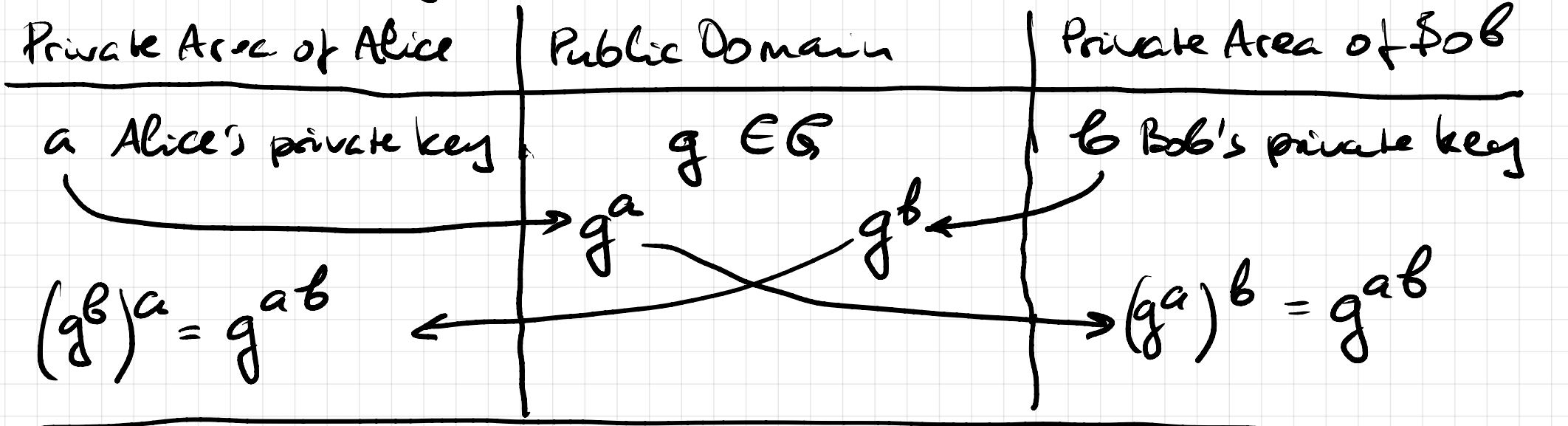
We can use ElGamal to let Alice and Bob generate shared private data by communicating exclusively over the public domain. For this, we need two copies of ElGamal, one for Alice and one for Bob, which share the generator $g \in G$ of the cycle $\langle g \rangle$.



g^{ab} is the shared secret (shared private information of Alice and Bob). This information can be used for symmetric encryption.

It's enough for Eve to determine a or b in order to obtain g^{ab}. But this requires solving the DLG.

The above system is called the Diffie-Hellman key exchange

One standard choice of the group for ElGamal and Diffie-Hellman is $(\mathbb{Z}_p \setminus \{0\}, \cdot)$ where p is a multidigit prime number. However, not every prime number is equally good. One normally uses the so called safe primes.

Def. A prime number p is called safe if $p > 2$ and $\frac{p-1}{2}$ is also a prime number.

Example

	safe?
2	×
3	×
5	✓
7	✓
11	✓
13	×

Open Problem Are there infinitely many safe prime numbers?

No one knows.

We want to clarify how we could pick a generator of $(\mathbb{Z}_p \setminus \{0\}, \cdot)$ when p is a safe prime number.

Theorem 17 (Lagrange) For every finite group $(G, \cdot)$ and a subgroup H of G, $|G|$ is divisible by $|H|$.

Proof: For every $x \in G$ we introduce the coset of x modulo H by $xH := \{x \cdot h : h \in H\}$.

Example if $\cdot$ is $+$, we write $x + H$.

