Week 6: Rudiments of Number Theory (Textbook Chapter 7)

Prof. Michael Gastpar

Slides by Prof. M. Gastpar and Prof. em. B. Rimoldi

EPFL

Spring Semester 2025

LAST WEEK

- BASIC NOTIONS:

  ENCRYPT / DECRYPT

  PLAINTEXT

  CIPHERTEXT / CRYPTOGRAM

COMPUTATIONAL SECURITY

- DIFFIE-HELLMAN KEY EXCHANGE.

EX: SELECT $p = 23, \quad g = 3$

ALICE'S SECRET: $a = 4 \qquad A = g^a = 3^4 = 12$

BOB'S SECRET: $b = 3 \qquad B = g^b = 3^3 = 4$

SHARED SECRET?

$$A^b = B^a =$$

COMPUTATIONAL SECURITY

- DIFFIE-HELLMAN KEY EXCHANGE.

EX: SELECT $p = 23$, $g = 3$

ALICE'S SECRET: $a = 4 \rightarrow A = 12$

BOB'S SECRET: $b = 3 \rightarrow B = 4$

SHARED SECRET?

$$A^b = B^a = 3$$

EL GAMAL CRYPTOSYSTEM

YOU WANT TO RECEIVE A MESSAGE FROM ME.

EL GAMAL CRYPTOSYSTEM

YOU WANT TO RECEIVE A MESSAGE FROM ME.

1. YOU PICK $p = 31, g = 3.$
2. YOU PICK SECRET $x = 5 \rightarrow B = 3^5$
3. YOU SEND ME:

EL GAMAL CRYPTOSYSTEM

YOU WANT TO RECEIVE A MESSAGE FROM ME.

① YOU PICK $p = 31, g = 3.$

② YOU PICK SECRET $x = 5 \rightarrow g^x = 26.$

③ YOU SEND ME: $p=31, g=3, g^x=26.$

t, PICK SECRET $y \rightarrow g^y$

↳ $(g^x)^y \cdot t$

EL GAMAL CRYPTOSYSTEM

YOU WANT TO RECEIVE A MESSAGE FROM ME.

① YOU PICK $p = 31, \; g = 3.$

② YOU PICK SECRET $x = 5 \rightarrow g^x = 26.$

③ YOU SEND ME: $p=31, \; g=3, \; g^x=26.$

NOW, MY TURN.

① MY MESSAGE FOR YOU IS $t = 23$

② I PICK SECRET $y = 4.$

③ I SEND YOU

EL GAMAL CRYPTOSYSTEM

YOU WANT TO RECEIVE A MESSAGE FROM ME.

① YOU PICK $p = 31, g = 3.$

② YOU PICK SECRET $x = 5 \rightarrow g^x = 26.$

③ YOU SEND ME: $p=31, g=3, g^x=26.$

NOW, MY TURN.

① MY MESSAGE FOR YOU IS $t = 23$

② I PICK SECRET $y = 4. \rightarrow g^y = 19$

③ I SEND YOU $g^y = 19, B^y t = 26^4 \cdot 23 = 22$

YOU CALCULATE

$$(g^y)^x = 19^5 = 5$$

OBS: $25 \cdot 5 \bmod 31 = 1.$

$\Rightarrow$ 25 IS THE MULTIPLICATIVE INVERSE OF 5.

FINALLY, YOU CALCULATE:

$$25 \cdot B^y t = 25 \cdot 22 = 23$$

↓

THIS IS THE MESSAGE!

Outline

Introduction and Organization

Entropy and Data Compression

Cryptography

- One-Time Pad, Perfect Secrecy, Public-Key (Diffie-Hellman)
- Rudiments of Number Theory
- Modular Arithmetic
- Commutative Groups
- Public-Key Cryptography
- Summary of Chapter 2

Channel Coding

Why Number Theory

Much of public-key cryptography is based on number theory.

More generally, in the digital world, the information is represented by the elements of a finite set, and we should be able to do math with them. Which means that the finite set should be a finite field. Our bigger goal of the next few lectures is to develop the tools to understand when and how we can turn a finite set into a finite field.

Operations with integers

Within $\mathbb{Z}$ (the set of integers) we can

- add, subtract, multiply
- but not divide: $\frac{7}{2}$ is not an integer
- what comes closest to the (regular) division is the Euclidean division

OPERATIONS WITH INTEGERS

Within $\mathbb{Z}$ (the set of integers) we can

- add, subtract, multiply
- but not divide: $\frac{7}{2}$ is not an integer
- what comes closest to the (regular) division is the Euclidean division

EUCLIDEAN DIVISION

7 divided by 2 = 3.5

because $2 \times 3.5 = 7$

7 modulo 2 = 1

because $2 \times 3 + 1 = 7$

$2 \times 4 - 1 = 7$

EUCLIDEAN DIVISION

25 divided by 4 = 6.25

$4 \times 6.25 = 25$

25 modulo 4 = 1

$4 \times 6 + 1$

EUCLIDEAN DIVISION

For **all** integers

a : the dividend

m : the divisor ($m \neq 0$)

there exist **unique** integers

q : the quotient

$r \in \{0, 1, 2, \ldots, m-1\}$: the remainder

such that

$$a = m \cdot q + r$$

EUCLIDEAN DIVISION

For all integers

$$a = 52$$

$$m = 7$$

there exist unique integers

$$q = 7$$

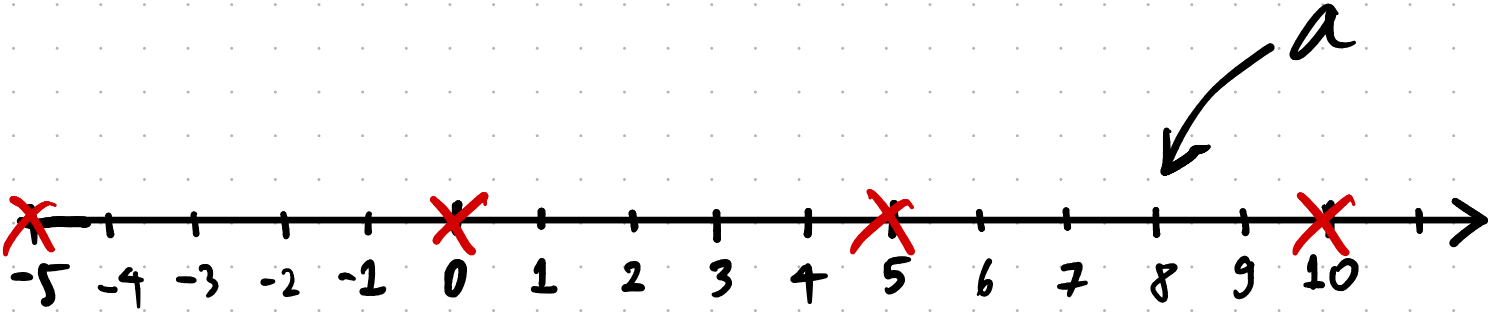
$$r \in \{0, 1, 2, 3, 4, 5, 6\} \qquad r = 3$$

such that

$$52 = 7 \cdot 7 + 3$$

PROOF: BY PICTURE

Let $m = 5$ for example.



