Sketch of Lecture 37

Mon, 4/22/2024

P versus NP: A Millennium Prize Problem

The Clay Mathematics Institute has offered 10^6 dollars each for the first correct solution to seven **Millennium Prize Problems**. Six of the seven problems remain open.

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

Comment. Grigori Perelman solved the Poincaré conjecture in 2003 (but refused the prize money in 2010).
https://en.wikipedia.org/wiki/Poincaré_conjecture

Example 227. (P vs NP) P versus NP is one of the Millennium Prize Problems that is of particular importance to cryptography.

"If the solution to a problem is easy to check for correctness, is the problem easy to solve?"

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

Roughly speaking, consider decision problems which have an answer of yes or no. P is the class of such problems, which can be solved efficiently. NP are those problems, for which we can quickly verify that the answer is yes if presented with suitable evidence.

For instance.

- It is unknown whether factoring (in the sense of: does N have a factor $\leqslant M$?) belongs to P or not.
  The problem is definitely in NP because, if presented with a factor $\leqslant M$, we can easily check that.
- Deciding primality is in P (maybe not so shocking since there are very efficient nondeterministic algorithms for checking primality; not so for factoring).
- In the (decisional) travelling salesman problem, given a list of cities, their distances and d, the task is to decide whether a route of length at most d exists, which visits each city exactly once.
  The decisional TSP is clearly in NP (take as evidence the route of length $\leqslant d$). In fact, the problem is known to be NP-complete, meaning that it is in NP and as "hard" as possible (in the sense that if it actually is in P, then $\mathrm{P}=\mathrm{NP}$; that is, we can solve any other problem in NP efficiently).
- Other NP-complete problems include:
  - Sudoku: Does a partially filled grid have a legal solution?
  - Subset sum problem: Given a finite set of integers, is there a non-empty subset that sums to 0?

Comment. "Efficiently" means that the problem can be solved in time polynomial in the input size.
Take for instance computing $2^n \pmod{n}$, where n is the input (it has size $\log_2(n)$). This can be done in polynomial time if we use binary exponentiation (whereas the naive approach takes time exponential in $\log_2(n)$).

Comment. This is one of the few prominent mathematical problems which doesn't have a definite consensus. For instance, in a 2012 poll of 151 researchers, about 85% believed $\mathrm{P}\neq\mathrm{NP}$ while about 10% believed $\mathrm{P}=\mathrm{NP}$.

Comment. NP are problems that can be verified efficiently if the answer is "yes". Similarly, co-NP are problems that can be verified efficiently if the answer is "no". It is an open problem whether $\mathrm{NP}\neq\text{co-NP}$ (as expected).

- Factoring is in both NP and co-NP (it is in co-NP because primality testing is in P).
- For all NP-complete problems it is unknown whether they are in co-NP. (If one of them is, then we would, unexpectedly, have $\mathrm{NP}=\text{co-NP}$.)

Example 228. (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 II types of people... those who understand Roman numerals, and those who don't.

It's not getting any better:

There are 10 types of people... those who understand hexadecimal, F the rest...

Example 229. (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 230. (Riemann hypothesis) Consider the **Riemann zeta function** $\zeta(s) = \sum_{n \geqslant 1} \frac{1}{n^s}$. 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 $\zeta(4), \zeta(6), \ldots$).

For complex values of $s \neq 1$, there is a unique way to "analytically continue" this function. It is then "easy" to see that $\zeta(-2) = 0$, $\zeta(-4) = 0$, ... 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:

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

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 $p \leqslant x$.

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 $\mathrm{Re}\, s = 1$ implies the prime number theorem.

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

Example 231. (combinatorial warm-up) A typical Amazon gift card code is of the form

$$\text{6DAG-KJ2PZ5-3ATM}.$$

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 LEQGX215988. 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 (you can 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 232. 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 muliplication 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?