Elementary problems in number theory

Csaba Szabó

Eötvös Loránd University, Budapest

June, 2010

Problem 1.

How many numbers do you have to choose from 1 to 2n such that at least two of them are relatively prime?

Problem 1.

How many numbers do you have to choose from 1 to 2n such that at least two of them are relatively prime?

Problem 1.

How many numbers do you have to choose from 1 to 2n such that at least two of them are relatively prime?

- $2n$ is enough (contains 1 and 2)

Problem 1.

How many numbers do you have to choose from 1 to 2n such that at least two of them are relatively prime?

- $2n$ is enough (contains 1 and 2)
- n is not enough: $2, 4, 6, \ldots, 2n$

Problem 1.

How many numbers do you have to choose from 1 to 2n such that at least two of them are relatively prime?

- $2n$ is enough (contains 1 and 2)
- n is not enough: $2, 4, 6, \ldots, 2n$

n+1 is enough:

There are two consecutive numbers among them.
Proof: Pigeon-holes: $\{1, 2\}$, $\{3, 4\}$, $\ldots$, $\{2n-1, 2n\}$,

Problem 2.

How many numbers do you have to choose from 1 to 2n such that there are two among them s.t. one divides the other?

Problem 2.

How many numbers do you have to choose from 1 to 2n such that there are two among them s.t. one divides the other?

Problem 2.

How many numbers do you have to choose from 1 to 2n such that there are two among them s.t. one divides the other?

- $2n$ is enough (contains 1 and 2)

Problem 2.

How many numbers do you have to choose from 1 to 2n such that there are two among them s.t. one divides the other?

- $2n$ is enough (contains 1 and 2)
- n is not enough: $n+1, n+2, \ldots, 2n$

Problem 2.

How many numbers do you have to choose from 1 to 2n such that there are two among them s.t. one divides the other?

- $2n$ is enough (contains 1 and 2)
- n is not enough: $n+1, n+2, \ldots, 2n$

n+1 is enough:

Proof: Pigeon-holes: $\{1 \cdot 2^t\}, \{3 \cdot 2^t\}, \ldots, \{(2n-1) \cdot 2^t\}$, labelled by odd numbers.

Problem 3.

How many numbers do you have to choose such that the sum of a *few* of them is divisible by n?

Problem 3.

How many numbers do you have to choose such that the sum of a *few* of them is divisible by n?

Problem 3.

How many numbers do you have to choose such that the sum of a *few* of them is divisible by n?

- $n-1$ is not enough: $1, 1, \ldots, 1$

Problem 3.

How many numbers do you have to choose such that the sum of a *few* of them is divisible by n?

- $n - 1$ is not enough: $1, 1, \ldots, 1$

n is enough:

Proof: Pigeon-holes: residue classes

Pigeons: a_1, $a_1 + a_2$, ..., $a_1 + a_2 + \cdots + a_n$

Two in the same pigeon-hole:

$$\sum_1^l a_i - \sum_1^k a_i = \sum_k^l a_i$$

Problem 4.

How many numbers do you have to choose such that the sum of n of them is divisible by n?

Problem 4.

How many numbers do you have to choose such that the sum of n of them is divisible by n?

Problem 4.

How many numbers do you have to choose such that the sum of n of them is divisible by n?

- $2n-2$ is not enough: $0, 0, \ldots, 0, 1, 1, \ldots, 1$

Problem 4.

How many numbers do you have to choose such that the sum of n of them is divisible by n?

- $2n-2$ is not enough: $0, 0, \ldots, 0, 1, 1, \ldots, 1$

$n^2 - n + 1$ is enough:

Proof: Pigeon-holes: resiude classes
At least n in a single pigeon-hole

Problem 4.

How many numbers do you have to choose such that the sum of n of them is divisible by n?

- $2n-2$ is not enough: $0, 0, \ldots, 0, 1, 1, \ldots, 1$

$n^2 - n + 1$ is enough:

Proof: Pigeon-holes: resiude classes
At least n in a single pigeon-hole

$(n-1)^2 + 1$ is enough:

Is there a better bound?

