Algebra - MATH310

Jacopo “quartztz” Moretti

January 2024

Preface

Helo! I'm Jack :3.

I'm a student that needs zto type out courses in order to make sure they properly understand them. So I put them out into the world! They might help you more than they help me :D. They are given as they are, with no guarantee of quality but guarantee of goodwill, bla bla bla. You know the gist of it.

Elements of notation

The group operation for a group G will usually be denoted $\cdot_G$, and its neutral element will be e_G. The index will be removed when it can be inferred from context.

For now, I'll denote $\mathbf{n} = \{1, ..., n\}$, because it's clunky to type and it's my notes, goddamnit. I might change it back at the end.

Contents

1 Introduction **3**

2 Primes **4**
2.1 Divisors and primes 4
2.2 Integer arithmetic 5

3 Groups **7**
3.1 Base definitions 7
3.1.1 Groups and cosets 7
3.1.2 RSA and back to primes 9
3.2 Homomorphisms 10
3.2.1 When the morphism is homo D: 10
3.2.2 Generators and Relations 11
3.3 Weirder groups 14
3.4 Actions of groups on sets 19
3.4.1 Orbits and stabilizers 19

A Proofs from exercise sets **22**
A.1 Theorem 1.1 22
A.2 Theorem 2.4 22
A.3 Theorem 2.4 22
A.4 Theorem 3.4.1 23

B Elliptic curves **24**
Elliptic curves 24

Chapter 1

Introduction

Week 1

Algebra rests on 3 basic principles, which are equivalent in nature.

1. **Induction:** Let $S \subset \mathbb{N}$ such that $0 \in S$ and $n \in S \Rightarrow n+1 \in S$. Then, $S = \mathbb{N}$.
2. **Well-ordering principle:** For any non-empty $A \subset \mathbb{N}$, there exists an element a : $\forall b \in A, a \leqslant b$.
3. **Strong induction:** Let $S \subset \mathbb{N}$ such that $0 \in S$ and $\{0, ..., n\} \in S \Rightarrow n+1 \in S$. Then, $S = \mathbb{N}$.

It is well-established that these three principles are equivalent. Let us prove it.

Theorem 1.1. ***I*** $\Rightarrow$ ***WOP*** $\Rightarrow$ ***SI*** $\Rightarrow$ ***I***.

Proof. We will prove each induction separately.

1. 1. $\Rightarrow$ 3. Let S be the construction from the strong induction definition, and let us consider $P(n) = \{0, 1, ..., n\} \subset S$. We can prove it by induction:

   Base: $0 \in S$ by construction $\Rightarrow \{0\} \subset S$.
   Induction: Let us prove that $P(k) \Rightarrow P(k+1)$ for some k.

   $$\begin{aligned} \{0, 1, ..., k\} \subset S \text{ [by IH]} &\Rightarrow k \in S && \text{[by construction]} \\ &\Rightarrow k+1 \in S && \text{[by definition]} \\ &\Rightarrow \{0, 1, ..., k, k+1\} \in S \end{aligned}$$

   Since it is hereditary and true for 0, it is true $\forall n \in \mathbb{N}$ by the induction principle.

   Since $\{0, 1, ..., n\} \subset \mathbb{N}\ \forall n$, then $S = \mathbb{N}$.

2. $2 \Rightarrow 1$. Suppose $S \subset \mathbb{N}$ such that $0 \in S$ and $n \in S \Rightarrow n+1 \in S$. Consider $S' = \mathbb{N} \setminus S$, which we assume to be nonempty by absurd. By the well-ordering principle, we can pick a least element in $k \in S'$, which is by definition not in S. k cannot be zero, since $0 \in S$ by definition, but it can also not be non-zero, since $k \neq 0 \Rightarrow k = m+1$ for some $m < k$ (therefore not in S'). $m \in S$, so by construction, $m+1 = k \in S$ as well, which is a contradiction. S' has to be empty, so $S = \mathbb{N}$.
3. $3 \Rightarrow 2$. Done in a Problem Set, found in appendix A.

□

Chapter 2

Primes

2.1 Divisors and primes

Definition 2.1. *Let* $a, b \in \mathbb{Z}$. *We say that* a *divides* b *(notate:* $a|b$*) if there exists* $k \in \mathbb{Z}$ *such that* $b = ka$.

Definition 2.2. *A number* $p \in \mathbb{Z}$ *is prime if* $p > 1$ *and the only numbers that divide it are itself and 1.*

Theorem 2.3. *Any* $n > 1$ *has a prime divisor.*

Proof. Let $S = \{n \in \mathbb{N} : n > 1 \wedge n \text{ has no prime divisors}\}$. We suppose S to be nonempty, meaning it contains a least element $k \in S$. k cannot be prime, since $k|k\ \forall k$. Therefore, it has to be true that $k = ab$ for $a, b < k \in \mathbb{N}$. Since k was the lest element, then, $a \notin S$, meaning that there exists a prime p such that $a = pt$ for $tin\mathbb{N}$. Therefore, $k = ab = ptb \Rightarrow p|k$, contradicting our construction of S. Therefore, S must be empty. $\square$

Theorem 2.4. *Any* $n > 1$ *can be expressed by the product of primes.*

> This proof was done in an exercise set, and can be found in the appendix.

Theorem 2.5. *The prime number factorization of a number is unique.*

Proof. Let $k = \prod^n p_i = \prod^m q_j$ two distinct prime sets. Suppose without loss of generality that $q_1 > p_1$ and let $t = (q_1 - p_1)q_2...q_m > 0$. Then:

$$\begin{aligned} t &= (q_1 - p_1)q_2...q_m \\ &= q_1q_2...q_m - p_1q_2...q_m \\ &= k - p_1q_2...q_m > 0 \Rightarrow p_1|t \end{aligned}$$

We know that $p_1 \neq q_j$ for all j, so we focus on the only "weird" term:

$$\begin{aligned} (q_1 - p_1) &= sp_1 \\ \Rightarrow q_1 &= (s+1)p_1 \end{aligned}$$

Which is a contradiction because q_1 is supposed to be prime. Therefore, the prime factorization is unique. $\square$

2.2 Integer arithmetic

Definition 2.6 (Euclidian division)**.** *Let $n \in \mathbb{Z}, d \in \mathbb{Z}^*$. There exists a unique pair $q, r \in \mathbb{Z}$ such that $n = qd + r$ with $0 < r < d$.*

Proof. **Existence.** Consider the set

$$S = \{n - kd\}_{k \in \mathbb{Z}} \cap \mathbb{N} = \{n - kd, kd \leqslant n\}_{k \in \mathbb{Z}}$$

We know that S is not empty, because:

▷ if $n >= 0$, then we set $k = 0$, meaning $n \in S$

▷ if $n < 0$, then we set $k = |n| + 1$, meaning $kd > |n|$ and $n + kd \in S$.

