Algebra II

IMC 2023 Training

Robin Visser
Mathematics Institute
University of Warwick

13 June 2023

Overview

1. **Linear Algebra**
2. **Polynomials**
3. **Inequalities**
4. **Number Theory**
5. **Group Theory**

Overview

1. Linear Algebra (see 25 January session and handout!)
2. Polynomials (see Oleg's 22 February session and handout!)
3. Inequalities (see Jun's 12 May session!)
4. **Number Theory**
5. **Group Theory**

Number Theory

Example

Let x, y and z be integers such that $S = x^4 + y^4 + z^4$ is divisible by 5. Show that S is divisible by 5^4.

Number Theory

Example

Let x, y and z be integers such that $S = x^4 + y^4 + z^4$ is divisible by 5. Show that S is divisible by 5^4.

Example

For every positive integer n, let $p(n)$ denote the number of ways to express n as a sum of positive integers (e.g. $p(4) = 5$). Prove that $p(n) - p(n-1)$ is the number of ways to express n as a sum of integers each of which is strictly greater than 1.

Number Theory

Example

Let x, y and z be integers such that $S = x^4 + y^4 + z^4$ is divisible by 5. Show that S is divisible by 5^4.

Example

For every positive integer n, let $p(n)$ denote the number of ways to express n as a sum of positive integers (e.g. $p(4) = 5$). Prove that $p(n) - p(n-1)$ is the number of ways to express n as a sum of integers each of which is strictly greater than 1.

Example

(a) Show that the unit square can be partitioned into n smaller squares if n is large enough.

Number Theory

Example

Let x, y and z be integers such that $S = x^4 + y^4 + z^4$ is divisible by 5. Show that S is divisible by 5^4.

Example

For every positive integer n, let $p(n)$ denote the number of ways to express n as a sum of positive integers (e.g. $p(4) = 5$). Prove that $p(n) - p(n-1)$ is the number of ways to express n as a sum of integers each of which is strictly greater than 1.

Example

(a) Show that the unit square can be partitioned into n smaller squares if n is large enough.

(b) Let $d \geq 2$. Show that the d-dimensional unit cube can be partitioned into n smaller cubes if n is large enough.

Number Theory

Theorem (Fundamental Theorem of Arithmetic)

Every positive integer n can be uniquely represented as a product of primes:

$$n = p_1^{\alpha_1} p_2^{\alpha_2} \cdots p_k^{\alpha_k}$$

up to ordering.

Number Theory

Theorem (Fundamental Theorem of Arithmetic)

Every positive integer n can be uniquely represented as a product of primes:

$$n = p_1^{\alpha_1} p_2^{\alpha_2} \cdots p_k^{\alpha_k}$$

up to ordering.

- Unique factorisation (up to units) also holds in the rings $\mathbb{Z}[i]$, $\mathbb{Z}[\sqrt{2}]$, $\mathbb{Z}[\sqrt{-2}]$, $\mathbb{Z}[\omega]$.

Number Theory

Theorem (Fundamental Theorem of Arithmetic)

Every positive integer n can be uniquely represented as a product of primes:

$$n = p_1^{\alpha_1} p_2^{\alpha_2} \cdots p_k^{\alpha_k}$$

up to ordering.

- Unique factorisation (up to units) also holds in the rings $\mathbb{Z}[i]$, $\mathbb{Z}[\sqrt{2}]$, $\mathbb{Z}[\sqrt{-2}]$, $\mathbb{Z}[\omega]$.

Theorem (Bezout's identity)

Let a, b be two integers. Then there exist integers x, y such that $ax + by = gcd(a, b)$.

Number Theory

Theorem (Fundamental Theorem of Arithmetic)

Every positive integer n can be uniquely represented as a product of primes:

$$n = p_1^{\alpha_1} p_2^{\alpha_2} \cdots p_k^{\alpha_k}$$

up to ordering.

- Unique factorisation (up to units) also holds in the rings $\mathbb{Z}[i]$, $\mathbb{Z}[\sqrt{2}]$, $\mathbb{Z}[\sqrt{-2}]$, $\mathbb{Z}[\omega]$.

Theorem (Bezout's identity)

Let a, b be two integers. Then there exist integers x, y such that $ax + by = gcd(a, b)$.

Theorem

Let $a > 1$ be a positive integer, and let m, n be a positive integer. Then

$$gcd(a^m - 1, a^n - 1) = a^{gcd(m,n)} - 1.$$

Examples

Example

Prove there are only finitely many positive integers n such that $n! + 1$ divides $(2012n)!$.