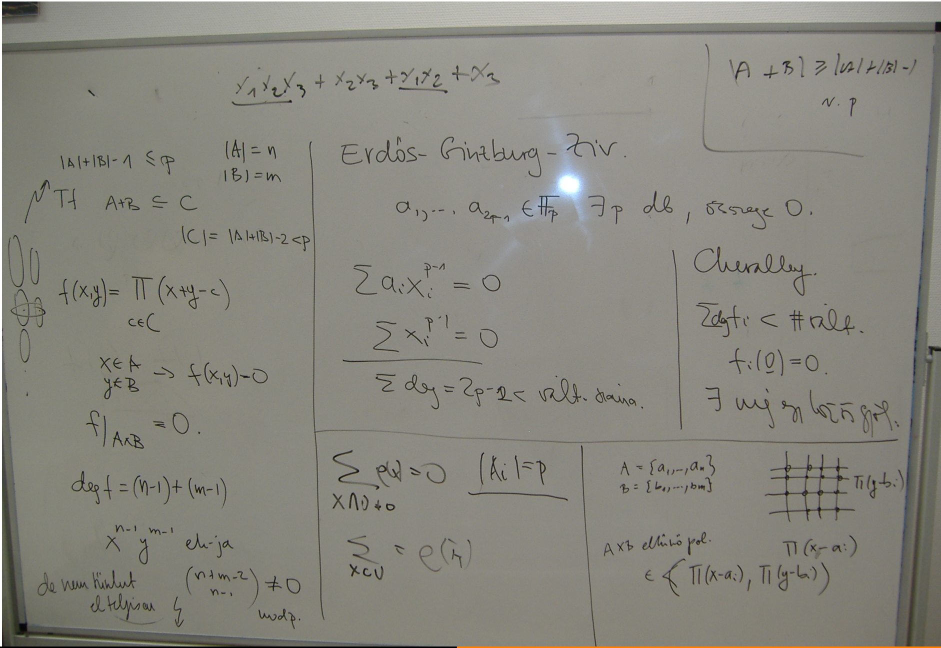
Chevalley's Theorem

Lemma

Let $A_1, \ldots, A_n$ *be subsets of* F_p*, the* p*-element field, and* $f \in F_p[x_1, \ldots, x_n]$ *such that*

$$\sum_{i=1}^{n}(|A_i| - 1) > (p-1)\deg f.$$

If the set $\{a \in A_1 \times \cdots \times A_n | f(a) = 0\}$ *is not empty, then it has at least two different elements.*


Erdős-Ginzburg-Ziv.
|A| = n
|B| = m
Tf A+B ⊆ C
Chevalley.
f(x,y) = Π (x+y-c)
deg f = (n-1)+(m-1)
A×B eltűnő pol.

Why am I talking about these problems?

Definition

Let **A** be an algebra and t_1 and t_2 be two terms over **A**.

Definition

Let $\mathbf{A}$ be an algebra and t_1 and t_2 be two terms over $\mathbf{A}$.

- We say that t_1 and t_2 are equivalent over $\mathbf{A}$ if $t_1(\bar{a}) = t_2(\bar{a})$ for every substitution $\bar{a} \in \mathbf{A}$

Definition

Let **A** be an algebra and t_1 and t_2 be two terms over **A**.

- We say that t_1 and t_2 are equivalent over **A** if $t_1(\bar{a}) = t_2(\bar{a})$ for every substitution $\bar{a} \in \mathbf{A}$

Definition

ID-CHECK **A**

Definition

Let **A** be an algebra and t_1 and t_2 be two terms over **A**.

- We say that t_1 and t_2 are equivalent over **A** if $t_1(\bar{a}) = t_2(\bar{a})$ for every substitution $\bar{a} \in \mathbf{A}$

Definition

ID-CHECK **A**

- Let **A** be an algebra

Definition

Let **A** be an algebra and t_1 and t_2 be two terms over **A**.

- We say that t_1 and t_2 are equivalent over **A** if $t_1(\bar{a}) = t_2(\bar{a})$ for every substitution $\bar{a} \in$ **A**

Definition

ID-CHECK **A**

- Let **A** be an algebra
- Input: t_1 and t_2 two terms over **A**

Definition

Let **A** be an algebra and t_1 and t_2 be two terms over **A**.

- We say that t_1 and t_2 are equivalent over **A** if $t_1(\bar{a}) = t_2(\bar{a})$ for every substitution $\bar{a} \in \mathbf{A}$

Definition

ID-CHECK **A**

- Let **A** be an algebra
- Input: t_1 and t_2 two terms over **A**
- Question: Are t_1 and t_2 equivalent over **A**?

Definition

Let **A** be an algebra and t_1 and t_2 be two terms over **A**.

- We say that t_1 and t_2 are equivalent over **A** if $t_1(\bar{a}) = t_2(\bar{a})$ for every substitution $\bar{a} \in$ **A**

Definition

ID-CHECK **A**

- Let **A** be an algebra
- Input: t_1 and t_2 two terms over **A**
- Question: Are t_1 and t_2 equivalent over **A**?

Always decidable: check every substitution

Another question

Another question

- t_1 and t_2 two polynomials over **A**

Another question

- t_1 and t_2 two polynomials over **A**
- $\mathrm{POL\text{-}SAT}$: Does $t_1 = t_2$ have a solution?

Another question

- t_1 and t_2 two polynomials over **A**
- POL-SAT : Does $t_1 = t_2$ have a solution?

Rings

Another question

- t_1 and t_2 two polynomials over **A**
- POL-SAT : Does $t_1 = t_2$ have a solution?

Rings

- ID-CHECK **R**: Is $t = t_1 - t_2$ identically 0?

Another question

- t_1 and t_2 two polynomials over **A**
- POL-SAT : Does $t_1 = t_2$ have a solution?

Rings

- ID-CHECK **R**: Is $t = t_1 - t_2$ identically 0?
- POL-SAT **R**: Does $t = t_1 - t_2$ have a root?