Since it's never empty, we can pick the least element of S by means of the well-ordering principle. Let's call it r. Therefore, we have $r = n - kd$ for some k. To prove $r < d$, we assume towards absurdity that $r >= d$, meaning that

$$n - (k+1)d = n - kd - d = r - d >= 0$$

meaning r wasn't minimal, which is a contradiction.

Uniqueness. Suppose $n = q_1 d + r_1 = q_2 d + r_2$. Without loss of generality, assume $q_1 > q_2$. Then:

$$(q_1 - q_2)d + r_1 = r_2 \geqslant d$$

Since r_1 and $q_1 - q_2$ are positive. This contradicts the definition of r_2, and is therefore absurd. □

Definition 2.7. *Let $a, b \in \mathbb{Z}$. We define the greatest common divisor (*gcd*) of two numbers as*

$$\gcd(a, b) = \max\{x \in \mathbb{Z} : x|a \wedge x|b\}$$

Theorem 2.8. *For $n, q \in \mathbb{Z}, d \in \mathbb{Z}^*$, such that $n = qd + r$, it is always the case that:*

$$\gcd(n, d) = \gcd(d, r)$$

Proof. By inspection of the relationship $n = qd + r$, it's clear that if $x|n \wedge x|d$ then $x|r$, and if $x|d \wedge x|r$ then $x|n$. □

> *Method* This induces a special algorithm to compute the gcd of two numbers! Let $d_1, d_2 \in \mathbb{Z}$. Then:
>
> $$\begin{aligned} d_1 &= q_1 d_2 + d_3 \\ d_2 &= q_2 d_3 + d_4 \\ &\dots \\ d_k &= q_k d_{k+1} + 0 \end{aligned}$$
>
> The relationship $\gcd(d_{i-1}, d_i) = \gcd(d_i, d_{i+1})$ holds down the tree, meaning that by the end
>
> $$\gcd(d_1, d_2) = d_{k+1}$$
>
> Additionally, we have:

Corollary 2.9. *For any $a, b \in \mathbb{Z}^+$, there exist $x, y \in \mathbb{Z}$ such that*

$$\gcd(a, b) = xa + yb$$

This is obtained by running Euclid "up the tree".

Example 1. *TODO*

Special consequence of corollary 2.9 is the following

Corollary 2.10. *If $a, b \in \mathbb{Z}^+$ are such that $d = \gcd(a, b)$, then the equation:*

$$c = ax + by$$

has solutions (x, y) if and only if $\exists\ k > 0 : c = kd$, and they can be found as the solutions in corollary 2.9 multiplied by k.

Final consequence of these facts is the well-known Bézout's theorem.

Theorem 2.11. *Two numbers $a, b \in \mathbb{Z}^+$ are relatively prime if and only if the equation*

$$1 = ax + by$$

has integer solutions.

Definition 2.12. *For any $n \in \mathbb{Z}^+$, Euler's totient function is defined as:*

$$\varphi(n) = \left|\left\{k \in \{1, ..., n\} : \gcd(k, n) = 1\right\}\right|$$

meaning the number of positive integers less than n that are coprime to it.

Properties Properties of the totient function include:

- $\varphi(p) = p - 1$ for any prime p.
- $\varphi(pq) = (p - 1)(q - 1)$ for any pair of distinct primes p, q.
- More generally, $\varphi(mn) = \varphi(m)\varphi(n)$ for any m, n coprime.

Chapter 3

Groups

Week 2

3.1 Base definitions

3.1.1 Groups and cosets

Definition 3.1. *A group is a set G with a binary operation $\cdot : G \times G \to G$, satisfying the following axioms:*

- $\cdot$ *is associative:* $(a \cdot b) \cdot c = a \cdot (b \cdot c)$
- *There exists a neutral element e such that $a \cdot e = e \cdot a = a \; \forall a \in G$.*
- *For any $a \in G$ there exists an inverse a^{-1} such that $a^{-1} \cdot a = a \cdot a^{-1} = e$.*

We say that G is a finite group if $|G| < \infty$. In that case, we say that G is of order $|G|$. We say that G is abelian (or commutative) if $a \cdot b = b \cdot a \; \forall a, b \in G$.

Definition 3.2. *$H \subset G$ is a subgroup if it contains the neutral element e_G and if it is closed with respect to $\cdot_G$, meaning that for every $a, b \in H$, $a \cdot b \in H$, and to inverses.*

We can note that any group has a subgroup generated by a single element:

$$\langle g \rangle = \{e, g^1, g^2, \ldots, g^{-1}, g^{-2}, \ldots\}$$

Since $g^i \cdot g^j = g^{i+j}$ by definition of the group operation, this set is closed under it, meaning it is a subgroup.

Definition 3.3. *If it exists, the minimal $n \in \mathbb{N}^*$ such that $g^n = e$ is called the order of g. It is finite for every element in a finite group.*

Definition 3.4. *Let $H \subset G$ be a subgroup of G. The left coset of g with respect to H, denoted gH, is the following set:*

$$gH = \{gh, h \in H\}$$

Theorem 3.5. *Let $H \subset G$ finite. Then:*

1. *Two left-cosets xH, yH are either disjoint ($xH \cap yH = \varnothing$) or equal.*

2. *For any element* $g \in G$ *there exists a left coset of* H *such that* $g \in H$.

3. $|xH| = |H| \; \forall x \in G$

Proof. We will prove each part separately:

1. Suppose xH, yH are such that $xH \cap yH \neq \varnothing$. This means that there exist h_1, h_2 such that $xh_1 = yh_2$. Therefore,

$$x = yh_2h_1^{-1} = yh_3 \in yH \Rightarrow xh = yh_3h \; \forall h \in H$$

This means that if there exists an element of xH that is in yH, then every element in xH can be written as an element in yH, meaning they are equal.

2. For any $g \in G$, one can construct $gH = \{e, g, g^2, ...\}$, which naturally contains g.

3. The mapping

$$\begin{aligned} f(h) : H &\to xH \\ h &\mapsto xh \end{aligned}$$

is surjective, by definition of $xH = \{xh, h \in H\}$, and it is also injective, since $xh_1 = yh_2 \Leftrightarrow h_1 = h_2$. This means it defines a bijection between H and xH, indicating they have the same cardinality.