Examples

Example

Prove there are only finitely many positive integers n such that $n! + 1$ divides $(2012n)!$.

Example

Let $n > 6$ be a perfect number, and let $n = p_1^{e_1} \cdots p_k^{e_k}$ be its prime factorisation with $1 < p_1 < \cdots < p_k$. Prove that e_1 is an even number.

Examples

Example

Prove there are only finitely many positive integers n such that $n! + 1$ divides $(2012n)!$.

Example

Let $n > 6$ be a perfect number, and let $n = p_1^{e_1} \cdots p_k^{e_k}$ be its prime factorisation with $1 < p_1 < \cdots < p_k$. Prove that e_1 is an even number.

Example

Show there does not exist 15 integers $m_1, \ldots, m_{15}$ such that

$$\sum_{k=1}^{15} m_k \cdot \arctan(k) = \arctan(16).$$

Examples

Example

Prove there are only finitely many positive integers n such that $n! + 1$ divides $(2012n)!$.

Example

Let $n > 6$ be a perfect number, and let $n = p_1^{e_1} \cdots p_k^{e_k}$ be its prime factorisation with $1 < p_1 < \cdots < p_k$. Prove that e_1 is an even number.

Example

Show there does not exist 15 integers $m_1, \ldots, m_{15}$ such that

$$\sum_{k=1}^{15} m_k \cdot \arctan(k) = \arctan(16).$$

Hint: Use complex numbers and rewrite the condition as $\arg(z_1) = \arg(z_2)$ for some suitable $z_1, z_2 \in \mathbb{C}$.

Chinese Remainder Theorem

Theorem (Chinese Remainder Theorem)

Let $m_1, \ldots, m_k$ be pairwise coprime positive integers. Let $c_1, \ldots, c_k$ be integers. Then the system of congruences

$$\begin{aligned} x &\equiv c_1 \pmod{m_1} \\ x &\equiv c_2 \pmod{m_2} \\ &\vdots \\ x &\equiv c_k \pmod{m_k} \end{aligned}$$

has a unique solution mod $m_1 m_2 \cdots m_k$.

Chinese Remainder Theorem

Theorem (Chinese Remainder Theorem)

Let $m_1, \ldots, m_k$ be pairwise coprime positive integers. Let $c_1, \ldots, c_k$ be integers. Then the system of congruences

$$\begin{aligned} x &\equiv c_1 \ (mod\ m_1) \\ x &\equiv c_2 \ (mod\ m_2) \\ &\vdots \\ x &\equiv c_k \ (mod\ m_k) \end{aligned}$$

has a unique solution mod $m_1 m_2 \cdots m_k$.

- Equivalently, let $M = m_1 m_2 \cdots m_k$. Then there's a ring isomorphism given by:

$$\mathbb{Z}/M\mathbb{Z} \longrightarrow \mathbb{Z}/m_1\mathbb{Z} \times \cdots \times \mathbb{Z}/m_k\mathbb{Z}$$
$$x \bmod M \longmapsto (x \bmod m_1, \ldots, x \bmod m_k)$$

Chinese Remainder Theorem

Example

Find the number of positive integers x satisfying the following two conditions:

1. $x < 10^{2006}$.
2. $x^2 - x$ is divisible by 10^{2006}.

Chinese Remainder Theorem

Example

Find the number of positive integers x satisfying the following two conditions:

1. $x < 10^{2006}$.
2. $x^2 - x$ is divisible by 10^{2006}.

Example

Let p and q be relatively prime positive integers. Prove that

$$\sum_{k=0}^{pq-1} (-1)^{\left\lfloor \frac{k}{p} \right\rfloor + \left\lfloor \frac{k}{q} \right\rfloor} = \begin{cases} 0 & \text{if } pq \text{ is even,} \\ 1 & \text{if } pq \text{ is odd.} \end{cases}$$

Chinese Remainder Theorem

Example

Find the number of positive integers x satisfying the following two conditions:

1. $x < 10^{2006}$.
2. $x^2 - x$ is divisible by 10^{2006}.

