Modular arithmetic.

Consider $\mathbb{Z}_n := \{0,1,2,\dots,n-1\}$, the set of residues modulo n with operations:

$$a \pm b := (a \pm b) \pmod n$$

$$a \cdot b := (ab) \pmod n$$

Example. $n=11$. Then, for instance, $\dots -5 \equiv 6 \equiv 17 \dots$,

$$7+8 \equiv 4, \quad 7 \cdot 8 \equiv 1.$$

Solving equations.

Example: $19x + 8 \equiv 7 \pmod 5$

$$4x \equiv -1 \text{ or } 4x \equiv 4$$

$$x \equiv 1$$

Check: $19 \cdot 1 + 8 = 27 \equiv 7 \pmod 5$

Answer: $x = 1 + 5k,\ k \in \mathbb{Z}$.

Remark: if $x=a$ is a solution of the initial equation (over $\mathbb{Z}$), it is a solution of the reduced one (over $\mathbb{Z}_n$), but the converse is not always true!

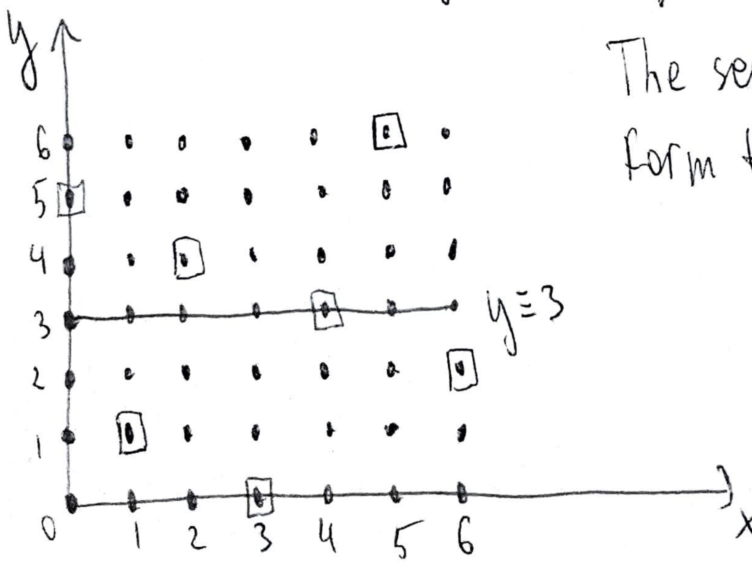
Example: $\begin{cases} 15x + 2y \equiv 24 \pmod 7 \iff x \equiv 24 - 2y \equiv 3 - 2y \\ 10y \equiv 37 \pmod 7 \end{cases}$

$3y \equiv 2 \iff 15y \equiv 10 \iff y \equiv 3.$

$x + 6 \equiv 3 \iff x \equiv -3$ or $x \equiv 4$

Answer: $(x,y) = (4,3) + 7(n,m)$ with $(n,m) \in \mathbb{Z}^2$.

Remark: solving a system of two linear eq-ns with two unknowns is equivalent to finding the intersection of two lines on a plane. In case of finite fields, like $\mathbb{F}_7 = \mathbb{Z}_7^\times$ in our example, the pictures are funny:



The seven points in '□' form the line $x \equiv 3 - 2y$.

Thm. An element x is invertible modulo n if and only if $\gcd(x,n) = 1$.

Proof:

(1) $\Rightarrow$: x is invertible, hence, $\exists a \in \mathbb{Z}_n$: $ax \equiv 1 \pmod n$ or $ax = 1 + kn$ for some k, then $ax - kn = 1$, extended Euclid's algorithm implies $\gcd(a,n) = 1$.

(2) $\Leftarrow$: $\gcd(x,n) = 1 \iff ax + bn = 1$ (for some a and b) $\iff$

$\iff ax \equiv 1 \pmod n$.

Cool application (divisibility criteria).

Examples.

(1) $a = \overline{a_n a_{n-1} \dots a_0}$ is divisible by 3 iff $\sum_{i=0}^{n} a_i$ is divisible by 3.

Proof: $10^1 \equiv 1 \pmod 3$

$10^2 \equiv 1$

$10^k \equiv 1^k \equiv 1 \pmod 3$ for any k.

$$a = \sum_{i=0}^{n} 10^i a_i \equiv \sum_{i=0}^{n} a_i .$$

(2) Let's find out when $a = \overline{a_n a_{n-1} \dots a_0}$ is divisible by 11.