> *Example* Let $G = (\mathbb{Z}, +, 0), H = 3\mathbb{Z} \subset \mathbb{Z}$. The left coset of 0 with respect to H is :
> $$\{0 + 3k\}_{k\in\mathbb{Z}} = H = \{3 + 3k\}_{k\in\mathbb{Z}}$$
> The left coset of 1 is
> $$\{1 + 3k\}_{k\in\mathbb{Z}} = \{1, 4, 7, -2, ...\}$$

□

Theorem 3.6 (Lagrange's theorem)**.** *Let* G *be a finite group,* $H \subset G$ *a subgroup. Then,* $|H|$ *divides* $|G|$.

Proof. Each $g \in G$ belongs to a left coset of H, which are either disjoint or equal. This means:

$$\begin{aligned} G &= \bigcup_{i=0}^{r} x_iH && \text{[disjoint union of finite \# of sets]} \\ \Rightarrow |G| &= \sum_{i=0}^{r} |x_iH| \\ \Rightarrow |G| &= \sum_{i=0}^{r} |H| && \text{[since } |xH| = |H|\text{]} \\ \Rightarrow |G| &= r|H| \end{aligned}$$

with $r \in \mathbb{N}$, meaning that $|H|$ divides $|G|$. □

Definition 3.7. *The number of left cosets of H of G is called the index of G:*

$$[G : H] = |G|/|H| \in \mathbb{N}^*$$

This means that the order of any element $g \in G$ (notated $\mathrm{ord}(g)$) divides the order of the group $|G|$, since every element generates a subgroup $\langle g \rangle$. Additionally, it implies

Corollary 3.8. $g^{|G|} = (g^{\mathrm{ord}(g)})^k = e^k = e$ *for some* k*.*

3.1.2 RSA and back to primes

Theorem 3.9 (Euler's theorem)**.** *Let $a, n \in \mathbb{Z}^+$. such that* $\gcd(a, n) = 1$*. Then,*

$$a^{\varphi(n)} \equiv 1 \mod n$$

Proof. Consider $G = (\mathbb{Z}/n\mathbb{Z}, \cdot, 1)$. Then,

$$a^{\varphi(n)} = a^{|G|} \overset{3.8}{=} 1$$

□

Theorem 3.10 (Fermat's little theorem)**.** *Let $a \in \mathbb{Z}^+$, p prime such that p does not divide a. Then, $a^{p-1} = 1$.*

Proof. Consider $G = (\mathbb{Z}/p\mathbb{Z}, \cdot, 1)$. Then, $|G| = \varphi(p) = p - 1$. By Euler's theorem,

$$a^{\varphi(p)} = a^{(p-1)} = 1$$

□

> *RSA* The RSA cryptosystem for message transmission works as follows:
>
> 1. Choose two distinct large primes p, q.
> 2. Compute $m = pq \Rightarrow \varphi(m) = (p - 1)(q - 1)$.
> 3. Choose $e \leqslant m$ an encryption key such that $\gcd(e, \varphi(m)) = 1$.
> 4. Use Euclid's algorithm to determine d such that $ed - k\varphi(m) = 1$ for some integer k.
> 5. The encoding key is the pair (m, e), and it can be published. To decode, you use the decoding key (m, d) which is to be kept private.
>
> To send a message x to someone, you need their public pair (m, e). You first compute $c \equiv x^e \bmod m$, which can be sent publicly. To decode, the person will use their private pair (m, d), computing $x \equiv c^d \bmod m \equiv x^{ed} \bmod m$.

Why is it the case that $x^{ed} \equiv x \bmod m$? Well... Week 3

Theorem 3.11. *Let p, q be two distinct primes, and $m = pq$. Let $e : \gcd(e, \varphi(m)) = 1$, and let $d \in \mathbb{Z} : ed - k\varphi(m) = 1$ for some $k \in \mathbb{Z}$. Then,*

$$x^{ed} \equiv x \bmod m$$

for all $x \in \mathbf{m}\}$*.*

Proof. If $x = pt$ for some t, then trivially $x \equiv x^{ed} \equiv 0 \bmod p$. If x is not divisible by p, then we can rewrite

$$x^{ed} = x^{k\varphi(m)+1}$$

By Fermat's theorem, we know that $x^{p-1} \equiv 1 \bmod p$, meaning:

$$x^{k\varphi(m)} = x^{k(p-1)(q-1)} = \left(x^{p-1}\right)^{k(q-1)} \equiv 1^{k(q-1)} \equiv 1 \bmod p \Rightarrow x^{k\varphi(m)+1} \equiv x \bmod p$$

Meaning in both cases $x^{ed} \equiv x \bmod p$. By a symmetric argument, the same is true $\bmod q$, allowing us to conclude

$$\begin{aligned} x^{ed} - x &\equiv 0 \bmod pq \\ &\equiv 0 \bmod m \\ \therefore x^{ed} &\equiv x \bmod m \end{aligned}$$

□

> *RSA* As a quick example, let's consider an RSA system with the following characteristics:
>
> $$p = 3, q = 11 \Rightarrow m = pq = 33, \varphi(m) = (p-1)(q-1) = 20$$
>
> We choose $e = 7$ which is coprime with $\varphi(m)$. We compute d:
>
> $$\begin{aligned} 20 &= 7 \cdot 2 + 6 \\ 7 &= 6 \cdot 1 + 1 \\ \Rightarrow 1 &= 7 - 6 \cdot 1 \\ &= 7 - (20 - 7 \cdot 2) \cdot 1 \\ &= \underbrace{7}_{e} \cdot \underbrace{3}_{d} - \underbrace{20}_{\varphi(m)} \end{aligned}$$

3.2 Homomorphisms

3.2.1 When the morphism is homo D:

> *Examples* Recall a few examples of groups:
>
> 1. $\mathbb{Z}/n\mathbb{Z} = \{[0], [1], ..., [n-1]\}$ with regular modular addition and 0 as the neutral element.
> 2. $(\mathbb{Z}/n\mathbb{Z})^* = \{a \in \mathbb{Z}/n\mathbb{Z} : \gcd(a, n) = 1\}$ with modular multiplication and 1 as the neutral element. This is a group because
>
> $$\begin{aligned} \gcd(a, n) = 1 &\Leftrightarrow \exists x, y \in \mathbb{Z} : ax + ny = 1 \\ &\Rightarrow [a] \cdot [n] = [1] \bmod n \end{aligned}$$
>
> These are two abelian!