$H = 3\mathbb{Z}$ the set of all integers multiples of 3, a subgroup of $(\mathbb{Z}, +)$

$z + H = z + 3\mathbb{Z}$

$z = 0 \Rightarrow \{0, \pm 3, \pm 6, \pm 9, \ldots\}$

$z = 1 \Rightarrow \{1, 1 \pm 3, 1 \pm 6, 1 \pm 9, \ldots\}$

$z = 2 \Rightarrow \{2, 2 \pm 3, 2 \pm 6, 2 \pm 9, \ldots\}$

$0 + 3\mathbb{Z} = 3\mathbb{Z}$

$1 + 3\mathbb{Z}$

$2 + 3\mathbb{Z}$

$3 + 3\mathbb{Z} = 3\mathbb{Z}$

The set xH has the same number of elements as H, because every element $h \in H$ determines the element $x \cdot h$ in xH and for two distinct elements $h_1, h_2 \in H$ the elements xh_1 and xh_2 in xH are also distinct; in fact, if they were equal: $xh_1 = xh_2$, then $x^{-1} \cdot (xh_1) = x^{-1} \cdot (xh_2)$ are by this $h_1 = h_2$, $\lightning$.

G is the union of all cosets xH with $x \in G$, because $x = x \cdot 1 \in xH$ for every $x \in G$ as $1 \in H$.

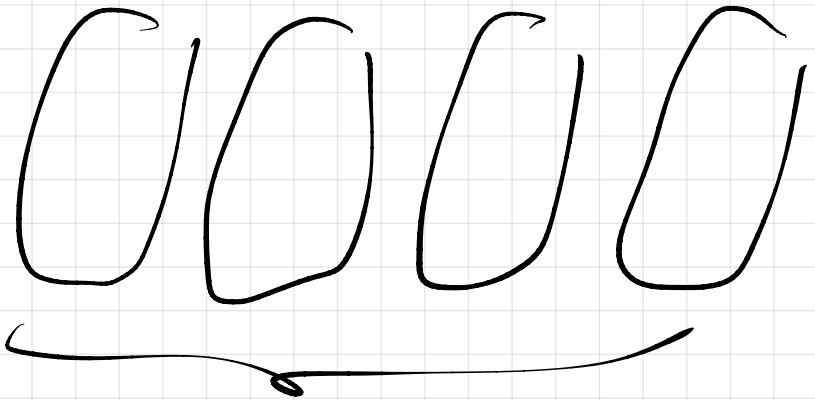
We show that the cosets partition G, which means that when aH and bH $(a, b \in G)$ have a common element, they coincide: $aH = bH$.

Let $x \in aH \cap bH$ be a common element. Then $x = a \cdot h_1 = b \cdot h_2$ for some $h_1, h_2 \in H$. It follows that every element $a \cdot h$ ($h \in H$) of aH also belongs to bH: $a \cdot h = a \cdot h_1 \cdot h_1^{-1} \cdot h = \underbrace{b \cdot h_2 \cdot h_1^{-1} \cdot h}_{\in H} \in bH$.

We have shown: $a \cdot H \subseteq b \cdot H$

Analogously, one can also show $b \cdot H \subseteq a \cdot H$.

$\Rightarrow a \cdot H = b \cdot H$

$G =$ 

cosets, each having $|H|$ elements.

$\Rightarrow |G| = (\text{Number of cosets}) \cdot |H| \Rightarrow |G|$ divisible by $|H|$. ∎

Corollary 18 Let $(G, \cdot)$ be a finite group and $g \in G$ an element of order $n \in \mathbb{N}$ in $(G, \cdot)$. Then $|G|$ is divisible by n.

Proof: $\langle g \rangle = \{g^0, g^1, \dots, g^{n-1}\}$ is known to be a subgroup of G with exactly n elements, so that Theorem 17 can be applied. □

Proposition 19 Let p be a safe prime ($p > 5$). Then, the group $(\mathbb{Z}_p \setminus \{0\}, \cdot)$ has exactly one element of order 1, which is $[1]$ and exactly one element of order 2, which is $[p-1]$. All the remaining elements $[2], \dots, [p-2]$ have orders $\frac{p-1}{2}$ or $p-1$.

Furthermore, for each $x \in \{[2], \dots, [p-2]\}$

one either has $x^{\frac{p-1}{2}} = [1]$, $\operatorname{ord}(x) = \frac{p-1}{2}$,
$\operatorname{ord}(-x) = p-1$ or $x^{\frac{p-1}{2}} = -[1]$, $\operatorname{ord}(x) = p-1$,
$\operatorname{ord}(-x) = \frac{p-1}{2}$.

