX215988. How does that change the odds? Here, it seems that there are 5 letters followed by 6 numbers for a total of $26^5 \cdot 10^6 \approx 1.19 \cdot 10^{13}$.

If there are 100,000 unredeemed gift cards and if an attacker can check 1000 codes per second, then it would take an average of about 33 hours for the attacker to run into an unredeemed code.

Hackers using bots to check for unredeemed gift cards is an actual problem, and the above calculation (adjust any assumptions if they don't sound reasonable) does indicate that the length of the gift codes could be a factor in making things easier for attackers.

Variation. A typical Spotify gift card is of the form 580 186 9104. How does that change the odds?

Example 225. Numberphile posted a popular video explaining Russian multiplication:

https://www.youtube.com/watch?v=HJ_PP5rqLg0

The method goes back to at least the Egyptians; it is also called Ethiopian multiplication.

https://en.wikipedia.org/wiki/Ancient_Egyptian_multiplication

Here is how the multiplications $12 \cdot 11 = 132$, $9 \times 31 = 279$, $18 \times 17 = 306$ and $17 \times 18 = 306$ are done in that system using halving and doubling; in the final step we add from those rows starting with an odd number.

12	11
6	22
3	44
1	88
	132

9	31
4	62
2	124
1	248
	279

18	17
9	34
4	68
2	136
1	272
	306

17	18
8	36
4	72
2	144
1	288
	306

Do you see the mechanics from these examples? Can you explain why that always works?

Solution. This is essentially long multiplication using binary! Can you spell this out?

The Egyptians apparently wrote things in a way that might be a tiny bit more revealing:

12	11
1	11
2	22
4	44
8	88
	132

9	31
1	31
2	62
4	124
8	248
	279

18	17
1	17
2	34
4	68
8	136
16	272
	306

17	18
1	18
2	36
4	72
8	144
16	288
	306

Can you see how this is analogous to our binary exponentiation method?