3. The n-th complex roots of unity!

$$\sqrt[n]{1} = \{e^{\frac{2\pi k i}{n}}, k = 0, ..., n-1\}$$

If you define $q = e^{i\frac{2\pi}{n}}$, then the group can be defined as the generated group:

$$\sqrt[n]{1} = \langle q \rangle = \{1, q, q^2, ..., q^{n-1}\} \overset{not.}{=} C_n$$

C_n is defined as the cyclic group of order n, and it's easy to convince yourself of the fact that $(C_n, \cdot, 1)$ is "the same" as $(\mathbb{Z}/n\mathbb{Z}, +, 0)$, in the sense that they have similar enough structure that you could map one onto the other and back.

Definition 3.12. *A map $\phi : G \to H$ between two groups is said to be a group homomorphism if*

$$\phi(x \cdot_G y) = \phi(x) \cdot_H \phi(y) \ \forall x, y \in G$$

This formally defines the "structure-maintaining" constraint on ϕ, and it also implies that $\phi(e_G) = e_H$ and $\phi(x^{-1}) = \phi(x)^{-1}$

Definition 3.13. *A group homomorphism that can be inverted to a group homomorphism is called a group isomorphism. If $\phi : G \to H, \psi : H \to G$ are two group homomorphisms such that $\phi \circ \psi = \mathrm{Id}_H, \psi \circ \phi = \mathrm{Id}_G$, then G and H are said to be isomorphic groups (denoted $G \simeq H$).*

Definition 3.14. *A group automorphism is a group isomorphism from a group onto itself $\phi : G \to G$.*

Example The map

$$\begin{aligned} \phi : C_n &\to \mathbb{Z}/n\mathbb{Z} \\ q^i &\mapsto [i] \end{aligned}$$

is a bijection, with inverse

$$\begin{aligned} \phi^{-1} : \mathbb{Z}/n\mathbb{Z} &\to C_n \\ [i] &\mapsto q^i \end{aligned}$$

and it respects the bounds on the group operations:

$$\phi(q^i \cdot q^j) = \phi(q^{i+j}) = [i+j]$$
$$\phi(q^i) \cdot \phi(q^j) = [i] + [j] = [i+j]$$

meaning that $C_n \simeq \mathbb{Z}/n\mathbb{Z}$.

3.2.2 Generators and Relations

We've seen that groups can be represented as a set of elements coupled with a binary operation on those elements. However, we can define another representation of a group, based on generators and relations:

Definition 3.15. *The set of generators of a group G is the minimal subset of elements of G such that any element of G can be written as a product of generators and their inverses.*

Definition 3.16. *A relation is an equation that is satisfied by every element of a group.*

Definition 3.17. *A presentation of a group G in generators and relations is an expression of the form :*

$$G = \langle S | R \rangle$$

With S a set of generators, and R a set of relations on elements of S, such that any other relation on G follows from them.

> *Example* For example, the cyclic group of order n, C_n, is generated by q, since every element can be written as q^k for some $0 < k < n$. Additionally, the relation $q^n = 1$ holds on q. This means that we can write:
>
> $$C_n = \{1, q^1, ..., q^{n-1}\} = \langle q | q^n = 1 \rangle$$

This representation allows us to define group homomorphisms in an easier way:

Proposition. *Let $G = \langle S | R_1 = 1, ..., R_k = 1 \rangle$, let H a group. We define a mapping $\phi : G \to H$ as follows:*

a) $\phi(s) \in H$ for every generator $s \in S$.

b) $\phi(x_1 \cdot_G x_2) = \phi(x_1) \cdot_H \phi(x_2)$ for any $x_1, x_2 \in G$.

Then, ϕ is a group homomorphism if and only if $R_1, ..., R_k$ are satisfied for any $\phi(s)$.

Week 4

Definition 3.18. *Let $\phi : G \to H$ a group homomorphism. The kernel of a group homomorphism is the set*

$$\ker \phi = \{g \in G : \phi(g) = e_H\} \subset G$$

Proposition. *Let $\phi : G \to H$ a group homomorphism. The kernel of ϕ is a subgroup of G.*

Proof. Let $a, b \in \ker \phi$. Then:

- ▷ $\phi(e_G) = e_H$ by definition of a group homomorphism, meaning that $e_G \in \phi$.
- ▷ $\phi(a \cdot b) = \phi(a) \cdot \phi(b) = e \cdot e = e$, meaning that $a, b \in \ker \phi \Rightarrow ab \in \ker \phi$.
- ▷ $\phi(a^{-1}) = (\phi(a))^{-1} = e^{-1} = e$, meaning that $a \in \ker \phi \Rightarrow a^{-1} \in \ker \phi$.

These three properties mean that $\ker \phi$ is a subgroup of G. □

Definition 3.19. *Let $\phi : G \to H$ a group homomorphism. The image of ϕ is the set $\phi(G) \subset H$.*

Proposition. *Let $\phi : G \to H$ a group homomorphism. The image $\phi(G) = \{\phi(g)\}_{g \in G} \subset H$ is a subgroup in H.*

Proof. Let $h_1, h_2 \in \phi(G)$. Then

- ▷ $\phi(e_G) = e_H$ by definition of a group homomorphism, meaning $e_h \in \phi(G)$.
- ▷ $h_1 h_2 = \phi(g_1) \cdot \phi(g_2) = \phi(g_1 g_2)$ for some $g_1, g_2 \in G$, meaning $h_1 h_2 \in \phi(G)$.
- ▷ $h_1^{-1} = \phi(g_1)^{-1} = \phi(g_1^{-1})$, meaning $h_1^{-1} \in \phi(G)$,

This means $\phi(G)$ is a subgroup of H. □

Definition 3.20. *A subgroup $H \subset G$ is a normal subgroup (notated $H \triangleleft G$) if $\forall h, \forall g$, we have $ghg^{-1} \in H$.*

For any group homomorphism $\phi : G \to H$, the kernel $\ker G$ is a normal subgroup of G. If you take any $g \in G, h \in H$, then we have:

$$\phi(ghg^{-1}) = \phi(g)\phi(h)\phi(g^{-1}) = \phi(g)(\phi(g))^{-1} = e$$

meaning that $ghg^{-1} \in \ker G$ as well.