Proof: An element $x \in \mathbb{Z}_p[\log]$ of order 1 satisfies
$x^1 = 1$. So, it can only be 1.

An element $x \in \mathbb{Z}_p[\log]$ of order 2 satisfies

$x^2 = 1 \Rightarrow x^2 - 1 = 0 \Rightarrow (x-1)\cdot(x+1) = 0$

$\Rightarrow x-1 = 0$ or $x+1 = 0 \Rightarrow$

$\mathbb{Z}_p$ field

$x = 1$ or $x = -1 = [p-1]$

$\Rightarrow -1 = [p-1]$ is the only element of order 2

Now, we take a look at the remaining elements.

For every $x \in \mathbb{Z}_p \setminus \{0\}$ we have $x^{p-1} = 1$

by Fermat's little theorem $\Rightarrow$

$$x^{p-1} - 1 = 0 \Rightarrow \left(x^{\frac{p-1}{2}} - 1\right) \cdot \left(x^{\frac{p-1}{2}} + 1\right) = 0$$

$$\Rightarrow \quad x^{\frac{p-1}{2}} - 1 = 0 \quad \text{or} \quad x^{\frac{p-1}{2}} + 1 = 0$$

$\mathbb{Z}_p$ field

$$\Rightarrow \quad x^{\frac{p-1}{2}} \text{ is } -1 \text{ or } 1 \text{ in } \mathbb{Z}_p.$$

So, if $x^{\frac{p-1}{2}} = 1$ and $x \in \{[2], \dots, [p-2]\}$

then $\operatorname{ord}(x) = \frac{p-1}{2}$ (since by Lagrange

and view of the fact that p is a safe prime,

the possible orders are $1, 2, \frac{p-1}{2}$ or $p-1$).

But if $x^{\frac{p-1}{2}} = 1$, then

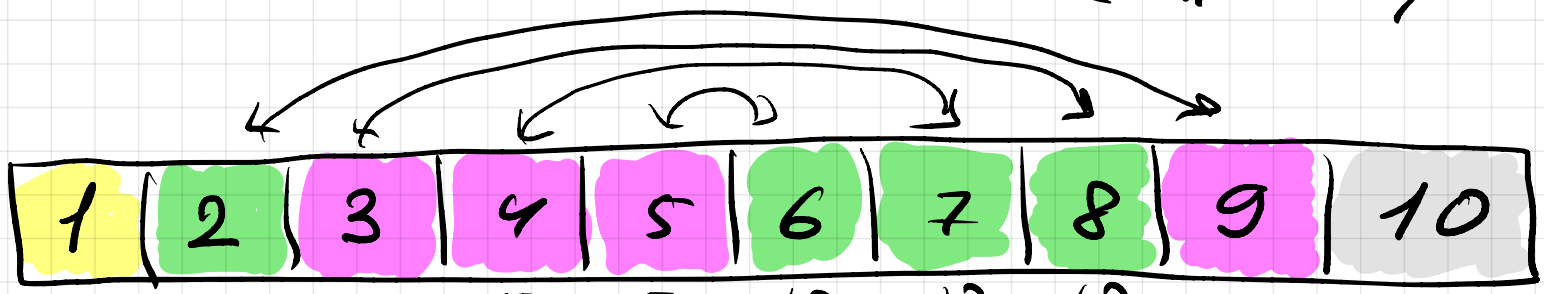
$$(-x)^{\frac{p-1}{2}} = (-1)^{\frac{p-1}{2}} \cdot x^{\frac{p-1}{2}} = -x^{\frac{p-1}{2}} = -1$$

$\frac{p-1}{2}$ odd, since p is a safe prime with $p > 5$

Hence, the order of $-x$ is $p-1$ (as there are no other options.)

Completely analogously, if $x^{\frac{p-1}{2}} = -1$, then $\operatorname{ord}(x) = p-1$ and $\operatorname{ord}(-x) = \frac{p-1}{2}$. □

Example orders of elements in $(\mathbb{Z}_{11}\setminus\{0\}, \cdot)$.