$10^1 \equiv 10 \pmod{11}$

$10^2 \equiv 1$

$\vdots$

$10^{2k-1} \equiv 10 \equiv -1$

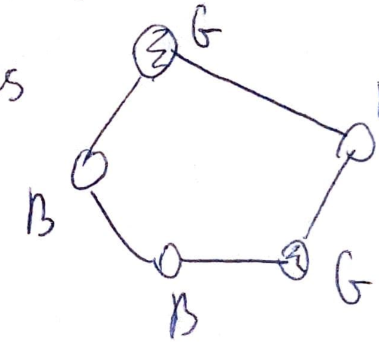
$10^{2k} \equiv 1$

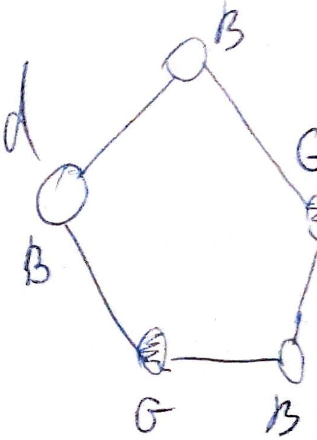
$$a = \sum_{i=0}^{n} 10^i a_i \equiv \sum_{\substack{0 \le i \le n \\ \text{even}}} a_i - \sum_{\substack{0 \le j \le n \\ \text{odd}}} a_j \equiv 0 \pmod{11} \iff$$

$$\iff \sum_{\substack{0 \le i \le n \\ \text{even}}} a_i \equiv \sum_{\substack{0 \le j \le n \\ \text{odd}}} a_j \pmod{11}$$

Thm (Fermat's little thm). Let p be a prime, then for any $a \in \mathbb{Z}, a \neq 0$: $a^{p-1} \equiv 1 \pmod{p}$.

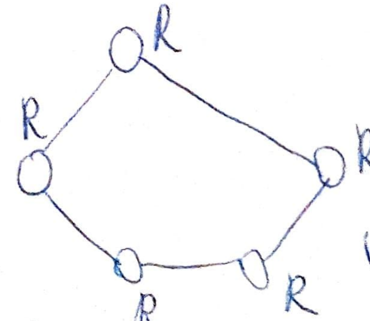
Proof: we consider a seemingly unrelated counting problem: Namely, let's find the number of necklaces with p beads and each bead having one of a possible colors. Well that is easy, we clearly get a^p. Now consider two necklaces identical if one can be obtained from the other via a rotation.

Example: the necklaces 

and 

are identical (B-blue, G-green are the colors).

How many different necklaces are there after identification?

Answer: a necklace of type 

(all beads

('R'=red)

of same color) does not give rise to any new ones under rotation. However, any 'nonidentical coloring' produces p different necklaces prior to identification.

This is not obvious! But not hard to show (see 'Bonus 2' set of problems).

We arrive with the answer that the number of distinct necklaces (multi-colored, i.e. not all beads have the same color), which are not equivalent under rotation is $\frac{a^p - a}{p}$ (we assume $0 < a < p$). As the number $\frac{a^p-a}{p}$ provides a solution to a counting problem, it must be an integer! In other words, we get

$$a^p - a \equiv 0 \pmod{p} \iff a(a^{p-1}-1) \equiv 0 \pmod{p}.$$

As p is prime, either $a \equiv 0$ or $a^{p-1} \equiv 1 \pmod{p}$ and the first possibility does not occur due to our assumption on a. $\boxtimes$.

This result is very very useful, as we will see time and again. Let's see one important corollary.

Recall that a group G is <u>cyclic</u>, if it is generated by a single element, i.e. $\exists g \in G$, s.t. $\forall h \in G$:

$$\exists k, \ h = g^k.$$

Example. Consider $G=(\mathbb{Z}/n\mathbb{Z}, +)$. It is cyclic and the generator can be chosen to be any element $\underset{0}{k<n}$, coprime ~~to~~ to n ($\gcd(k,n)=1$).

Thm. The multiplicative group $\mathbb{Z}/p\mathbb{Z}^{\times}$ is cyclic.

Proof: we have already established that for any

$$a \in \mathbb{Z}/p\mathbb{Z}^{\times} : a^{p-1} = 1 \text{ (identity in the group)}.$$

In other words the order of every element divides $p-1$.