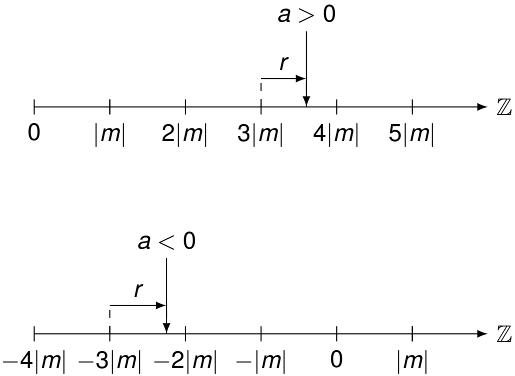
EUCLIDEAN DIVISION

The Division Algorithm: Given integers a (the dividend) and m (the divisor), there exist unique integers q (quotient) and r (remainder), such that

$$a = mq + r, \quad 0 \leq r < |m|.$$

Note: The computation of q and r as above is called Euclidean division.

In spite of its name, the above should be seen as a theorem. It's proof is obvious from a drawing: find the *mq* to the left of *a*.



- The Euclidean division of 8 by 3 yields

$$8 = 3 \times 2 + 2$$

- The Euclidean division of -8 by 3 yields

$$-8 = 3 \times (-3) + 1$$

- The Euclidean division of 8 by -3 yields

$$8 = -3 \times (-2) + 2$$

- The Euclidean division of -8 by -3 yields

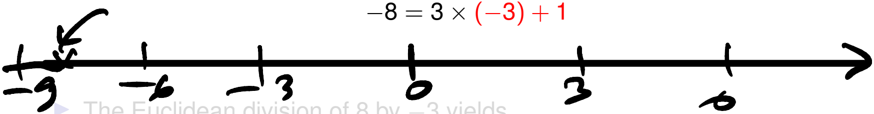
$$-8 = -3 \times 3 + 1$$

- The Euclidean division of 8 by 3 yields

$$8 = 3 \times 2 + 2$$

- The Euclidean division of -8 by 3 yields

$$-8 = 3 \times (-3) + 1$$



- The Euclidean division of 8 by -3 yields

$$8 = -3 \times (-2) + 2$$

- The Euclidean division of -8 by -3 yields

$$-8 = -3 \times 3 + 1$$

- The Euclidean division of 8 by 3 yields

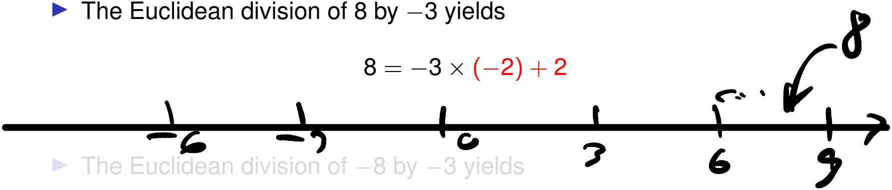
$$8 = 3 \times 2 + 2$$

- The Euclidean division of -8 by 3 yields

$$-8 = 3 \times (-3) + 1$$

- The Euclidean division of 8 by -3 yields

$$8 = -3 \times (-2) + 2$$



- The Euclidean division of -8 by -3 yields

$$-8 = -3 \times 3 + 1$$

- The Euclidean division of 8 by 3 yields

$$8 = 3 \times 2 + 2$$

- The Euclidean division of -8 by 3 yields

$$-8 = 3 \times (-3) + 1$$

- The Euclidean division of 8 by -3 yields

$$8 = -3 \times (-2) + 2$$

- The Euclidean division of -8 by -3 yields

$$-8 = -3 \times 3 + 1$$

Euclidean division in mainstream programming languages

In `C/C++/Java/Python` we use the operator % to compute r as follows.

If a and m are both positive, then $r = a \,\%\, m$.

If one or the other or both are negative, different languages behave differently, but the general rule is:

- if $a \,\%\, m$ is nonnegative, then $r = a \,\%\, m$;
- if $a \,\%\, m$ is negative, then $r = a \,\%\, m + m$.

More precisely about the value of $a \% m$:

- `C/C++/Java`: $a \% m$ has the same sign as a.
- `Python`: $a \% m$ has the same sign as m.

Example

a	m	$a \% m$ in `C/C++/Java`	$a \% m$ in `Python`	r
8	3	2	2	2
−8	3	−2	1	1
8	−3	2	−1	2
−8	−3	−2	−2	1

USEFUL INTERNET TOOLS

- Wolfram Alpha: `https://www.wolframalpha.com`

EXAMPLE

```
5%3
```

- Python in browser: `https://trinket.io/python`

EXAMPLE

```
a= 5%3
print a
```

Both behave like Python, i.e., the sign of $a \,\%\, m$ is that of m.

mod OPERATION

From now on, unless otherwise specified, the divisor will be a positive integer m.

By

$$r = a \mod m,$$

we denote the remainder r when the integer a is divided by m.

Example

A pie that has 7 slices has to be divided evenly among 3 people. Then $7 \mod 3$ is the number of slices left over.

Example

The arrival time of a trip that starts at time 13 h and lasts 40 hours is $5 = 13 + 40 \mod 24$.

Congruence

Sometimes we are interested in knowing if two numbers have the same remainder when divided by m.

Definition

Two integers a and b are said to be **congruent modulo** m, denoted

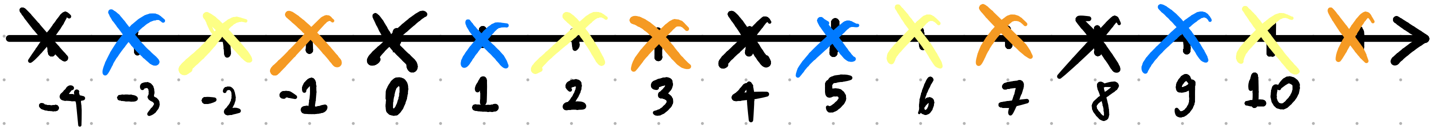
$$a \equiv b \pmod{m},$$

if $m \mid a - b$.
(Read m divides $a - b$.)

Note: do not confuse the relation $a \equiv b \pmod{m}$ and the function $a \to a \mod m$.