Example

Let p and q be relatively prime positive integers. Prove that

$$\sum_{k=0}^{pq-1} (-1)^{\left\lfloor \frac{k}{p} \right\rfloor + \left\lfloor \frac{k}{q} \right\rfloor} = \begin{cases} 0 & \text{if } pq \text{ is even,} \\ 1 & \text{if } pq \text{ is odd.} \end{cases}$$

Hint: The map $k \mapsto (k \bmod p, k \bmod q)$ is a bijection between $\mathbb{Z}/pq\mathbb{Z}$ and $\mathbb{Z}/p\mathbb{Z} \times \mathbb{Z}/q\mathbb{Z}$.

Number Theory

Theorem (Wilson's Theorem)

If p is prime, then $(p-1)! \equiv -1 \pmod{p}$.

Number Theory

Theorem (Wilson's Theorem)

If p is prime, then $(p-1)! \equiv -1 \pmod{p}$.

Theorem (Fermat's Little Theorem)

Let p be a prime, and a an integer not divisible by p. Then $a^{p-1} \equiv 1 \pmod{p}$.

Number Theory

Theorem (Wilson's Theorem)

If p is prime, then $(p-1)! \equiv -1 \pmod{p}$.

Theorem (Fermat's Little Theorem)

Let p be a prime, and a an integer not divisible by p. Then $a^{p-1} \equiv 1 \pmod{p}$.

Example

Let p be a prime number. Prove that

$$x^{p^p-1} - 1 = (x^p - x + 1)f(x) + pg(x)$$

for some polynomials f and g with integer coefficients.

Number Theory

Theorem (Wilson's Theorem)

If p is prime, then $(p-1)! \equiv -1 \pmod{p}$.

Theorem (Fermat's Little Theorem)

Let p be a prime, and a an integer not divisible by p. Then $a^{p-1} \equiv 1 \pmod{p}$.

Example

Let p be a prime number. Prove that

$$x^{p^p-1} - 1 = (x^p - x + 1)f(x) + pg(x)$$

for some polynomials f and g with integer coefficients.

Hint: Prove that $x^{p^p-1} - 1$ is divisible by $x^p - x + 1$ over $\mathbb{F}_p[x]$.

Number Theory

Euler's function

Let n be a positive integer. The Euler function $\varphi(n)$ is the number of positive integers less than n coprime to n. It holds that

$$\varphi(n) = n\left(1 - \frac{1}{p_1}\right) \cdots \left(1 - \frac{1}{p_k}\right),$$

where $n = p_1^{\alpha_1} \cdots p_k^{\alpha_k}$ is the factorization of n into primes.

Number Theory

Euler's function

Let n be a positive integer. The Euler function $\varphi(n)$ is the number of positive integers less than n coprime to n. It holds that

$$\varphi(n) = n\left(1 - \frac{1}{p_1}\right) \cdots \left(1 - \frac{1}{p_k}\right),$$

where $n = p_1^{\alpha_1} \cdots p_k^{\alpha_k}$ is the factorization of n into primes.

Theorem (Euler's theorem)

Let n be a positive integer, and a an integer coprime to n. Then $a^{\varphi(n)} \equiv 1 \pmod{n}$.

Quadratic residues

Legendre symbol

$$\left(\frac{a}{p}\right) := \begin{cases} 1 & \text{if } a \text{ is a quadratic residue mod } p \text{ and } p \nmid a, \\ 0 & \text{if } p \mid a, \\ -1 & \text{otherwise.} \end{cases}$$

Quadratic residues

Legendre symbol

$$\left(\frac{a}{p}\right) := \begin{cases} 1 & \text{if } a \text{ is a quadratic residue mod } p \text{ and } p \nmid a, \\ 0 & \text{if } p \mid a, \\ -1 & \text{otherwise.} \end{cases}$$

- Properties: $\left(\frac{a}{p}\right) = \left(\frac{a+p}{p}\right)$ and $\left(\frac{a}{p}\right)\left(\frac{b}{p}\right) = \left(\frac{ab}{p}\right)$.

Quadratic residues

Legendre symbol

$$\left(\frac{a}{p}\right) := \begin{cases} 1 & \text{if } a \text{ is a quadratic residue mod } p \text{ and } p \nmid a, \\ 0 & \text{if } p \mid a, \\ -1 & \text{otherwise.} \end{cases}$$

- Properties: $\left(\frac{a}{p}\right) = \left(\frac{a+p}{p}\right)$ and $\left(\frac{a}{p}\right)\left(\frac{b}{p}\right) = \left(\frac{ab}{p}\right)$.