(*) Consider the polynomial $f(x) = x^{p-1} - 1$ (modulo p). Notice that $f(a) = 0 \ \forall a \in \mathbb{Z}/p\mathbb{Z}^{\times}$. Suppose, contrary to the cyclicity property we are trying to establish the order of every element is strictly less than $p-1$: $\operatorname{ord}(a) < p-1 \ \forall a \in \mathbb{Z}/p\mathbb{Z}^{\times}$. Let $k := \gcd\limits_{a \in \mathbb{Z}/p\mathbb{Z}^{\times}} (\operatorname{ord}(a))$, then $k < p-1$ is a divisor of $p-1$ and, moreover every el-t a is a root of $g(x) := x^k - 1$. The crucial observation here is that a polynomial of degree k cannot have more than k roots unless it is identically 0, from which we conclude that there must exist an el-t $g \in \mathbb{Z}/p\mathbb{Z}^{\times}$ with $\operatorname{ord}(g) = p-1$, which automatically generates the group.

(*) a polynomial $f(x) \not\equiv 0$, s.t. $f(a) = 0 \ \forall a \in \mathbb{Z}/p\mathbb{Z}^{\times}$ of minimal degree.

Example. $\mathbb{Z}/_{5\mathbb{Z}}^{*}$, then $g=2$ is a generator. Indeed, $\{2, 4, 3, 1\}$ is the full collection of elements.

$$\begin{array}{cccc} 2, & 4, & 3, & 1 \\ \shortparallel & \equiv & \equiv & \equiv \\ 2^1 & 2^2 & 2^3 & 2^4 \end{array}$$

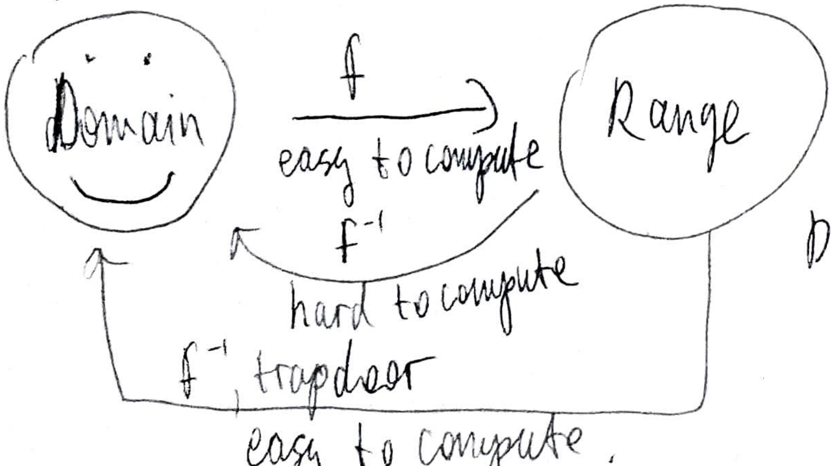
Let's try $g=3$: $3^1 \equiv 3$, $3^2 \equiv 4$, $3^3 \equiv 2$, $3^4 \equiv 1$. Works as well!
What about $g=4$? $4^1 \equiv 4$, $4^2 \equiv 1$ Oops... 4 is not a generator.

Back to Cryptography

We will need to familiarize ourselves with a few concepts:

- A <u>one-way function</u> is an invertible function, which is easy to compute, but the inverse is difficult to find (no known algorithm can compute it reasonably fast, say, within 100^{100} years) without additional info.
- A <u>trapdoor</u> is a piece of auxiliary info that allows to compute the inverse fast and easy.

<u>Summary</u>:



Public Key Crypto-system (PKC), after Diffie and Hellman

One of the most famous PKCs is the one invented by Rivest, Shamir, and Adleman (known as RSA). It is used since late 1970's and has withstood the test of time.

Next we describe the most widely used way to obtain PKCs.

The discrete logarithm problem (DLP).

Let G be a finite group, consider an element g of known order $k = \operatorname{ord} g$.

DLP is the following problem: given (G, g, k) and $h = g^s$, find s.

Examples:

(1) $G = (\mathbb{Z}/100\mathbb{Z}, +)$; $g = 5$, $h = 35$.

DLP: $5s \equiv 35 \rightsquigarrow s \equiv 7$. Easy!

(1)' Same G, $g = 31$, $h = 7$.