CONGRUENCE BY COLOR

Let $m = 4$ for example.



$$-3 = 1 \equiv 5 \equiv 9 \pmod{4}$$

Example

- $23 \equiv 21 \pmod{2}$
- $23 \equiv 3 \pmod{5}$
- $x \equiv 0 \pmod{5}$ means that x is a multiple of 5

Exercise

Which of these are true statements?

1. If $x \equiv 3 \pmod 5$, then x is not a multiple of 5.
2. If $x \equiv 25 \pmod 5$, then x is not a multiple of 5.
3. If $x \equiv 0 \pmod 5$, then x is a multiple of 5.

Solution

1. (true:) $x \equiv 3 \pmod{5}$ means that $x - 3$ is divisible by 5.
   $\Rightarrow$ x is not a multiple of 5.

2. (false:) $x \equiv 25 \pmod{5}$ means that $x - 25$ is divisible by 5.
   $\Rightarrow$ x is divisible by 5.

3. (true:) $x \equiv 0 \pmod{5}$ means that x is divisible by 5.

The following statements are equivalent:

- $a \equiv b \pmod{m}$
- $(a - b) \bmod m = 0$
- $a \bmod m = b \bmod m$

Congruence is an equivalence relation

A binary relation $\sim$ on a set is an **equivalence relation** iff the following three axioms are satisfied:

- $a \sim a$ (reflexivity)
- if $a \sim b$ then $b \sim a$ (symmetry)
- if $a \sim b$ and $b \sim c$ then $a \sim c$ (transitivity)

Substitute $a \sim a$ with $a \equiv a \pmod{m}$ etc. to see that congruence is an equivalence relation.

One of the consequences is that we can form equivalence classes and we can work with one representative of each class. (This will become useful later.)

EXAMPLE

Let $\mathcal{A} = \mathbb{Z}$ and consider modulo $m = 4$.

$3 \sim 7 \qquad 3 \equiv 7 \pmod{4}$

$3 \sim 11 \qquad 3 \equiv 11 \pmod{4}$

EQUIVALENCE CLASSES

AN EQUIVALENCE RELATION $\sim$ BREAKS $\mathcal{A}$ INTO DISJOINT SETS, CALLED $\boxed{\text{EQUIVALENCE CLASSES}}$

(EVERY $a \in \mathcal{A}$ IS IN ONE OF THE CLASSES)

EXAMPLE

Let $\mathcal{A} = \mathbb{Z}$ and consider modulo $m = 4$.

$$\{ \ldots, -8, -4, 0, 4, 8, 12, 16, \ldots \}$$

$$\{ 1, 5, 9, \}$$

$$\{ 2, 6, 10, 14, \ldots \}$$

$$\{ \ldots, -5, -1, 3, 7, 11, \ldots \}$$

MODULO RULES

(1) $a + b \mod m$

$$= (a \mod m) + (b \mod m) \mod m$$

(2) $ab \mod m$

$$= (a \mod m)(b \mod m) \mod m$$

MODULO RULES

(MORE GENERAL VERSION)

(1) $$a + b \bmod m$$

$$= a + (b \bmod m) \bmod m$$

(2) $$ab \bmod m$$

$$= a\,(b \bmod m) \bmod m$$

MODULO RULES

(MORE GENERAL VERSION)

(1) $$a + b \mod m$$

$$= a + (b \mod m) \mod m$$

THIS IMPLIES:

$$a + b \mod m = a + \underbrace{(b \mod m)}_{=\tilde{b}} \mod m$$

$$= \tilde{b} + a \mod m$$

$$= \tilde{b} + (a \mod m) \mod m$$

MODULO RULES

RECALL:

(2) $$ab \bmod m$$

$$= (a \bmod m)(b \bmod m) \bmod m$$

THIS DIRECTLY IMPLIES:

(3) $$a^n \bmod m$$

$$= (a \bmod m)^n \bmod m$$

MODULO RULES

PROOF:

$$a = m q_a + r_a$$
$$b = m q_b + r_b$$

$$a+b = m q_a + r_a + m q_b + r_b$$
$$= m(q_a + q_b) + r_a + r_b$$

MODULO RULES

PROOF:

$$\boxed{\begin{aligned} a &= m q_a + r_a \\ b &= m q_b + r_b \end{aligned}}$$

$$\begin{aligned} a+b &= (m q_a + r_a) + (m q_b + r_b) \\ &= m(q_a + q_b) + r_a + r_b \end{aligned}$$

$$\begin{aligned} (a+b) \bmod m &= (m(q_a+q_b) + r_a + r_b) \bmod m \\ &= (r_a + r_b) \bmod m \end{aligned}$$

MODULO RULES

PROOF:

$$\boxed{\begin{aligned} a &= m q_a + r_a \\ b &= m q_b + r_b \end{aligned}}$$

$$\begin{aligned} ab &= (m q_a + r_a)(m q_b + r_b) \\ &= m^2 q_a q_b + m q_a r_b + m q_b r_a + r_a r_b \end{aligned}$$

MODULO RULES

PROOF:

$$\boxed{\begin{aligned} a &= m q_a + r_a \\ b &= m q_b + r_b \end{aligned}}$$

$$ab = (mq_a + r_a)(mq_b + r_b)$$

$$= (m^2 q_a q_b + m q_a r_b + m q_b r_a + r_a r_b)$$

$$(ab) \bmod m = (r_a r_b) \bmod m$$

MODULO RULES

EXPRESSED IN "CONGRUENCE":

IF $a \equiv a' \pmod{n}$

$\boxed{a, a', b, b' \in \mathbb{Z}}$ $b \equiv b' \pmod{n}$

THEN $a+b \equiv a'+b' \pmod{n}$

$ab \equiv a'b' \pmod{n}$

Useful Rules (Thm 7.9 of textbook)

If

$$\begin{aligned} a &\equiv a' \pmod{m} \\ b &\equiv b' \pmod{m} \end{aligned}$$

then

$$\begin{aligned} a + b &\equiv a' + b' \pmod{m} \\ ab &\equiv a'b' \pmod{m} \\ a^n &\equiv (a')^n \pmod{m} \end{aligned}$$

In particular, if $a' = (a \mod m)$ and $b' = (b \mod m)$, then we obtain the following facts (useful in $\mod$ calculations)

- $(a+b) \equiv \big((a \mod m) + (b \mod m)\big) \pmod{m}$
- hence
- $(a+b) \mod m = \big((a \mod m) + (b \mod m)\big) \mod m$

- $ab \equiv \big((a \mod m)(b \mod m)\big) \pmod{m}$
- hence
- $(ab) \mod m = \big((a \mod m)(b \mod m)\big) \mod m$

- $a^n \equiv \big(a \mod m\big)^n \pmod{m}$
- hence
- $a^n \mod m = \big(a \mod m\big)^n \mod m$

Bottom line: If the final result is mod m, then intermediate results can be reduced mod m.