Theorem (Euler's criterion)

For any odd prime p, and integer a,

$$\left(\frac{a}{p}\right) \equiv a^{\frac{p-1}{2}} \pmod{p}.$$

Theorem (Gauss reciprocity)

For any two distinct odd primes p and q,

$$\left(\frac{p}{q}\right)\left(\frac{q}{p}\right) = (-1)^{\frac{p-1}{2}\frac{q-1}{2}}.$$

Pell's equation

Theorem (Pell's equation)

Let $D \in \mathbb{N}$ be a positive nonsquare integer. Then the equation

$$x^2 - Dy^2 = 1$$

has infinitely many integer solutions.

Pell's equation

Theorem (Pell's equation)

Let $D \in \mathbb{N}$ be a positive nonsquare integer. Then the equation

$$x^2 - Dy^2 = 1$$

has infinitely many integer solutions.

Example

Prove that is p and q are rational numbers and $r = p + q\sqrt{7}$, then there exists a matrix $\begin{pmatrix} a & b \\ c & d \end{pmatrix} \neq \pm \begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix}$ with integer entries and with $ad - bc = 1$ such that $\dfrac{ar + b}{cr + d} = r$.

Pell's equation

Theorem (Pell's equation)

Let $D \in \mathbb{N}$ be a positive nonsquare integer. Then the equation

$$x^2 - Dy^2 = 1$$

has infinitely many integer solutions.

Example

Prove that is p and q are rational numbers and $r = p + q\sqrt{7}$, then there exists a matrix $\begin{pmatrix} a & b \\ c & d \end{pmatrix} \neq \pm \begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix}$ with integer entries and with $ad - bc = 1$ such that $\frac{ar + b}{cr + d} = r$.

Hint: Consider the minimal polynomial of r in $\mathbb{Z}[x]$. Reduce the problem to solving a Pell-like equation.

More problems!

Example

Let a, b be two integers and suppose that n is a positive integer for which the set

$$\mathbb{Z} \setminus \{ax^n + by^n \mid x, y \in \mathbb{Z}\}$$

is finite. Prove that $n = 1$.

More problems!

Example

Let a, b be two integers and suppose that n is a positive integer for which the set

$$\mathbb{Z} \setminus \{ax^n + by^n \mid x, y \in \mathbb{Z}\}$$

is finite. Prove that $n = 1$.

Example

Prove that there exists an infinite number of relatively prime pairs (m, n) of positive integers such that the equation $(x + m)^3 = nx$ has three distinct integer roots.

More problems!

Example

Let a, b be two integers and suppose that n is a positive integer for which the set

$$\mathbb{Z} \setminus \{ax^n + by^n \mid x, y \in \mathbb{Z}\}$$

is finite. Prove that $n = 1$.

Example

Prove that there exists an infinite number of relatively prime pairs (m, n) of positive integers such that the equation $(x + m)^3 = nx$ has three distinct integer roots.

Example

Let A be an $n \times n$-matrix with integer entries and $b_1, \ldots, b_k$ be integers satisfying $detA = b_1 \cdot \cdots \cdot b_k$. Prove that there exist $n \times n$-matrices $B_1, \ldots, B_k$ with integer entries such that $A = B_1 \cdot \cdots \cdot B_k$ and $detBi = bi$ for all $i = 1, \ldots, k$.

Groups, Rings and Fields

Group

A **group** is a set G equipped with a binary operation $*$ such that the operation is *associative*, an *identity element* exists and every element has an *inverse*.

Groups, Rings and Fields

Group

A **group** is a set G equipped with a binary operation $*$ such that the operation is *associative*, an *identity element* exists and every element has an *inverse*.

- G is **abelian** if $*$ is commutative.

Groups, Rings and Fields

Group

A **group** is a set G equipped with a binary operation $*$ such that the operation is *associative*, an *identity element* exists and every element has an *inverse*.

- G is **abelian** if $*$ is commutative.

Ring

A **ring** is a set R equipped with two binary operations, $+$ and $\times$, such that $(R, +)$ is an abelian group, $(R, \times)$ is a monoid (*identity and associative*), and $\times$ is distributive over $+$.

Groups, Rings and Fields

Group

A **group** is a set G equipped with a binary operation $*$ such that the operation is *associative*, an *identity element* exists and every element has an *inverse*.

- G is **abelian** if $*$ is commutative.

Ring

A **ring** is a set R equipped with two binary operations, $+$ and $\times$, such that $(R, +)$ is an abelian group, $(R, \times)$ is a monoid (*identity and associative*), and $\times$ is distributive over $+$.