DLP: $31s \equiv 7 \pmod{100}$

Notice that $\gcd(31, 100) = 1$, hence 31 is invertible modulo 100. Let's find the inverse:

$$100 = 3 \cdot 31 + 7$$
$$31 = 4 \cdot 7 + 3$$
$$7 = 2 \cdot 3 + 1$$

$$1 = 7 - 2 \cdot 3 = 7 - 2 \cdot (31 - 4 \cdot 7) = 9 \cdot 7 - 2 \cdot 31 = 9 \cdot (100 - 3 \cdot 31) - 2 \cdot 31 =$$
$$= 9 \cdot 100 - 29 \cdot 31.$$

Hence, $-29 \cdot 31 + 9 \cdot 100 = 1 \Leftrightarrow -29 \cdot 31 \equiv 1 \pmod{100} \Leftrightarrow 71 \cdot 31 \equiv 1$

$31s \equiv 7 \Leftrightarrow s \equiv 71 \cdot 7 \Leftrightarrow s \equiv 97 \Leftrightarrow s \equiv -3.$

A bit harder, but not a big deal!

(2) $G = \mathbb{F}_p^\times$ (or $\mathbb{Z}/p\mathbb{Z}^\times$ in our old notation).

$\mathbb{F}_{13}$, $g=2$, $\mathrm{ord}(g)=12$ (it is a generator), $h=7$

DLP: find s with $2^s \equiv 7 \pmod{13}$.

stupid (straightforward) approach:

$2^1 \equiv 2, 2^2 \equiv 4, 2^3 \equiv 8, \dots, 2^{12} \equiv 7$.

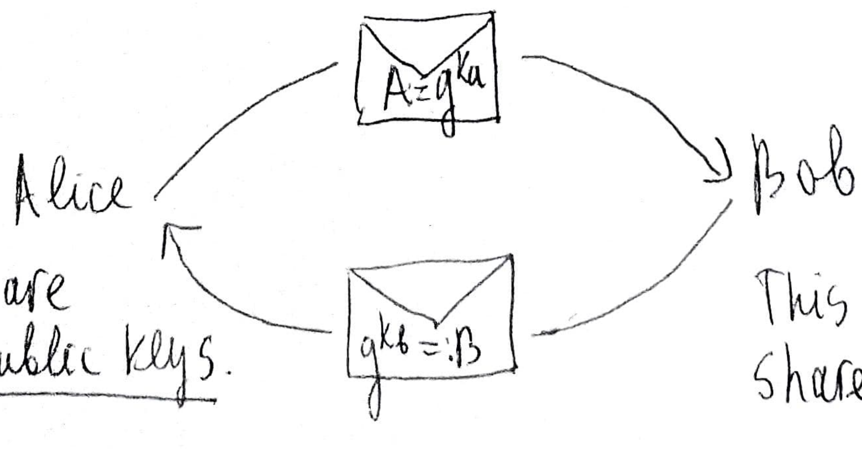
Doesn't look like a fast algorithm. Say, p ~~of~~ order 10^{10} would be a problem...

There are faster algorithms (we will discuss them later), but not fast enough...

Diffie-Hellman key exchange.

Goal: Alice and Bob want to share a secret key to use in a symmetric cipher, but do not have a secure channel of communication.

Solution: they choose a large p and $g \in \mathbb{F}_p^\times$ of large prime order q. Alice chooses a secret number k_a and Bob k_b.



Upon receiving:

Bob: A^{k_b}

Alice: B^{k_a}

Notice: $A^{k_b} \equiv g^{k_a k_b} \equiv B^{k_a}$

This number becomes their shared key k.

A and B are called public keys.

Symmetric ciphers.

Now Alice and Bob have a secret shared key k, consider the encryption map

$$e: \underset{\text{plaintexts}}{\mathcal{M}} \to \underset{\text{ciphertexts.}}{\mathcal{C}} \quad (e \text{ is a function of } k \text{ and } m).$$

and decryption map:

$$d: \mathcal{C} \to \mathcal{M} \quad (\text{again a function of } k \text{ and } c).$$

Obviously, it is natural to impose that d is the inverse of e, i.e.

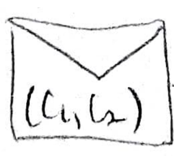
$$d(k, \underbrace{e(k,m)}_{= e_k(m)}) = m \quad \forall m \in \mathcal{M}.$$

The Elgamal PKC.

We present a very natural symmetric PKC using the shared key k described above discovered by Elgamal.

Bob needs to send Alice a message $m \in \mathbb{F}_p^\times$ (plaintext).

1. Bob computes a pair of numbers (c_1, c_2): $c_1 \equiv g^{k_b}$ and $c_2 \equiv m A^{k_b}$ (where $k_b \in \mathbb{F}_p^\times$ is a random number chosen by Bob) and sends to Alice:

Bob ——  ⟶ Alice

2. Alice decodes m via $C_2 \cdot C_1^{-k_a} \equiv m \cdot g^{k_b \cdot k_a} \cdot g^{-k_b \cdot k_a}$,