Example

- $23 \equiv 3 \pmod{5}$

- $2 \equiv 2 \pmod{5}$

- Hence $23 + 2 \equiv 5 \pmod{5}$

Example

- $(123 + 97) \pmod 2 = (1 + 1) \pmod 2 = 0$

- $(123 \cdot 97) \pmod 2 = (1 \cdot 1) \pmod 2 = 1$

- $\big((1234 \cdot 333) + 41(76 + 5)\big) \mod 2 = \big((0 \cdot 1) + 1(0 + 1)\big) \mod 2 = 1$

Exercise

Which of these is/are correct?

1. $23 \equiv 3 \pmod{5}$
2. $-23 \equiv -3 \pmod{5}$
3. $-23 \equiv 2 \pmod{5}$

Exercise

Which of these is/are correct?

1. $23 \equiv 3 \pmod 5$
2. $-23 \equiv -3 \pmod 5$
3. $-23 \equiv 2 \pmod 5$

Solution

1. $23 \equiv 3 \pmod 5$ is correct: $23 - 3$ is divisible by 5
2. $-23 \equiv -3 \pmod 5$ is correct: multiply the above on both sides by -1
3. $-23 \equiv 2 \pmod 5$ is correct: use item 2 and $0 \equiv 5 \pmod 5$.

EXAMPLE

IS $2 + 2^{1000}$ DIVISIBLE BY 3 ?

$$\left(2 + 2^{1000}\right) \bmod 3$$

$$= \left((2 \bmod 3) + (-1 \bmod 3)^{1000} \right) \bmod 3$$

$$= \left(2 + (-1)^{1000} \right) \bmod 3$$

$$= (2 + 1) \bmod 3$$

$$= 0$$

Less Trivial example

Example (Is $2 + 2^{1000}$ divisible by 3?)

- $2 \equiv -1 \pmod 3$
- $2^{1000} \equiv (-1)^{1000} \equiv 1 \pmod 3$
- $2 + 2^{1000} \equiv -1 + 1 \equiv 0 \pmod 3$

Hence $2 + 2^{1000}$ is divisible by 3.

Attention: we cannot reduce the exponent!

$$2^2 \mod 2 = 0 \neq 2^0 \mod 2 = 1.$$

Exercise

Is $9^{1000} + 9^{10^6}$ divisible by 5?

$$\left(9^{1000} + 9^{10^6}\right) \bmod 5$$

$$= \left(\left(-1 \bmod 5\right)^{1000} + \left(-1 \bmod 5\right)^{10^6}\right) \bmod 5$$

$$= \left((-1)^{1000} + (-1)^{10^6}\right) \bmod 5$$

Exercise

Is $9^{1000} + 9^{10^6}$ divisible by 5?

Solution

- $9 \equiv -1 \pmod 5$
- $9^{1000} + 9^{10^6} \equiv (-1)^{1000} + (-1)^{10^6} \equiv 1 + 1 \equiv 2 \pmod 5$

Hence $9^{1000} + 9^{10^6}$ is not divisible by 5.

Even Numbers

- $10 \equiv 0 \pmod{2}$
- $10^n \equiv 0^n \equiv 0 \pmod{2}$, n positive integer

$$\begin{aligned} 1234 &= 1 \cdot 10^3 + 2 \cdot 10^2 + 3 \cdot 10^1 + 4 \\ &\equiv 1 \cdot 0 + 2 \cdot 0 + 3 \cdot 0 + 4 \pmod{2} \\ &\equiv 4 \pmod{2} \\ &\equiv 0 \pmod{2} \end{aligned}$$

Hence 1234 is divisible by 2.

We see that a decimal number is divisible by 2 iff the last digit is divisible by 2. (Not new to us, but the method generalizes.)

MOD 9 IN THE DECIMAL SYSTEM IS SPECIAL!

EX: 579'146 mod 9

$$= (5 \cdot 10^5 + 7 \cdot 10^4 + 9 \cdot 10^3 + 1 \cdot 10^2 + 4 \cdot 10^1 + 6) \bmod 9$$

$$= (5 + 7 + 9 + 1 + 4 + 6) \bmod 9$$

Remainder after division by 9

- $10 \equiv 1 \pmod 9$
- $10^n \equiv 1^n \equiv 1 \pmod 9$, n positive integer

$$\begin{aligned} 1234 &= 1 \cdot 10^3 + 2 \cdot 10^2 + 3 \cdot 10^1 + 4 \\ &\equiv 1 \cdot 1 + 2 \cdot 1 + 3 \cdot 1 + 4 \pmod 9 \\ &\equiv 1 + 2 + 3 + 4 \pmod 9 \\ &\equiv 10 \pmod 9 \\ &\equiv 1 \pmod 9 \end{aligned}$$

Hence the remainder after division of 1234 by 9 is 1.

To obtain the rest after division of a decimal number by 9, we can substitute the number with the sum of its digits.

Example (mod 9)

$$\begin{aligned}
1234567890 &\equiv 1+2+3+4+5+6+7+8+9+0 \pmod 9\\
&\equiv 45 \pmod 9\\
&\equiv 0 \pmod 9
\end{aligned}$$

EXERCISE

180'000 MOD 97

$= 18 \cdot 100 \cdot 100 \mod 97$

$= 18 \cdot 3 \cdot 3 \mod 97$

$= 162 \mod 97$

$= 65.$

YESTERDAY

- MODULO STRUCTURE

→ EQUIVALENCE RELATION

→ EQUIVALENCE CLASSES

- MODULO TRICKS
  - ADDITION
  - MULTIPLICATION

$28^{42} \bmod 67$

$$
\begin{aligned}
& 28^{2} \bmod 67 \\
&= 4 \cdot 7 \cdot 4 \cdot 7 \bmod 67 \\
&= 7(4 \cdot 4 \cdot 7) \bmod 67 \\
&= 7(4 \cdot 4 \cdot 7 \bmod 67) \bmod 67 \\
&= 7(112 \bmod 67) \bmod 67
\end{aligned}
$$