Definition 3.21. *The group of rigid symmetries of a flat regular n-gon is called the dihedral group of order n, and it is denoted D_n.*

> *About symmetries* It is generated by a single rotation counterclockwise, leaving the shape self-similar but with vertices "shifted" by one to the left, and one "mirroring" of the shape per axis of symmetry.
>
> For example, for a square, we have: TODO: ADD IMAGE
>
> $$D_4 = \{1, r, r^2, r^3, r^4, s_1, s_2, s_3, s_4\}$$
>
> with r a counterclockwise rotation and s_i a reflection across the i-th axis. The group operation is concatenation of action: it's easy to see how two consecutive rotations r might yield a double rotation ($r \cdot r = r^2$) and how concatenating a rotation and a symmetry can be defined as rs_i
>
> This is group is not commutative: take a piece of paper, draw a labelled square, and you'll soon convince yourself of the fact that $rs \neq sr$, i.e. that a rotation followed by a mirroring does not yield the same result as the same mirroring followed by the same rotation.
>
> In general, $|D_n| = 2n$: due to the nature of our moves, if after a move we have n "free" spots where vertex 1 could have ended up, after we choose that one, there's only two spots for vertex 2 (either right before or right after it) before defining a full state for the figure. This means $|D_n| \leqslant 2n$, and since we can lay out $2n$ elements, then $|D_n| = 2n$.
>
> Playing around with the polygon shows the evident relation $srs = r^{-1}$, equivalent to $(sr)^2 = 1$. With this, we can write:
>
> $$\begin{aligned} D_n &= \langle r, s | r^n = 1, s^2 = 1, srs = r^{-1} \rangle \\ &= \{1, r, r^2, ..., r^{n-1}, s, sr, sr^2, ..., sr^{n-1}\} \end{aligned}$$
>
> Thanks to our relations, we know that we can write any product of moves under the form $s^a r^b$ for some a, b.
>
> The two subgroups that are worth mentioning are:

- ▷ the group of rotations $R = \langle r \rangle = \{1, r, ..., r^{n-1}\}$, which defines two cosets, the coset of rotations $1R$ and the coset of all symmetries $sR = \{s, sr, ..., sr^{n-1}\}$. It is a normal subgroup, since $gr^k g^{-1} \in R$ no matter what g you use.
- ▷ the group of symmetries $K = \langle s \rangle = \{1, s\}$. This is not a normal subgroup, as $rsr^{-1} = sr^{-1}r^{-1} = sr^{-2} \notin K$.

3.3 Weirder groups

Proposition. *Let $H \lhd G$. We define the product on left cosets of H as*

$$(xH) \cdot (yH) = (xyH)$$

with eH the neutral element, and $x^{-1}H$ the inverse. This product is well-defined and it induces a group structure on the set of cosets.

Proof. We just have to check that the product does not depend on the choice of coset representatives: let $x' \in xH, y' \in yH$, let us check that $x'y' \in xyH$. We know that $x' = xh_1, y' = yh_2$ for some $h_1, h_2 \in H$. We can write:

$$x'y' = xh_1yh_2 = xy(y^{-1}h_1y)h_2 \overset{(*)}{=} xyh_3h_2 = xyh_4 \in xyH$$

where step $(*)$ is motivated by the fact that H is normal. Since $x'y' \in xyH$, the product is well defined. □

Definition 3.22. *The group of left cosets of $H \lhd G$ is called the the quotient group G/H.*

Example The cosets of $R \lhd D_n = \{1R, sR\}$ form the quotient group D_n/R, with the operations between them being the product of their representatives and the neutral element being the coset of 1 wrt R. The operations are

$$\begin{aligned}(1R)(1R) &= (1R)\\ (1R)(sR) &= (sR)\\ (sR)(1R) &= (sR)\\ (sR)(sR) &= (1R)\end{aligned}$$

This pattern seems a little familiar: this group is isomorphic to $C_2 = \langle t | t^2 = 1 \rangle$ (which are the two square roots of unity!), with the mapping function

$$\begin{aligned}\phi : R/D_n &\to C_2\\ 1R &\mapsto 1\\ sR &\mapsto t\end{aligned}$$

Proposition. *In an abelian group G, every subgroup $H \subset G$ is normal.*

This is barely a theorem, and is easily proven as $ghg^{-1} = hgg^{-1} = h \in H$ for any g. Week 5

Definition 3.23. *S_n is the group of permutations of sets of n elements* **n**.

> *Properties* A permutation is an element of S_n, for which we'll see a few different representations; the group operation is composition between two elements; the neutral element is the trivial permutation that moves no element.
>
> For an element $s \in S_n$, we denote si the index on which it sends the number $i \in \mathbf{n}$
>
> In general, $|S_n| = n^1$.

.

We introduce a new notation for elements of S_n. In the meantime, let us denote a permutation as two lists: the first is the input one, and the second is the result of applying the permutation once. On S_4, the trivial permutation would look like:

$$\begin{pmatrix} 1 & 2 & 3 & 4 \\ 1 & 2 & 3 & 4 \end{pmatrix}$$

Consider an arbitrary element $\rho \in S_n$, of order k, and construct $\langle \rho \rangle = \{1, \rho, ..., \rho^{k-1}\}$. Take $x \in \mathbf{n}$: then we can construct the orbit $\operatorname{Orb}_\rho x := \{x, \rho x, ...\}$. This orbit is unique to each x: if there were two x_1, x_2 such that their orbits aren't disjoint, there would exist i, j such that

$$\rho^i x_1 = \rho^j x_2 \Leftrightarrow \rho^{i-j} x_1 = x_2 \Rightarrow x_2 \in \operatorname{Orb}_\rho x_1$$

This implies that $\operatorname{Orb}_\rho x_2 \subset \operatorname{Orb}_\rho x_1$, and we can find $\operatorname{Orb}_\rho x_1 \subset \operatorname{Orb}_\rho x_2$ pretty symmetrically: this means $\operatorname{Orb}_\rho x_1 = \operatorname{Orb}_\rho x_2$.