Orders: 1 10 5 5 5 10 10 10 5 2

$2 \to 4 \to 8 \to 5 \to 10 \to 9 \to 7 \to 3 \to 6 \to 1$

$\|\|\|$ $\|\|\|$ $\|\|\|$ $\|\|\|$ $\|\|\|$

-1 -2 -4 -8 -5

powers of 2 modulo 11, -1 in the middle of the 10-element sequence

$9 \equiv -2 \to 4 \to -8 \to 5 \to -10 \equiv 1$

powers of -2, $(-2)^5 \equiv -2^5 \equiv 1$ as the 5th power

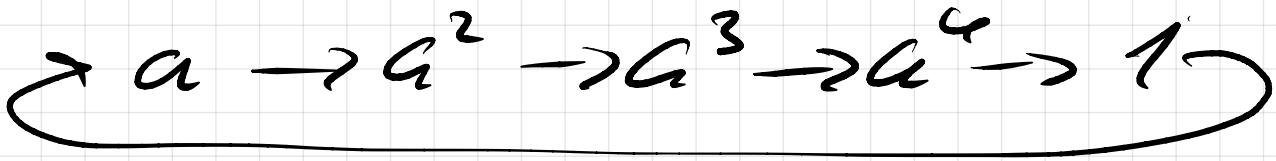
$3 \to 9 \to 5 \to 4 \to 1$

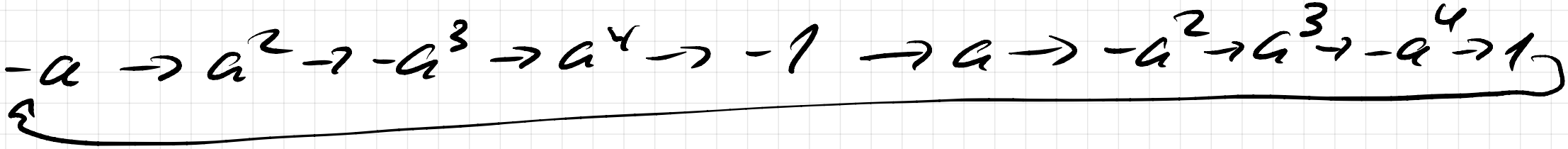
$8 \equiv -3 \to 9 \to -5 \to 4 \to -1 \to 3 \to -9 \to 5 \to -4 \to 1$

$4 \to 5 \to 9 \to 3 \to 1$

$7 \equiv -4 \to 5 \to -9 \to 3 \to -1 \to 4 \to -5 \to 9 \to -3 \to 1$

$5 \to 3 \to 4 \to 9 \to 1$





1.7. Solving the discrete logarithm problem

We have an element g of order $n \in \mathbb{N}$ in a group $(G, \cdot)$ and some $h \in \langle g \rangle$ and want to determine $i = 0, \dots, n-1$ such that $g^i = h$.

g, h known, i unknown.

A naive method: walk through the cycle $\langle g \rangle$ until you hit h, counting steps you made.

```
i := 0
p := 1
while p ≠ h:
        p := p · g
        i := i + 1
return i
```

At most $n-1$ group operations, and it can be that bad.

Can we go a little bit down from order n to some lower order of magnitude.

Here is an algorithm: Baby-step giant-step algorithm of Shanks

Let $m := \lceil \sqrt{n} \rceil$ i.e. rounding up.

i gets represented as

$i = s + t \cdot m$ with $s = 0, \dots, m-1$ and $t = 0, \dots, m-1$

in view of the long division.

So our equation $g^i = h$ gets replaced by the equation $g^{s+t\cdot m} = h$ in the unknown $s, t = 0, \dots, m-1$. It means that our new equation is:

$$g^s = h \cdot (g^m)^{-t}$$

We will need the power of g: $g^0, g^1, \dots, g^{m-1}$

(going from g^0 to g^1 to g^2 etc. is doing baby steps)

and we will need the powers of g^m

$(g^m)^0, \ldots, (g^m)^{m-1}$ (going through this sequence is doing giant steps).

We can store pairs

$(h \cdot (g^m)^{-t}, t)$ for

$t = 0, \ldots, m-1$ as key-value pairs in a dictionary so that a value can be found for a given key quite quickly (one can use hash tables or various kinds of search trees for that purpose).