$= 7 \cdot 45 \mod 67$

$= 7 \cdot 9 \cdot 5 \mod 67$

$= (63 \mod 67) \cdot 5 \mod 67$

$= (-4 \mod 67) \cdot 5 \mod 67$

$= -20 \mod 67$

$= 47$

- MODULO TRICKS
  - ADDITION
  - MULTIPLICATION

$28^{42} \mod 67$

$28^{2} \mod 67$

$= 4 \cdot 4 \cdot 7 \cdot 7 \mod 67$

$= 7 \cdot 112 \mod 67 = 7 \cdot 45 \mod 67$

$= 7 \cdot 9 \cdot 5 \mod 67 = 63 \cdot 5 \mod 67$

$= -4 \cdot 5 \mod 67 = -20 \mod 67 = \underline{\underline{47}}.$

- MODULO TRICKS
  - ADDITION
  - MULTIPLICATION

$28^{42} \bmod 67$

$28^2 \bmod 67 = 47$

$$\begin{aligned} 28^4 \bmod 67 &= (28^2)^2 \bmod 67 \\ &= (28^2 \bmod 67)^2 \bmod 67 \\ &= 47^2 \bmod 67 \end{aligned}$$

$$= (47 \bmod 67)^2 \bmod 67$$

$$= (-20 \bmod 67)^2 \bmod 67$$

$$= 400 \bmod 67$$

$$= 4 \cdot (100 \bmod 67) \bmod 67$$

$$= 4 \cdot 33 \bmod 67$$

$$= 65$$

- MODULO TRICKS
  - ADDITION
  - MULTIPLICATION

$$28^{42} \bmod 67$$

$$28^{2} \bmod 67 = 47$$

$$28^{4} \bmod 67 = (28^{2})^{2} \bmod 67$$

$$= (28^{2} \bmod 67)^{2} \bmod 67$$

$$= 47^{2} \bmod 67$$

$28^{42} \mod 67$

$28^{2} \mod 67 = 47$

$28^{4} \mod 67 = 65$

$28^{8} \mod 67 = 4$

$28^{16} \mod 67 = 16$

$28^{32} \mod 67 = 55$

$28^{42} = 28^{32} \cdot 28^{8} \cdot 28^{2}$

$$
\begin{aligned}
28^{42} &\equiv 55 \cdot 4 \cdot 47 \pmod{67} \\
&\equiv (-12) \cdot 4 \cdot (-20) \\
&\equiv 12 \cdot 13 \\
&\equiv 2 \cdot 6 \cdot 13 \equiv 2 \cdot 11 \equiv 22
\end{aligned}
$$

CHECK DIGITS MOD 97

- Write down an integer in decimal notation, e.g.,

$$021\,235\,1234$$

- Compute its remainder after division by 97:

$$021\,235\,1234 \mod 97 = 95$$

- Append the remainder to the number, as a check digit:

$$021\,235\,1234\,95$$

- A common mistake consists in transposing two digits:

$$021\,253\,1234\,95$$

- The check digits are no longer consistent:

$$021\,253\,1234 \mod 97 = 63$$

PROCEDURE MOD $97 - 10$

It is a variant of the previous one:

1. Append 00 (i.e., multiply the number by 100)
2. Let r be the remainder after division by 97
3. The check digits are $c = 98 - r$ (written as a 2-digit number, e.g., 03)
4. Replace 00 with c
5. Check: the resulting number mod 97 equals 1

PROCEDURE MOD $97-10$: WHY THE CHECK IS AS STATED

Encoding:

$$n \longmapsto 100n + \underbrace{98 - (100n \mod 97)}_{\text{check digits}}$$

Check: we compute the resulting number mod 97:

$$\begin{aligned} & 100n + 98 - (100n \mod 97) \mod 97 \\ = \quad & 100n + 98 - 100n \mod 97 \\ = \quad & 98 \mod 97 \\ = \quad & 1 \end{aligned}$$

Example (mod $97-10$)

1. $n = 212351234$
2. $n \longmapsto 21235123400 + \underbrace{(98-91)}_{\text{check digits}} = 21235123407$
3. Check: $21235123407 \mod 97 = 1$. Check passed
4. If we transpose: 21253123407
5. Check: $21253123407 \mod 97 = 2$. Check **not** passed

Next lecture we will see why Mod $97-10$ always detects a transposition.

IBAN (International Bank Account Number)

Main difference to MOD $97 - 10$: The check digits are in position 3 and 4

Example:

1. Account number: $\overbrace{00243}^{\text{bank, 5 digits}}\ \overbrace{0001\,2345\,6789}^{\text{account, 12 digits}}$
2. Append CH (for a Swiss bank account): 00243 0001 2345 6789 CH
3. Convert into numbers according to: $A \mapsto 10, \ldots, Z \mapsto 35$:

   00243 0001 2345 6789 1217

4. MOD $97 - 10$ procedure:

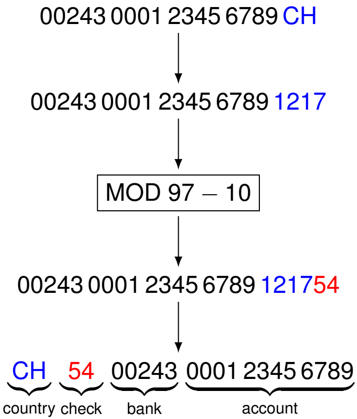
   00243 0001 2345 6789 121754

5. Reposition:

   CH54 00243 0001 2345 6789

6. To verify, we undo the repositioning and do the MOD $97 - 10$ check.

IBAN construction



00243 0001 2345 6789 CH

00243 0001 2345 6789 1217

MOD 97 – 10

00243 0001 2345 6789 121754

$\underbrace{\text{CH}}_{\text{country}}\ \underbrace{\text{54}}_{\text{check}}\ \underbrace{\text{00243}}_{\text{bank}}\ \underbrace{\text{0001 2345 6789}}_{\text{account}}$

MOD 12

YES!

SUPPOSE $2 + x \equiv 2+y \pmod{12}$

DOES THIS IMPLY $x \equiv y \pmod{12}$

$$a = 2+x \qquad a' = 2+y$$

$$b = -2 \qquad b' = -2$$

$$\left.\begin{aligned} a+b &\equiv a'+b' \\ 2+x-2 &\equiv 2+y-2 \\ x &\equiv y \end{aligned}\right\} \pmod{12}$$

MOD 12

COUNTER EX: $x=6$, $y=12$.

NO!

SUPPOSE $2x \equiv 2y \pmod{12}$

DOES THIS IMPLY $x \equiv y \pmod{12}$

$a = 2x$ $\qquad$ $a' = 2y$

$b =$ CANNOT FIND! $b' =$

$$ab \equiv a'b'$$

$$b2x \equiv b'2y$$

MOD 12

YES!

SUPPOSE $5x \equiv 5y \pmod{12}$

DOES THIS IMPLY $x \equiv y \pmod{12}$

$a = 5x \qquad a' = 5y$

$b = 5 \qquad b' = 5$

$$ab \equiv 25x \equiv a'b' \equiv 25y$$

$$\underbrace{(25 \bmod 12)}_{=1} x \equiv \underbrace{(25 \bmod 12)}_{=1} y$$

CONCLUSION:

MOD 12 IS NOT SUCH A PRETTY PLACE!

Exercise

Is the following statement correct?

$$2 + x \equiv 2 + y \pmod{12} \implies x \equiv y \pmod{12}$$

Exercise

Is the following statement correct?

$$2 + x \equiv 2 + y \pmod{12} \implies x \equiv y \pmod{12}$$

Solution

We are allowed to add and multiply on both sides as we do when we solve equations over the reals.

