A BRIEF INTRODUCTION TO PRIMES AND FINITE FIELDS

[UNDERGRADUATE STUDENTS SEMINAR]

SAINT LOUIS UNIVERSITY – MADRID CAMPUS
FALL, 2022

Alexandru Iosif
Saint Louis University
Madrid Campus

An uneven game

- Form pairs of two and each one secretly pick a prime number from the following list:
  - **17, 19, 23, 29, 31, 37, 41, 43, 47**
- Person 1 asks Person 2 to
  - Multiply Person's 1 primes (call this product P_1).
  - Multiply Person's 2 primes and give the result to Person 1 (call this product P_2).
- Person 2 ask Person 1 what were the original primes that were multiplied to get P_2.

Whose task is more difficult?

Who is performing more operations?

An uneven game (example)

- Suppose that
  - Person 1 choses the primes 31 and 41.
  - Person 2 choses the primes 43 and 29.
- Person 1 asks Person 2 to
  - Multiply Person's 1 primes (call this product P_1): $P_1 = 1271$.
  - Multiply Person's 2 primes and give the result to Person 1 (call this product P_2): $P_2 = 1247$.
- Person 2 ask Person 1 what were the original primes that were multiplied to get $P_2 = 1247$. That is, Person 2 asks Person 1 to factor $P_2 = 1247$.

Who is performing more operations?

- Person 2 has to do two multiplications.
- Person 1 has to check one by one which are the primes that divide $P_2 = 1247$.
  - In principle, using the most naïve algorithm, 9 operations.
- Also, note how similar P_1 and P_2 are.

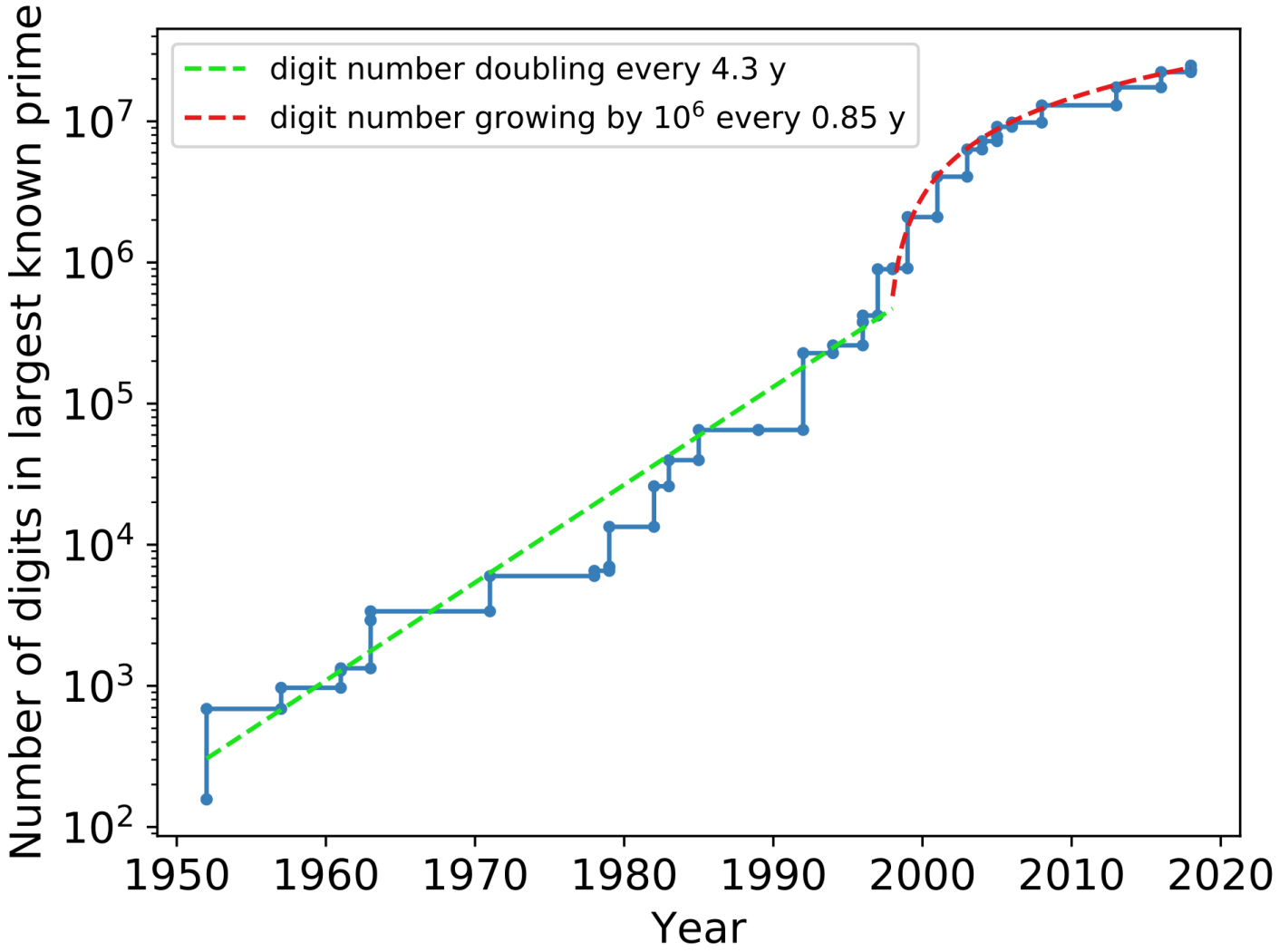
RSA Algorithm

[Source: Wikipedia]

Ron Rivest Adi Shamir Leonard Adleman

It uses the fact that factorization is much harder than multiplication.
I plan to talk about it next day.