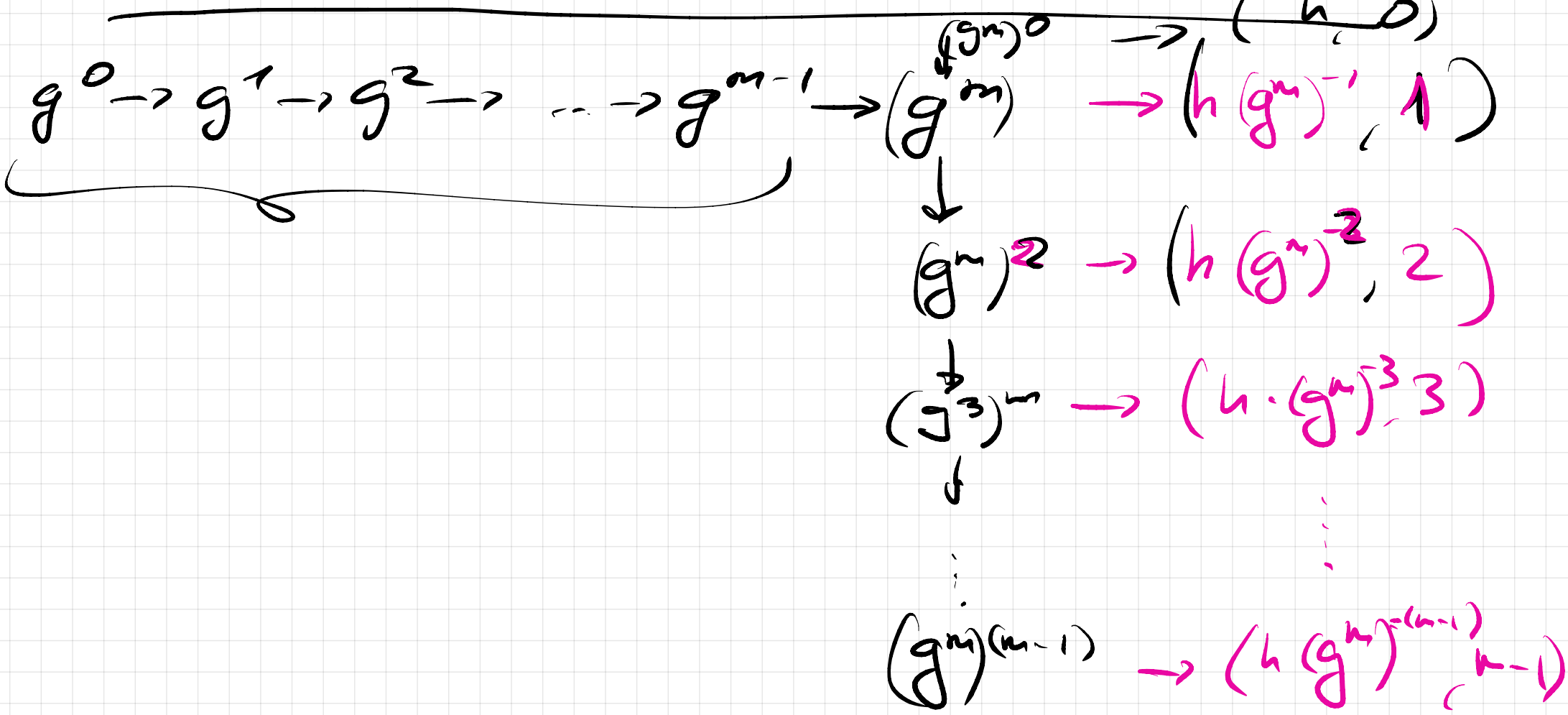
After this we iterate over g^s with $s = 0, \ldots, m-1$ and check if g^s is a key in our dictionary.

Once g^s is found in the dictionary

the value t in the key value pair

$(h \cdot (g^m)^{-t}, t)$ when was found, gives

the $i = s + tm$, we are looking for.



This algorithm takes about $\sqrt{n}$ group operations.

Order $\sqrt{n}$.