- R is **commutative** if multiplication $\times$ is commutative.

Groups, Rings and Fields

Group

A **group** is a set G equipped with a binary operation $*$ such that the operation is *associative*, an *identity element* exists and every element has an *inverse*.

- G is **abelian** if $*$ is commutative.

Ring

A **ring** is a set R equipped with two binary operations, $+$ and $\times$, such that $(R, +)$ is an abelian group, $(R, \times)$ is a monoid (*identity and associative*), and $\times$ is distributive over $+$.

- R is **commutative** if multiplication $\times$ is commutative.

Field

A **field** F is a commutative ring such that every non-zero element has a multiplicative inverse.

Groups, Rings and Fields

Example

Does there exist a field such that its multiplicative group is isomorphic to its additive group?

Groups, Rings and Fields

Example

Does there exist a field such that its multiplicative group is isomorphic to its additive group?

Example

Suppose that in a not necessarily commutative ring R the square of any element is 0. Prove that $abc + abc = 0$ for any three elements a, b, c.

Groups, Rings and Fields

Example

Does there exist a field such that its multiplicative group is isomorphic to its additive group?

Example

Suppose that in a not necessarily commutative ring R the square of any element is 0. Prove that $abc + abc = 0$ for any three elements a, b, c.

Example

Let R be a commutative ring of characteristic zero. Let e, f, and g be idempotent elements of R satisfying $e + f + g = 0$. Show that $e = f = g = 0$.

Group Theory

Theorem (Lagrange's Theorem)

Let G be a finite group of order n. Then any subgroup H of G has order dividing n.

Group Theory

Theorem (Lagrange's Theorem)

Let G be a finite group of order n. Then any subgroup H of G has order dividing n.

Theorem (Orbit-stabiliser theorem)

Let G be a finite group acting on a set X. The orbit of x is $G \cdot x = \{gx \mid g \in G\}$. and the stabiliser subgroup of g with respect to x is $G_x = \{g \in G \mid gx = x\}$.
Then $|G \cdot x||G_x| = |G|$.

Group Theory

Theorem (Lagrange's Theorem)

Let G be a finite group of order n. Then any subgroup H of G has order dividing n.

Theorem (Orbit-stabiliser theorem)

Let G be a finite group acting on a set X. The orbit of x is $G \cdot x = \{gx \mid g \in G\}$. and the stabiliser subgroup of g with respect to x is $G_x = \{g \in G \mid gx = x\}$.
Then $|G \cdot x||G_x| = |G|$.

Theorem ("Burnside's" lemma)

Let G be a finite group acting on a set X. The number of orbits $|X/G|$ of X is

$$|X/G| = \frac{1}{|G|} \sum_{g \in G} |X^g|$$

where $X^g := \{x \in X \mid gx = x\}$ is the set of points fixed by g.

Examples

Example

Let r, s, t be positive integers which are pairwise relatively prime. If a and b are elements of an abelian group with unity element e, and $a^r = b^s = (ab)^t = e$, prove that $a = b = e$. Does the same conclusion hold if a and b are elements of an arbitrary non-commutative group?

Examples

Example

Let r, s, t be positive integers which are pairwise relatively prime. If a and b are elements of an abelian group with unity element e, and $a^r = b^s = (ab)^t = e$, prove that $a = b = e$. Does the same conclusion hold if a and b are elements of an arbitrary non-commutative group?

Example

Denote by S_n the group of permutations of the sequnece $(1, 2, \dots, n)$. Suppose that G is a subgroup of S_n, such that for every $\pi \in G \backslash \{e\}$ there exists a unique $k \in \{1, 2, \dots, n\}$ for which $\pi(k) = k$. Show that this k is the same for all $\pi \in G \backslash \{e\}$.

Examples

Example

Let r, s, t be positive integers which are pairwise relatively prime. If a and b are elements of an abelian group with unity element e, and $a^r = b^s = (ab)^t = e$, prove that $a = b = e$. Does the same conclusion hold if a and b are elements of an arbitrary non-commutative group?

Example

Denote by S_n the group of permutations of the sequnece $(1, 2, \ldots, n)$. Suppose that G is a subgroup of S_n, such that for every $\pi \in G \backslash \{e\}$ there exists a unique $k \in \{1, 2, \ldots, n\}$ for which $\pi(k) = k$. Show that this k is the same for all $\pi \in G \backslash \{e\}$.