By adding -2 on both sides:

$$2 + x \equiv 2 + y \pmod{12} \Rightarrow x \equiv y \pmod{12}$$

The statement is true.

(Which property of the "useful rules" have we used?)

EXERCISE

Is the following statement correct?

$$2x \equiv 2y \pmod{12} \implies x \equiv y \pmod{12}$$

Exercise

Is the following statement correct?

$$2x \equiv 2y \pmod{12} \implies x \equiv y \pmod{12}$$

Solution

No. The multiplicative inverse of 2 does not exist $\pmod{12}$.

For instance

$$2 \times 9 \equiv 2 \times 3 \pmod{12},$$

however

$$9 \not\equiv 3 \pmod{12}$$

(Why can't we say that $\frac{1}{2} \equiv \frac{1}{2} \pmod{12}$ and multiply both sides by $\frac{1}{2}$?)

PRIME NUMBERS

DEFINITION

A **prime number** (or a **prime**) is an integer > 1 that has no positive divisors other than 1 and itself.

$2, 3, 5, 7, 11, 13, 17, 19, 23, 29, \ldots$ are prime numbers.

Non-primes are called **composites**.

EXERCISE

Many people forget if 1 is prime or not. Why is it not?

Exercise

Many people forget if 1 is prime or not. Why is it not?

Solution

Because if we declare 1 to be a prime number, then the following fundamental theorem is no longer valid.

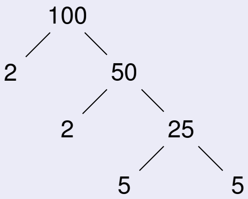
PRIME NUMBERS

THEOREM (PRIME FACTORIZATION: SHORT VERSION)

Every integer greater than 1 has a unique prime factorization (except for order).

$$12 = 2^2 \cdot 3^1 \cdot 5^0 \cdot 7^0 \cdot$$

Example



$\Rightarrow 100 = 2 \times 2 \times 5 \times 5$

PRIME FACTORIZATION: A DIFFICULT TASK

- a number as big as 2^{700} (700 bits) can be factored
- a 1000 bits number cannot be factored (with today's technology)

  "Among the b-bit numbers, the most difficult to factor in practice using existing algorithms are those that are products of two primes of similar size. For this reason, these are the integers used in cryptographic applications. The largest such semiprime yet factored was RSA-250, an 829-bit number with 250 decimal digits, in February 2020. The total computation time was roughly 2700 core-years of computing using Intel Xeon Gold 6130 at 2.1 GHz. Like all recent factorization records, this factorization was completed with a highly optimized implementation of the general number field sieve run on hundreds of machines."

  [Wikipedia, March 23, 2023]

Theorem (Textbook Thm 7.3)

Let *a* and *b* be positive integers. *a* divides *b* iff all prime factors of *a* are present in the prime factorization of *b* with an equal or greater exponent.

$$a \mid b \iff \beta_i \geq \alpha_i \quad \forall\, i$$

$$a = p_1^{\alpha_1}\, p_2^{\alpha_2}\, p_3^{\alpha_3} \cdots p_n^{\alpha_n} \qquad \alpha_i \geq 0$$

$$b = p_1^{\beta_1}\, p_2^{\beta_2}\, p_3^{\beta_3} \cdots p_n^{\beta_n} \qquad \beta_i \geq 0$$

Example

$$168 = 2^3 \cdot 3 \cdot 7$$

$$12 = 2^2 \cdot 3$$

Hence 12 divides 168.

Example

$$30 = 2 \cdot 3 \cdot 5$$

$$12 = 2^2 \cdot 3$$

Hence 12 does not divide 30.

Definition

Let a and b be integers, not both zero. The largest integer that divides both is called the **greatest common divisor** of a and b. It is denoted by $\gcd(a, b)$.

Theorem (Textbook Thm 7.4)

Let a and b be positive integers, not both zero, and let $p_1 < p_2 < \cdots < p_k$ be the sequence of prime numbers that divide a or b. Write

$$\begin{aligned} a &= p_1^{\alpha_1} \cdots p_k^{\alpha_k} \\ b &= p_1^{\beta_1} \cdots p_k^{\beta_k}, \end{aligned}$$

with $0 \leq \alpha_i$ and $0 \leq \beta_i$. Then

$$\gcd(a, b) = p_1^{\gamma_1} \cdots p_k^{\gamma_k},$$

with $\gamma_i = \min(\alpha_i, \beta_i)$.

Example

$$\begin{aligned} 12 = 2^2 \cdot 3 &= 2^2 \cdot 3^1 \cdot 5^0 \\ 30 = 2 \cdot 3 \cdot 5 &= 2^1 \cdot 3^1 \cdot 5^1 \\ \gcd(12, 30) &= 2^1 \cdot 3^1 \cdot 5^0 = 6 \end{aligned}$$

It is an immediate consequence of the above theorem that $\gcd(a, b) = 1$ iff a and b have no common factor.

Definition

When $\gcd(a, b) = 1$, we say that a and b are **coprime** (or **relatively prime**, or **mutually prime**).

Example

$$\begin{aligned} 9 &= 3^2 \\ 100 &= 2^2 \cdot 5^2 \\ \gcd(9, 100) &= 1 \end{aligned}$$

9 and 100 are thus coprime.

COPRIME

a	b	COPRIME?
2	5	✓
6	12	✗
10	12	✗
9	15	✗
9	20	✓

COPRIME

a	b	COPRIME?
2	5	✓
6	15	✗
12	63	✗
11	47	✓
11	5	✓

Theorem (Textbook Thm 7.6)

Let p be a prime number and let a be an integer such that $0 < a < p$. Then

$$\gcd(p, a) = 1$$

Proof

The prime factorization of a cannot contain p.

EXERCISE TRUE/FALSE

IF $ab \mid c$ THEN $a \mid c$ <u>AND</u> $b \mid c$

EXERCISE TRUE/FALSE

IF $ab \mid c$ THEN $a \mid c$ **AND** $b \mid c$

$\Updownarrow$

PRIME FACTORS

$$a = p_1^{\alpha_1} p_2^{\alpha_2} \cdots$$

$$b = p_1^{\beta_1} p_2^{\beta_2} \cdots$$

$$c = p_1^{\gamma_1} p_2^{\gamma_2} \cdots$$

IF $\alpha_i + \beta_i \leq \gamma_i$ for all i

THEN

$$\left.\begin{array}{l} \alpha_i \leq \gamma_i \\ \beta_i \leq \gamma_i \end{array}\right\} \text{for all } i$$

CLEARLY TRUE!

Exercise (True or False?)