Very large primes



[Source: Wikipedia]

- Integers are sublime:
  - We can add them.
    - For each number, n, there is another number, $-n$, such that, when we add them, we get 0:

$$n + (-n) = 0$$

    - 0 is called the additive identity.
    - $-n$ is called the additive inverse of n.
  - We can multiply them:

$$ab = ba$$
$$a(b + c) = ab + ac$$

But there are no multiplicative inverses:

$$\mathbf{2} \cdot ??? = \mathbf{1}$$

The Trouble with (primes) Nature

- Rational numbers are nice from this point of view:

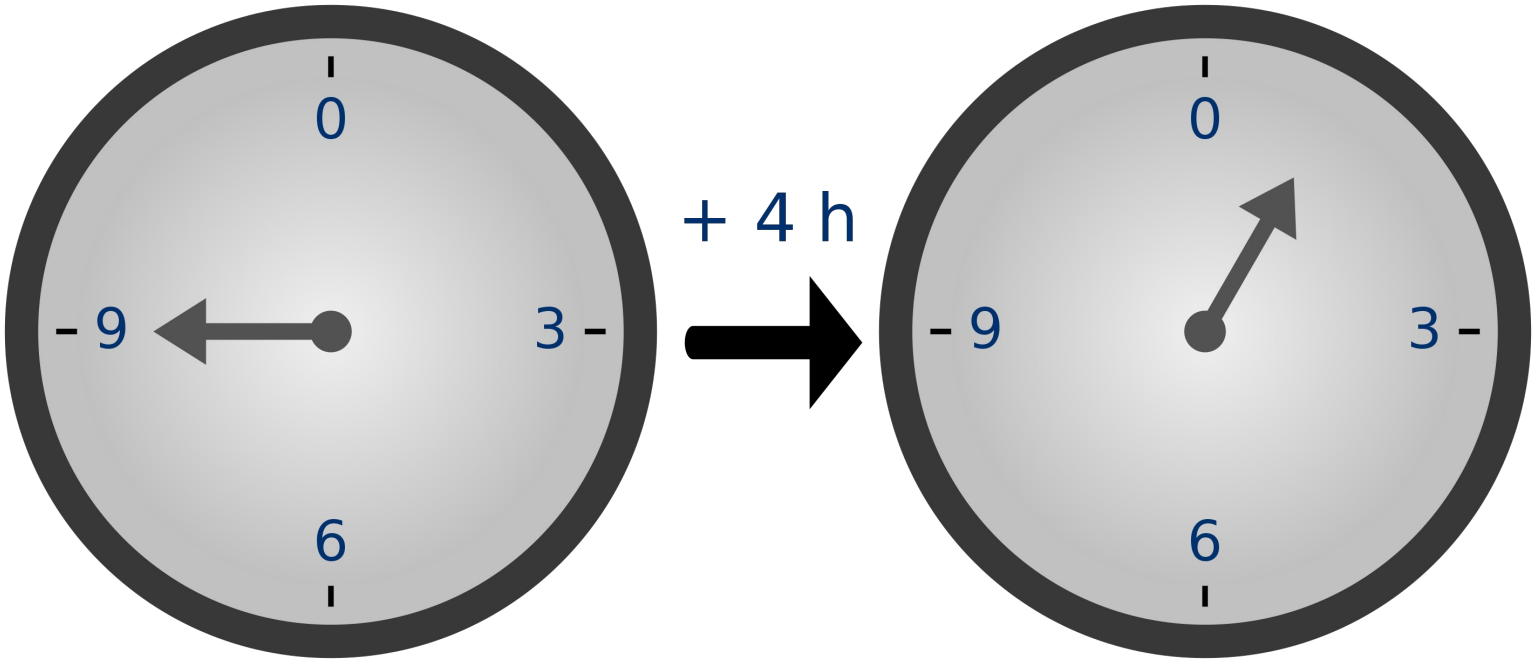
$$2\frac{1}{2} = 1$$

- Real numbers are nice from this point of view:

$$\mathrm{e}\frac{1}{e} = 1$$

- They have additive inverses.
- Such sets of numbers are called fields.
- But the integers do not form fields.
  - Unless we make them shrink.