Hint: Consider G acting on the set $X = \{1, 2, \ldots, n\}$ and apply orbit-stabiliser theorem.

Group theory

Example

Let G be a group of $n \geq 2$ be an integer. Let H_1 and H_2 be two subgroups of G that satisfy

$$[G : H_1] = [G : H_2] = n \quad \text{and} \quad [G : (H_1 \cap H_2)] = n(n-1).$$

Prove that H_1 and H_2 are conjugate in G.

Group theory

Example

Let G be a group of $n \geq 2$ be an integer. Let H_1 and H_2 be two subgroups of G that satisfy

$$[G : H_1] = [G : H_2] = n \quad \text{and} \quad [G : (H_1 \cap H_2)] = n(n-1).$$

Prove that H_1 and H_2 are conjugate in G.

Hint: Express H_1, H_2 both as the disjoint union of left cosets with respect to H_2 and and as the disjoint union of right cosets with respect to H_1.

Permutation groups

Symmetric group

The **symmetric group** S_n is the group of all $n!$ permutations on a set of n elements.

Permutation groups

Symmetric group

The **symmetric group** S_n is the group of all $n!$ permutations on a set of n elements.

Example

For a prime number p, let $\mathrm{GL}_2(\mathbb{Z}/p\mathbb{Z})$ be the group of invertible 2×2 matrices of residue modulo p. Show that there is no injective group homomorphism $\varphi : \mathrm{GL}_2(\mathbb{Z}/p\mathbb{Z}) \to S_p$.

Permutation groups

Symmetric group

The **symmetric group** S_n is the group of all $n!$ permutations on a set of n elements.

Example

For a prime number p, let $\mathrm{GL}_2(\mathbb{Z}/p\mathbb{Z})$ be the group of invertible 2×2 matrices of residue modulo p. Show that there is no injective group homomorphism $\varphi : \mathrm{GL}_2(\mathbb{Z}/p\mathbb{Z}) \to S_p$.

Example

Prove that the following proposition holds for $n = 3$, but not for $n = 4$.
For any permutation π_1 of $\{1, 2, \ldots, n\}$ different from the identity there is a permutation π_2 such that any permutation π can be obtained from π_1 and π_2 using only compositions (e.g. $\pi = \pi_1 \circ \pi_1 \circ \pi_2 \circ \pi_1$).

Permutation groups

Symmetric group

The **symmetric group** S_n is the group of all $n!$ permutations on a set of n elements.

Example

For a prime number p, let $\mathrm{GL}_2(\mathbb{Z}/p\mathbb{Z})$ be the group of invertible 2×2 matrices of residue modulo p. Show that there is no injective group homomorphism $\varphi : \mathrm{GL}_2(\mathbb{Z}/p\mathbb{Z}) \to S_p$.

Example

Prove that the following proposition holds for $n = 3$, but not for $n = 4$.
For any permutation π_1 of $\{1, 2, \ldots, n\}$ different from the identity there is a permutation π_2 such that any permutation π can be obtained from π_1 and π_2 using only compositions (e.g. $\pi = \pi_1 \circ \pi_1 \circ \pi_2 \circ \pi_1$).

Hint: For $n = 4$, let $\pi_1 = (12)(34)$ and consider $S_4/\{\mathrm{id}, (12)(34), (13)(24), (14)(23)\}$.

More problems!

Example

Let $n > 1$ be an integer. Two players, A and B, play the following game. Taking turns, they select elements (one element at a time) from the group S_n. It is forbidden to select an element that has already been selected. The game ends when the selected elements generate the whole group S_n. The player who made the last move loses the game. The first move is made by A. Which player has a winning strategy?

More problems!

Example

Let $n > 1$ be an integer. Two players, A and B, play the following game. Taking turns, they select elements (one element at a time) from the group S_n. It is forbidden to select an element that has already been selected. The game ends when the selected elements generate the whole group S_n. The player who made the last move loses the game. The first move is made by A. Which player has a winning strategy?

Example

Find all positive integers n for which there exists a family $\mathcal{F}$ of three-element subsets of $S = \{1, 2, \ldots, n\}$ satisfying the following two conditions:

(i) for any two different elements $a, b \in S$, there exists exactly one $A \in \mathcal{F}$ containing both a, b;

(ii) if a, b, c, x, y, z are elements of S such that if $\{a, b, x\}, \{a, c, y\}, \{b, c, z\} \in \mathcal{F}$, then $\{x, y, z\} \in \mathcal{F}$.