If $ab \mid c$, then $a \mid c$ and $b \mid c$.

Exercise (True or False?)

If $ab \mid c$, then $a \mid c$ and $b \mid c$.

Solution

If $ab \mid c$, then we can write $c = abd$ for some integer d.

Clearly both a and b divide c.

EXERCISE TRUE/FALSE

IF $a \mid c$ <u>AND</u> $b \mid c$ THEN $ab \mid c$

PRIME FACTORS

$$a = p_1^{\alpha_1} p_2^{\alpha_2} \cdots$$

$$b = p_1^{\beta_1} p_2^{\beta_2} \cdots$$

$$c = p_1^{\gamma_1} p_2^{\gamma_2} \cdots$$

$$\boxed{\text{EXERCISE TRUE/FALSE}}$$

IF $a \mid c$ <u>AND</u> $b \mid c$ THEN $ab \mid c$

PRIME FACTORS

$$a = p_1^{\alpha_1} p_2^{\alpha_2} \cdots$$

$$b = p_1^{\beta_1} p_2^{\beta_2} \cdots$$

$$c = p_1^{\gamma_1} p_2^{\gamma_2} \cdots$$

IF $\alpha_i \leq \gamma_i$

$\beta_i \leq \gamma_i$

for all i

THEN

$\alpha_i + \beta_i \leq \gamma_i$

for all i

$$\boxed{\text{NOT TRUE}}$$

Exercise (True or False?)

If $a \mid c$ and $b \mid c$, then $ab \mid c$.

Exercise (True or False?)

If $a \mid c$ and $b \mid c$, then $ab \mid c$.

Solution

$a \mid c$ and $b \mid c$ does not imply $ab \mid c$.

In fact, ab could exceed c.

Example: $a = b = c$.

EXERCISE TRUE/FALSE

IF $a \mid c$ <u>AND</u> $b \mid c$ <u>AND</u> $\gcd(a,b)=1$

THEN $ab \mid c$

PRIME FACTORS

$$a = p_1^{\alpha_1} p_2^{\alpha_2} \cdots$$

$$b = p_1^{\beta_1} p_2^{\beta_2} \cdots$$

$$c = p_1^{\gamma_1} p_2^{\gamma_2} \cdots$$

EXERCISE TRUE/FALSE

IF $a \mid c$ **AND** $b \mid c$ **AND** $GCD(a,b)=1$

THEN $ab \mid c$ $\Leftrightarrow$

PRIME FACTORS

$$a = p_1^{\alpha_1} p_2^{\alpha_2} \cdots$$

$$b = p_1^{\beta_1} p_2^{\beta_2} \cdots$$

$$c = p_1^{\gamma_1} p_2^{\gamma_2} \cdots$$

IF $\alpha_i \le \gamma_i$, $\beta_i \le \gamma_i$

AND $\{$IF $\alpha_i > 0$ THEN $\beta_i = 0\}$

AND $\{$IF $\beta_i > 0$ THEN $\alpha_i = 0\}$

THEN $\alpha_i + \beta_i \le \gamma_i$ for all i

$\boxed{\text{THIS IS TRUE}}$

However

Theorem

If $a \mid c$ and $b \mid c$ and $\gcd(a, b) = 1$, then $ab \mid c$.

Proof

- the prime factorization of c contains all the prime factors of a.
- the prime factorization of c contains all the prime factors of b.
- a and b have distinct prime factors.

$\Rightarrow$ $\frac{c}{a}$ is an integer that has all the prime factors of b in it.

$\Rightarrow$ Hence it is divisible by b.

- This proves that $ab \mid c$.

Example

- $a = 2 \cdot 3$
- $b = 5 \cdot 7$
- $c = 2 \cdot 3 \cdot 5 \cdot 7 \cdot 11$

EXERCISE TRUE/FALSE

IF $a \mid c$ **AND** $a \mid c+d$ THEN $a \mid d$.

EXERCISE TRUE/FALSE

IF $a \mid c$ <u>AND</u> $a \mid c+d$ THEN $a \mid d$.

$$\boxed{\text{TRUE}}$$

$$c \text{ mod } a = 0$$

$$\underbrace{c+d \text{ mod } a = 0}$$

$$\underbrace{\left\{\underbrace{(c \text{ mod } a)}_{=0}+(d \text{ mod } a)\right\} \text{ mod } a}$$

$$d \text{ mod } a = 0$$

HOW MANY PRIMES ?

HOW MANY PRIMES ?

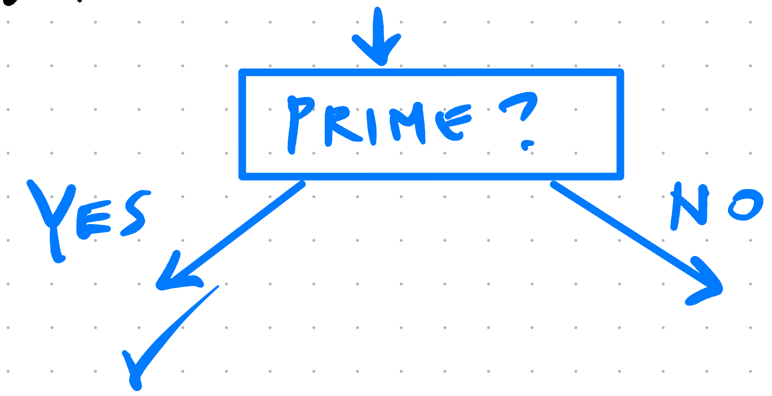
$\{2, 3, 5\}$ ← set of some primes

↳ $$\underbrace{m = 2\cdot 3\cdot 5 + 1}_{\text{IS EITHER A PRIME OR NOT!}}$$

HOW MANY PRIMES ?