The Trouble with (primes) Nature



[Source: Wikipedia]

MODULAR ARITHMETIC

Modular arithmetic

A few calculations in $\mathbb{Z}_{12}$:

$$13 \equiv 1 \bmod 12$$
$$13 = 1 \cdot 12 + 1$$
$$\frac{13}{12} = 1 \ (\text{rem} = 1)$$

$$50 \equiv 2 \bmod 12$$
$$50 = 4 \cdot 12 + 2$$
$$\frac{50}{12} = 4 \ (\text{rem} = 2)$$

Only reminders matter:

$$\mathbb{Z}_{12} = \{0, 1, 2, 3, 4, 5, 6, 7, 8, 9, 10, 11\}.$$

That is, $\mathbb{Z}_{12}$ contains the possible reminders of division by 12.

And we can build, in a similar way, $\mathbb{Z}_2$, $\mathbb{Z}_3$, $\mathbb{Z}_4$, et caetera.

In a letter to Bernard Frenicle de Bessy (∼1605–1675), dated October 18th, 1640, Pierre de Fermat (1601–1665) stated that

$$x^{p-1} \equiv 1 \bmod p$$

whenever p is a prime that does not divide x (Dickson 1971, p. 59). This letter I believe is the birth certificate of Galois field theory. The first proof of this result was published by Leonhard Euler (1707–1783) in 1741. He published two more proofs, the second one in 1750 and the third one in 1761 (see the bibliography for details). Two of the three proofs are inductive and use the binomial formula

$$(x+1)^p = \sum_{i:=0}^{p} \binom{p}{i} x^i \equiv x^p + 1 \bmod p.$$

[Source: https://www.asc.tuwien.ac.at/~herfort/W_Hojka/Lueneburg_history_of_galois_theory.pdf]

Tout nombre premier (1) mesure infailliblement une des puissances — 1 de quelque progression que ce soit, et l'exposant de la dite puissance est sous-multiple du nombre premier donné — 1; et, après qu'on a trouvé la première puissance qui satisfait à la question, toutes celles dont les exposants sont multiples de l'exposant de la première satisfont tout de même à la question.

Exemple : soit la progression donnée

1	2	3	4	5	6	
3	9	27	81	243	729	etc.

avec ses exposants en dessus.

Prenez, par exemple, le nombre premier 13. Il mesure la troisième puissance — 1, de laquelle 3, exposant, est sous-multiple de 12, qui est moindre de l'unité que le nombre 13, et parce que l'exposant de 729, qui est 6, est multiple du premier exposant, qui est 3, il s'ensuit que 13 mesure aussi la dite puissance 729 — 1.

(1) C'est de cet énoncé qu'a été tirée la proposition connue sous le nom de *Théorème de Fermat*, à savoir que si p est premier et ne divise pas a, il divise $a^{p-1} - 1$.

Fermat:
on the margins of maths

Modular arithmetic

But are there multiplicative inverses? Lets look at an example in $\mathbb{Z}_6$

$$5 \cdot 5 = 25 = 4 \cdot 6 + 1 \equiv 1 \bmod 6$$

It looks like, in $\mathbb{Z}_6$, multiplying 5 by 5 gives 1. That is, 5 is its own multiplicative inverse.

Let's now check all multiplications in $\mathbb{Z}_6$.

Multiplication table of $\mathbb{Z}_6$

·	**0**	**1**	**2**	**3**	**4**	**5**
0	0	0	0	0	0	0
1	0	1	2	3	4	5
2	0	2	4	6	8	10
3	0	3	6	9	12	15
4	0	4	8	12	16	20
5	0	5	10	15	20	25

·	**0**	**1**	**2**	**3**	**4**	**5**
0	0	0	0	0	0	0
1	0	**1**	2	3	4	5
2	0	2	4	**0**	2	4
3	0	3	**0**	3	**0**	3
4	0	4	2	**0**	4	2
5	0	5	4	3	2	**1**

This is not a field. Not all elements have multiplicative inverses.

Multiplication table of $\mathbb{Z}_5$

·	**0**	**1**	**2**	**3**	**4**
0	0	0	0	0	0
1	0	1	2	3	4
2	0	2	4	6	8
3	0	3	6	9	12
4	0	4	8	12	16

·	**0**	**1**	**2**	**3**	**4**
0	0	0	0	0	0
1	0	**1**	2	3	4
2	0	2	4	**1**	3
3	0	3	**1**	4	2
4	0	4	3	2	**1**

This is a field. Every element has a multiplicative inverse.

Finite Fields (or Galois Fields)

- They are ensembles of the form

$$\mathbb{Z}_{p^n}$$

where p is a prime number and n is a positive integers.

- Coding theory and cryptography operations are performed in such fields.

Polynomials on Finite Fields

- Analyze the following polynomial over $\mathbb{Z}_2$

$$p(x) = x^2 - 2x + 1$$

Galois:
a life at the limit

References:

- https://www.asc.tuwien.ac.at/~herfort/W_Hojka/Lueneburg_history_of_galois_theory.pdf
- Oevres de Fermat
- https://www.youtube.com/watch?v=Ij01HGgxnkA
- https://www.youtube.com/watch?v=Mc0bvea6G3I

¡Thank you!