Definition 3.24. *We say that $\pi \in S_n$ is a cycle if it has a single non-trivial (containing more than a single element) orbit. The length of this non-trivial orbit is said to be the length of the cycle.*

Therefore, we have that

$$\rho = \begin{pmatrix} 1 & 2 & 3 & 4 \\ 2 & 1 & 3 & 4 \end{pmatrix}$$

is a cycle because $\operatorname{Orb}_\rho 1 = \operatorname{Orb}_\rho 2 = \{1, 2\}$ is its only nontrivial orbit, but

$$\sigma = \begin{pmatrix} 1 & 2 & 3 & 4 \\ 2 & 1 & 4 & 3 \end{pmatrix}$$

isn't because it has two nontrivial orbits, $\operatorname{Orb}_\rho 1 = \operatorname{Orb}_\rho 2 = \{1, 2\}$ and $\operatorname{Orb}_\rho 3 = \operatorname{Orb}_\rho 4 = \{3, 4\}$. A cycle of length k, will be notated as such:

$$\pi \in S_n : (x, \pi(x), \pi^2(x), ..., \pi^{k-1}(x))$$

taking x an arbitrary element such that the orbit $\operatorname{Orb}_\pi x$ is nontrivial.

$$\rho = \begin{pmatrix} 1 & 2 & 3 & 4 \\ 2 & 1 & 3 & 4 \end{pmatrix}$$

would be notated as $\rho = (12)$.

This means that the cycle

$$(i_1, i_2, ..., i_k)$$

is the permutation that sends $i_1 \mapsto i_2, i_2 \mapsto i_3, ..., i_k \mapsto i_1$, and leaves every other element unchanged.

[1] This follows from CS101. I didn't pass that class, but I hear it's where we saw it first.

Proposition. *Let S_n be the group of permutations on* $\mathbf{n}$*. Then, disjoint cycles commute in S_n under composition.*

Proof. Let π_1, π_2 two disjoint cycles of nontrivial orbits O_1, O_2. This means that $O_1 \cap O_2 = \varnothing$. We are looking to prove $\pi_1\pi_2(x) = \pi_2\pi_1(x) \forall x \in \mathbf{n}$. To do that, we split the posisble cases:

1. $x \notin O_1 \cup O_2$. Then, $\pi_1\pi_2(x) = \pi_2\pi_1(x) = x$ since x feels no action from either.
2. $x \in O_1 \Rightarrow x \notin O_2$. Then $\pi_1\pi_2(x) = \pi_1(x) = y \in O_1$, and $\pi_2\pi_1(x) = \pi_2(y) = y$.
2. $x \in O_2 \Rightarrow x \notin O_1$. Using a similar argument, the two expressions are equal.

Therefore, if two cycles in S_n are disjoint, then their product is commutative. □

> *Method* Computation of the product of two cycles is done right to left. Consider (12) and (23). We evaluate their product:
>
> $$(12)(23)$$
>
> ▷ 3 is mapped to 2 by the second cycle, and 2 is mapped to 1 by the first: this means that 3 is mapped to 1.
>
> ▷ 2 is mapped to 3 by the second cycle, which is left untouched by the first, meaning 2 is mapped to 3.
>
> ▷ 1 is untouched by the second, and mapped to 2 by the first, meaning 1 is mapped to 2.
>
> We see a single apparent cycle within this mapping, meaning that the result is the nontrivial (123).
>
> Consider now (1435)(326): we describe it more concisely, but the idea is the same:
>
> $$6 \to 3 \to 5;\ 2 \to 6;\ 3 \to 2;$$
> $$5 \to 1;\ 4 \to 3;\ 1 \to 4$$
>
> We pick any number to start : (143265).
>
> Last example: consider (1435)(321). Then, we have:
>
> $$1 \to 3 \to 5;\ 2 \to 1 \to 4;\ 3 \to 2$$
> $$4 \to 3;\ 5 \to 1$$
>
> Picking a random start, we try proceeding. If we hit a cycle before we're done, that means that there is still at least a number we haven't hit: we start from it, and keep going. In this case (15)(243).

Theorem 3.25 (Unproven[2])**.** *Any permutation $\sigma \in S_n$ can be written as the product of disjoint cycles, uniquely, up to the order of cycles used.*

[2]Meaning that it will not be proven here. you can find the proof in the teacher's summaries.

Definition 3.26. *The notation of $\sigma \in S_n$ as the product of disjoint cycles is called the cycle notation of σ. The lengths of these disjoint cycles is called the cycle type of σ.*

Proposition. *The cycle notation for $\pi\rho\pi^{-1}$ can be obtained from the cycle notation for ρ by replacing each i in ρ with $\pi(i)$.*

Proof. We have $\pi\rho\pi^{-1}(\pi(x)) = \pi\rho\pi^{-1}\pi(x) = \pi\rho(x)$. Now, we suppose ρ is a cycle:

$$\begin{aligned} \rho &: i \to \rho(i) & \rho &: (i, \rho(i), \rho^2(i), ...) \\ \pi\rho\pi^{-1} &: \pi(i) \to \pi\rho(i) & \pi\rho\pi^{-1} &: (\pi(i), \pi\rho(i), ...) \end{aligned}$$

□

Definition 3.27. *$s \in S_n$ is a transposition if it is a two-cycle, of the form (ij).*

Proposition. *Every k-cycle can be written as the product of $(k-1)$ transpositions.*

Proof. We prove this by induction:

Base: $k = 2$ is trivial, $k = 3$ is unpacked easily as $(123) = (13)(12)$.

Induction: Suppose $(123...k) = (1k)...(13)(12)$. We consider :

$$(1\ k+1)(123...k) \overset{(1)}{=} (123...k\ k+1) \overset{(2)}{=} (1k)...(13)(12)$$

where we obtain (1) by direct computation of the product and (2) by direct application of the induction hypothesis.

□

As a direct result of this, we can say that S_n is generated by the transpositions $\{(ij)\}_{i<j}$: since every permutation is the product of disjoint cycles, and every cycle is the product of transpositions, then every permutation is the product of transpositions, which might not be disjoint.

Theorem 3.28. *The product of an odd number of transposition cannot be equal to the product of an even number of transpositions.*

Proof. The proof of this can be found by considering the number of inversions present after a given permutation. Consider the state after the permutation σ as:

$$s_1 s_2 ... i m_1 m_2 ... m_k ... k e_1 e_2 ...$$

Now, consider $(ij)\sigma$ and any m_k.

- ▷ If $i < m_k, j < m_k$ or $m_k < i, m_k < j$, then swapping i and j does not contribute to the amount of inversions $\Rightarrow \pm 0$ inversions;
- ▷ If $i < m_k < j$ or $j < m_k < i$, then swapping i and j changes the inversion state between i and m_k, and between m_k and $j \Rightarrow \pm 2$ inversions.

Additionally, since $i \neq j$, swapping them adds or removes an inversion, as well, in such a way that in total, an additional transposition changes the number of inversions by 1.