Example $(G, \cdot) = (\mathbb{Z}_{11}^{*}, \cdot)$

$g = [6]$ $\quad h = [2]$

We are solving $g^i = h$ in the unknown

$i = 0, \ldots, 10$ $\quad n = 10$ $\quad m = \lceil \sqrt{n} \rceil = 4$

$i = s + 4 \cdot t$ $\quad s, t = 0, 1, 2, 3$

Baby steps $\quad g^0 = [1]$ $(s=0)$ $\quad g^1 = [6]$ $(s=1)$ $\quad g^2 = [3]$ $(s=2)$ $\quad g^3 = [7]$ $(s=3)$

$g^0 = [1]$ $(t=0)$ $\quad g^4 = [9]$ $(t=1)$ $\quad g^8 = [4]$ $(t=2)$ $\quad g^{12} = [3]$ $(t=3)$

$g^0 = [1]$ $g^{-4} = [5]$ $g^{-8} = [3]$ $g^{-12} = [4]$

$hg^0 = [2]$ $hg^{-4} = [10]$ $hg^{-8} = [6]$ $hg^{-12} = [8]$

s	g^s
0	1
1	6
2	3
3	7

t	$h \cdot g^{-4t}$
0	2
1	10
2	6
3	8

$$g^1 = h \cdot g^{-4 \cdot 2}$$

$$g^{1+4 \cdot 2} = h$$

$$i = 9 = \underset{\text{"s}}{1} + \underset{\text{"t}}{4 \cdot 2}$$

$$i = s + mt$$

$$g^i = h$$

$$g^{s+mt} = h$$

$$g^s = h \cdot (g^{-m})^t$$

2 Symmetric cryptography

Alice and Bob have the role
(that's why symmetric)
they share a private key k have access
to an encryption method e_k and
and a decryption method d_k and both can
use them.

Encryption and decryption functions need to operate on some domain, which is usually chosen to be a finite algebraic structure. A finite field is a good choice. And we already know some finite fields:

$(\mathbb{Z}_p, +, \cdot)$ where p is a prime number.

But we don't know all finite fields. It's worth finding all finite fields.

2.1. Fields and finite fields

Assume that you know some field K and you want to create a larger field F out of K. You can do it using polynomials.

Def. Let t be a formal variable (a symbol).

And K be a field. By $K[t]$ we denote the set of formal expressions of the form

$$f = \sum_i a_i t^i$$ where i runs over $\mathbb{N}_0$,

$a_i \in K$ and the set

$$\operatorname{supp} f := \{ i \in \mathbb{N}_0 : a_i \neq 0 \}$$ is finite

($\operatorname{supp} f$ is called the support of f)

Elements of $K[t]$ are called polynomials in the variable t with coefficients in K.

$d = \deg(f) = \max(\operatorname{supp}(f))$ is called the degree of f. If $\operatorname{supp}(f) = \emptyset$, $d = -\infty$.

a_i are called the coefficients of f

$a_i t^i$ is called the term of degree i

t^i is called the monomial of degree i

Ex $\mathbb{Q}[t]$

$$f = \frac{3}{2} + 5 \cdot t - \frac{1}{2} t^{10} = \frac{3}{2} \cdot t^0 + 5 \cdot t^1 - \frac{1}{2} t^{10}$$

$\operatorname{supp}(f) = \{0, 1, 10\}$ $\quad t^0, t^1, t^{10}$

$\max(\operatorname{supp}(f)) = 10$

$\operatorname{supp}(0) = \emptyset$

$\deg(0) = \max \emptyset = -\infty.$

$\operatorname{supp}(1) = \{0\}$

$\operatorname{supp}(2) = \{0\}$

$\operatorname{supp}(t^{100}) = \{100\}$

$$\operatorname{supp}(1) = \operatorname{supp}(1 \cdot t^0) = \{0\}$$

$$\operatorname{supp}(5) = \operatorname{supp}(5 \cdot t^0) = \{0\}$$

$$\operatorname{supp}(5+t) = \operatorname{supp}(5 \cdot t^0 + 1 \cdot t^1) = \{0,1\}$$

Def. We introduce $+$ and $\cdot$ in $K[t]$ by the following rules:

$$\sum_i a_i t^i + \sum_i b_i t^i := \sum_i (a_i + b_i) t^i$$

$$\left(\sum_i a_i t^i\right) \cdot \left(\sum_j b_j t^j\right) := \sum_{i,j} a_i b_j t^{i+j}$$