$\{2, 3, 5\}$ ← set of some primes

↳ $m = 2 \cdot 3 \cdot 5 + 1 = 31$



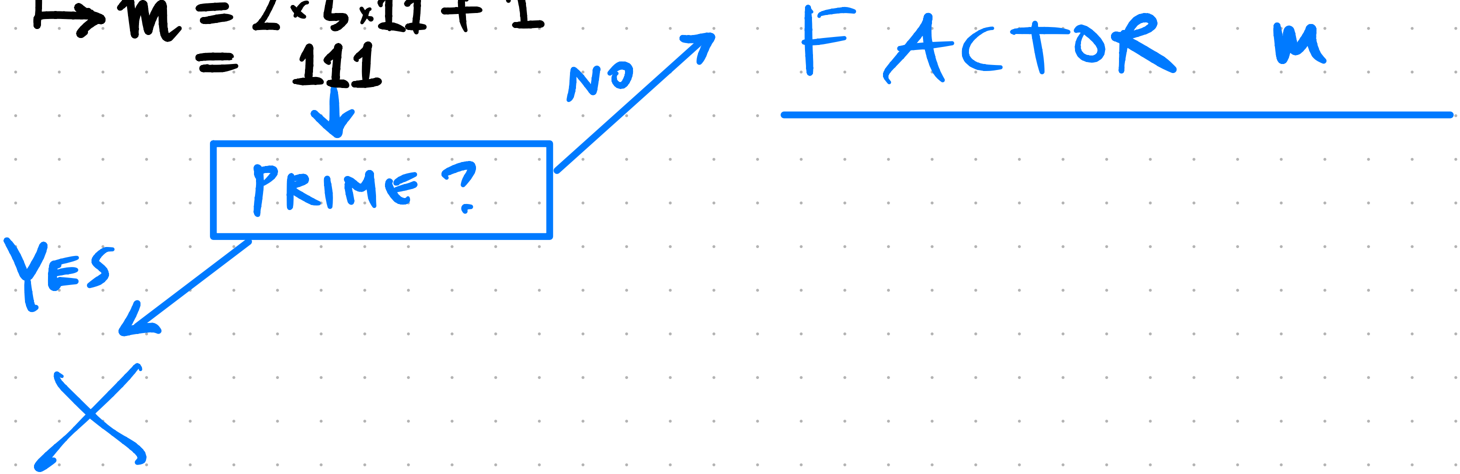
⇒ WE HAVE A NEW PRIME !

HOW MANY PRIMES ?

$\{2, 5, 11\}$ ← set of some primes

↳ $m = 2 \times 5 \times 11 + 1$

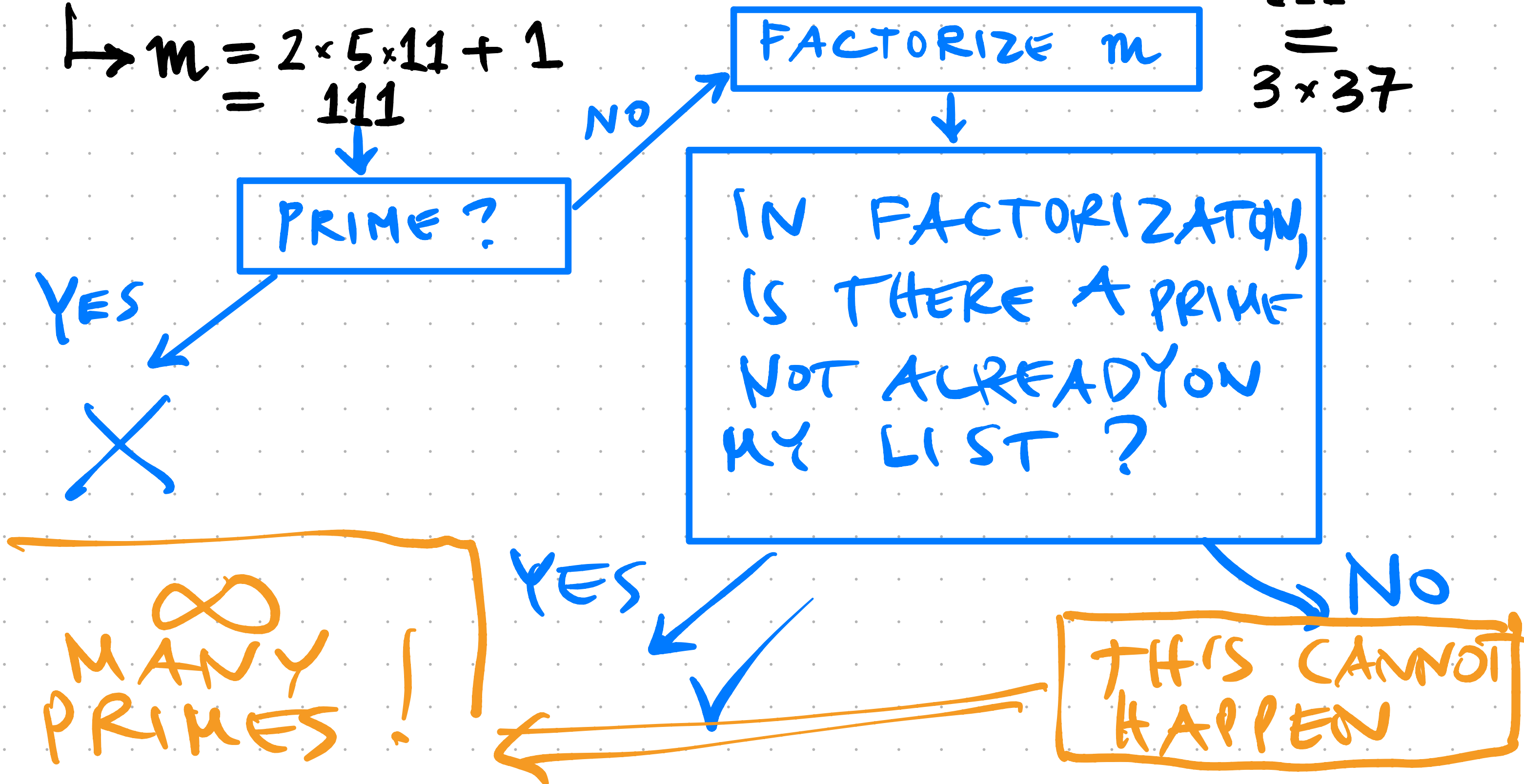
$= 111$



HOW MANY PRIMES ?

$\{2, 5, 11\}$ ← set of some primes

$\hookrightarrow m = 2 \times 5 \times 11 + 1 = 111$



PRIME ?

YES

✗

NO

FACTORIZE m

$111 = 3 \times 37$

IN FACTORIZATON, IS THERE A PRIME NOT ALREADY ON MY LIST ?

YES

✓

NO

THIS CANNOT HAPPEN

∞ MANY PRIMES !

WHY CAN'T $\circledast$ HAPPEN?

START OUT WITH LIST OF PRIMES

$$\{p_1, p_2, p_3\}$$

$$m = p_1 p_2 p_3 + 1$$

one from the list

FACTORIZE m: $\quad m = p \cdot c$

HENCE:

$$\left\{\begin{array}{l} p \mid p_1 p_2 p_3 + 1 \\ p \mid p_1 p_2 p_3 \end{array}\right.$$

$$\hookrightarrow p \mid 1$$

BUT THIS IS A CONTRADICTION.

⇒ THE ALGORITHM CANNOT TAKE THIS PATH!

NEXT QUESTION:

HOW DENSE ARE THE PRIMES?

$$\frac{N}{\log N}$$

AVERAGE DISTANCE BETWEEN PRIMES $\{1, 2, 3, \ldots, N\}$ IS ABOUT $\log N$.