Therefore, it is impossible to obtain the same number with $2k$ and $2k'+1$ transpositions, no matter the values of $k, k' \in \mathbb{N}$. □

Definition 3.29. *We use the number of inversions in a given permutation to define its sign as*

$$\operatorname{sgn}\sigma = (-1)^{\operatorname{inv}\sigma} = \begin{cases} 1 & ,\sigma \text{ has an even number of inversions} \\ -1 & ,\sigma \text{ has an odd number of inversions} \end{cases}$$

This can easily be shown to verify $\operatorname{sgn}(\sigma\tau) = \operatorname{sgn}(\sigma)\operatorname{sgn}(\tau)$...: $\operatorname{sgn} : S_n \to \{0,1\}$ is a group homomorphism! Recalling that the kernel of an homomorphism is a subgroup, we get that

$$A_n = \ker \operatorname{sgn} \triangleleft S_n = \{\sigma \in S_n : \operatorname{inv}\sigma \text{ is even}\}$$

A_n is called the alternating group, and it is of size $n!/2$ (can be shown by Lagrange.)

Proposition. *Let $g, h \in S_n$, consider $ghg^{-1} \in S_n$. If h is the product of disjoint cycles of lengths $\{l_1, l_2, ..., l_n\}$, then ghg^{-1} is the product of disjoint cycles of same length set. Therefore, any element that is the product of disjoint cycles of given lengths can be obtained from another of same lengths by conjugation with another element.*

Proof. Let us consider a single cycle ρ_l of length l. Then, we have that

$$\rho_l = (i_1 i_2 ... i_l) \Rightarrow g\rho_l g^{-1} = (g(i_1)...g(i_l))$$

is a cycle of the same length! This being said, we consider h as the product of disjoint cycles, with their relative lengths:

$$h = \rho_{l_1}...\rho_{l_r} \Rightarrow ghg^{-1} = (g\rho_{l_1}g^{-1})...(g\rho_{l_r}g^{-1}) = \gamma_{l_1}...\gamma l_r$$

where we introduce neutral elements in the product under the form $e = gg^{-1}$. Therefore, we see here that the action is obtained by mapping every element in every cycle of h to the corresponding element in the new cycles γ. $\square$

We can use conjugates to define classes:

Definition 3.30. *The conjugacy class of h, $\{ghg^{-1}\}_{g \in S_n}$ is the set of all elements conjugated to h in S_n. More informally, as we've seen, it's the set of all elements that have the same cycle type as h.*

> *Conclusion* This allows us to more formally define the idea that S_n is the disjoint union of the classes of elements that have same cycle type. These conjugacy classes are in bijection with the partitions of the integer n, of the form:
>
> $$\{\{i_1, ..., i_k\} : n = i_1 + ... + i_k, i_1 \geqslant ... \geqslant i_k\}$$
>
> with $\{i_1, ..., i_k\}$ corresponding to the cycle lengths of the elements in the class. For example, take the partitions of the number 4, matched with the corresponding

elements in S_4:

$$\{4\} \to \{(1234), (2143), ...\}$$
$$\{3,1\} \to \{(123), (234), ...\}$$
$$\{2,2\} \to \{(12)(34), (24)(13), ...\}$$
$$\{2,1,1\} \to \{(12), (13), (32), ...\}$$
$$\{1,1,1,1\} \to \{e\}$$

3.4 Actions of groups on sets

3.4.1 Orbits and stabilizers

Definition 3.31. *Let a finite group G, and a finite set E. We say that G acts on E by permutations if one can define the product $g \cdot x$ for any $g \in G, x \in E$ in such a way that*

$$e \cdot x = x \ \forall x \in E$$
$$g_1 g_2 \cdot x = g_1 \cdot (g_2 \cdot x) \ \forall g_1, g_2 \in G, x \in E$$

We also define the orbit of $x \in E$ under the action of G as the subset

$$\mathrm{Orb}_x = \{g \cdot x\}_{g \in G} \subset E$$

Proposition. *Let E a finite set, $x, y \in E$, G a finite group. Then,*

$$\mathrm{Orb}_x = \mathrm{Orb}_y \ \ ou \ \ \mathrm{Orb}_x \cap \mathrm{Orb}_y = \varnothing$$

Proof of this was done in an exercice set, and can be found in the appendix.

Since every element of E belongs to some orbit (at the very least Orb_x), we can write

$$E = \bigcup_{i=0}^{k} \mathrm{Orb}_{x_i}$$

with a set of orbit representatives $\{x_i\}_{i=0}^k$. If we consider the case of G acting on itself by conjugation, then the orbit of h in G is the conjugacy class $C_h = \{ghg^{-1}\}_{g \in G}$. This yields, similarly,

$$G = \bigcup_{i=0}^{k} C_{h_i}$$

which is not very interesting group for an abelian group as $C_h = ghg^{-1}{}_{g \in G} = \{gg^{-1}h\}_{g \in G} = \{h\}$, meaning they are all disjoint as they contain a single element.

Definition 3.32. *Let G, E be a finite group and a finite set, respectively, such that G acts on E. The stabilizer of x is the set:*

$$\mathrm{Stab}_x = \{g \in G : g \cdot x = x\}$$

It is a subgroup of G.

Theorem 3.33 (Orbit-Stabilizer Theorem)**.** *Let G be a finite group acting on E a finite set, let $x \in E$. Then,*

$$|\operatorname{Orb}_x| = [G : \operatorname{Stab}_x] = |G|/|\operatorname{Stab}_x|$$

Proof. Consider the left cosets with respect to $H = \operatorname{Stab}_x$. We have a bijection μ between $gH_{g\in G}$ and Orb_x. We define it as:

$$\mu : gH \mapsto g \cdot x$$

This mapping is surjective, because every g appears in a left coset of H. To prove it is injective, we consider two g, f such that $\mu(gH) = \mu(fH) \in Orb_x$:

$$g \cdot x = f \cdot x \Rightarrow f^{-1}g \cdot x = x \Rightarrow f^{-1}g \in \operatorname{Stab}_x \Rightarrow f^{-1}gH \subset H$$

This means $gH \subset fH$. Symmetrically, we establish $fH \subset gH$, meaning $fH = gH$. This implies μ is injective, meaning that the number of left cosets of H is the same as the number of elements in the orbit of x. Using the formula for the number of left cosets, we get

$$|Orb_x| = \#\text{ of left } H\text{-cosets} = [G : H] = [G : \operatorname{Stab}_x]$$

□

Definition 3.34. *The center of a group is the set of all elements that commute with every $g \in G$:*

$$\begin{aligned} Z(G) &= \{x \in G : g \cdot x = x \cdot g\ \forall g \in G\} \\ &= \{x \in G : g \cdot x \cdot g^{-1} = x\ \forall g \in G\} \end{aligned}$$

It is also the set of all 1-element conjugacy classes of G.

Theorem 3.35. *Using the center, we define the class equation of G, for a finite group G:*

$$|G| = |Z(G)| + \sum_{i=0}^{r} C_{x_i} = |Z(G)| + \sum_{i=0}^{r} [G : G_{x_i}]$$

Where G_{x_i} is the stabilizer of x_i with respect to conjugation.

Proof. We know that G is the disjoint union of its conjugacy classes

$$|G| = \sum_{i=0}^{m} |C_{x_i}| = \underbrace{\sum_{i=0}^{r} |C_{x_i}|}_{\text{conj. cl. of size } 1} + \underbrace{\sum_{j=0}^{s} |C_{x_j}|}_{\text{conj. cl. of size } \neq 1}$$

$$\Rightarrow |G| = |Z(G)| + \sum_{j=0}^{s} |C_{x_j}| = |Z(G)| + \sum_{j=0}^{s} |[G : G_{x_i}]|$$

Since the size of the conjugacy class is the number of left cosets of stabilizer subgroup. □

Application A group of order p^n with p prime has nontrivial center.

Proof.

$$|G| = |Z(G)| + \sum_{j=0}^{s} |[G : G_{x_i}]|$$

where $|G| = p^n$, which is divisible by p, and $[G : G_{x_i}] = |G|/|G_{x_i} = p^n/|G_{x_i}| > 1$, meaning it is divisible by p as well. This implies $|Z(G)|$ is also divisible by p, and since it contains e, it cannot be 0. Therefore, it has to be a nontrivial multiple of p. $\square$

Appendix A

Proofs from exercise sets

This barely needs such pompous titles but oh well. It's fun.

A.1 Theorem 1.1

Proposition. *Strong Induction $\Rightarrow$ Well-ordering principle.*

Proof. We can prove this by induction. Suppose there exists a subset $Y \subset \mathbb{N}$ such that it contains no least element. Consider $P(n) =$ "$n \notin Y$".

> **Base:** If 0 was in Y, then it would be its least element, since there are no smaller elements of $\mathbb{N}$. As such, it cannot be that $0 \in Y$, meaning $P(0)$ is true.
>
> **Induction:** Assume $P(k)$ is true for any $k \in \{0, 1, ..., n\}$. Then, if it was in Y, $n+1$ would be its smallest element, since every smaller element is not in Y. As such, $P(n+1)$ holds as well. Since P is hereditary and true for 0, it is true for any $n \in \mathbb{N}$.

$\square$

A.2 Theorem 2.4

Proposition. *Any $n > 1$ can be expressed by the product of primes.*

Proof. Consider $S = \{n \in \mathbb{N} : n > 1 \land n \text{ does not have a prime factorization}\}$. Then, we take the smallest element in this set, k. k cannot be a prime, so there exists $a, b < k$ such that $k = ab$. However, a and b cannot be in S, since they are smaller than k. This means that $a = \prod {p_{a,k}}^{a_k}, b = \prod {p_{b,k}}^{b_k}$, meaning that their product is the product of primes. Therefore, k cannot be in S, so S has to be empty. $\square$

A.3 Theorem 2.4

Proposition. *Any $n > 1$ can be expressed by the product of primes.*

Proof. Consider $S = \{n \in \mathbb{N} : n > 1 \wedge n \text{ does not have a prime factorization}\}$. Then, we take the smallest element in this set, k. k cannot be a prime, so there exists $a, b < k$ such that $k = ab$. However, a and b cannot be in S, since they are smaller than k. This means that $a = \prod {p_{a,k}}^{a_k}, b = \prod {p_{b,k}}^{b_k}$, meaning that their product is the product of primes. Therefore, k cannot be in S, so S has to be empty. $\square$

A.4 Theorem 3.4.1

Proposition. *Let E a finite set, $x, y \in E$, G a finite group. Then,*

$$\mathrm{Orb}_x = \mathrm{Orb}_y \ \ ou \ \ \mathrm{Orb}_x \cap \mathrm{Orb}_y = \varnothing$$

Proof. Assume that there exists an $s \in Orb_x : s \in Orb_y$. Then, there exist $g_x, g_y \in G$ such that

$$s = g_x \cdot x = g_y \cdot y \Leftrightarrow x = g_x^{-1} g_y \cdot y = g \cdot y$$

meaning that $x \in \mathrm{Orb}_y$, which in turn means $\mathrm{Orb}_x = \mathrm{Orb}_y$. Therefore, if there is an intersection between two orbits, then they must be the same. $\square$

Appendix B

Elliptic curves

Consider the equation

$$\Gamma : y^2 = x^3 + ax + b$$

for rational pairs $(x, y) \in \mathbb{Q}^2$. This is an elliptic curve. The set of points on this curve has group structure! We introduce the relation $P + Q = -R$ for three points P, Q, R colinear on the curve. Therefore, the relationships that follow from it are as follows:

] The neutral 0 element is at infinity (when there aren't three intersections with the curve, for example).

$P + 0 = 0 + P = P \ \forall P$

$-P$ is the point obtained from P by symmetry wrt. the x axis.

The group operation is therefore defined, in the general case, geometrically: to compute $P + Q$, you draw a line through P and Q, and you denote the intersection with the curve R. Then, $P + Q := -R$. For edge cases, we have:

- If P and Q are each other's reflection across the x axis, then $P + Q = 0$ (since there's no third intersection with the curve, we take the point at infinity).
- If $P = Q$, then you pick the line tangent to Γ at Q, find its intersection with Γ, denoted $2Q$. Then, $Q + Q = -2Q$.

This induces a specific algorithm to factorize a number $n \in \mathbb{N}$.

1. Define an elliptic curve $y^2 = x^3 + ax + b$ over $\mathbb{Z}/n\mathbb{Z}$, and pick a point $P = (x_0, y_0)$ on it.

2. Compute $i!P$ up to some integer $k > 0$. If we take the example of $3!P$, then we can show the process:

$$3!P = 3(2P) = 2 \cdot 2P + 2P$$

   This involves finding the slopes of tangent lines to the curve, as well as their integer intersections. This so