Abelian groups

A Abelian group

Abelian groups

A Abelian group

- $t(x_1, \ldots, x_n) = x_1^{k_1} \ldots x_n^{k_n}$

Abelian groups

$\mathbf{A}$ Abelian group

- $t(x_1, \ldots, x_n) = x_1^{k_1} \ldots x_n^{k_n}$
- $t(x_1, \ldots, x_n) \overset{?}{\equiv} 1$ over $\mathbf{A}$

Abelian groups

A Abelian group

- $t(x_1, \ldots, x_n) = x_1^{k_1} \ldots x_n^{k_n}$
- $t(x_1, \ldots, x_n) \overset{?}{\equiv} 1$ over **A**
- $x_1^{k_1} \ldots x_n^{k_n} \equiv 1$

Abelian groups

A Abelian group

- $t(x_1, \ldots, x_n) = x_1^{k_1} \ldots x_n^{k_n}$
- $t(x_1, \ldots, x_n) \overset{?}{\equiv} 1$ over **A**
- $x_1^{k_1} \ldots x_n^{k_n} \equiv 1$
- $\forall i \neq m \; x_i = 1 \Longrightarrow x_m^{k_m} \equiv 1$

Abelian groups

A Abelian group

- $t(x_1,\dots,x_n)=x_1^{k_1}\dots x_n^{k_n}$
- $t(x_1,\dots,x_n)\overset{?}{\equiv}1$ over $\mathbf{A}$
- $x_1^{k_1}\dots x_n^{k_n}\equiv 1$
- $\forall i\neq m\ x_i=1\Longrightarrow x_m^{k_m}\equiv 1$
- $\exp\mathbf{A}\mid k_m$ for every m

Abelian groups

A Abelian group

- $t(x_1, \dots, x_n) = x_1^{k_1} \dots x_n^{k_n}$
- $t(x_1, \dots, x_n) \overset{?}{\equiv} 1$ over $\mathbf{A}$
- $x_1^{k_1} \dots x_n^{k_n} \equiv 1$
- $\forall i \neq m\ x_i = 1 \Longrightarrow x_m^{k_m} \equiv 1$
- $\exp \mathbf{A} \mid k_m$ for every m
- $x_1^{k_1} \dots x_n^{k_n} \equiv 1 \Longleftrightarrow \forall m\colon\ \exp \mathbf{A} \mid k_m$

Nilpotent rings

Idziak- Szabó

Let A be a nilpotent algebra of size r and of nilpotency class k, and $f(\bar{x}) \in R[x_1, x_2, \ldots, x_n]$ be a polynomial over A.
Then for every $\bar{a} \in R^n$ there is a $\bar{b} \in R^n$ such that

Nilpotent rings

Idziak- Szabó

Let A be a nilpotent algebra of size r and of nilpotency class k, and $f(\bar{x}) \in R[x_1, x_2, \ldots, x_n]$ be a polynomial over A.
Then for every $\bar{a} \in R^n$ there is a $\bar{b} \in R^n$ such that

- $b_i = 0$ or $b_i = a_i$

Nilpotent rings

Idziak- Szabó

Let A be a nilpotent algebra of size r and of nilpotency class k, and $f(\bar{x}) \in R[x_1, x_2, \ldots, x_n]$ be a polynomial over A.
Then for every $\bar{a} \in R^n$ there is a $\bar{b} \in R^n$ such that

- $b_i = 0$ or $b_i = a_i$
- $b_i = a_i$ for at most $\mathbf{r}^{\mathbf{r}^{\cdots^{\mathbf{r}^{\mathbf{k}}}}}$ many i-s (there are k-many r-s in the tower)

Nilpotent rings

Idziak- Szabó

Let A be a nilpotent algebra of size r and of nilpotency class k, and $f(\bar{x}) \in R[x_1, x_2, \ldots, x_n]$ be a polynomial over A.
Then for every $\bar{a} \in R^n$ there is a $\bar{b} \in R^n$ such that

- $b_i = 0$ or $b_i = a_i$
- $b_i = a_i$ for at most $\mathbf{r^{r^{\cdots^{r^k}}}}$ many i-s (there are k-many r-s in the tower)
- $f(\bar{a}) = f(\bar{b})$

Nilpotent rings

Idziak- Szabó

Let A be a nilpotent algebra of size r and of nilpotency class k, and $f(\bar{x}) \in R[x_1, x_2, \ldots, x_n]$ be a polynomial over A.
Then for every $\bar{a} \in R^n$ there is a $\bar{b} \in R^n$ such that

- $b_i = 0$ or $b_i = a_i$
- $b_i = a_i$ for at most $\mathbf{r}^{\mathbf{r}^{\cdots^{\mathbf{r}^{\mathbf{k}}}}}$ many i-s (there are k-many r-s in the tower)
- $f(\bar{a}) = f(\bar{b})$

G. Horváth

same bound, simpler proof for groups and rings

Nilpotent rings

Let $F(\bar{a}) = F(a_1, \ldots, a_n) = b$.

For $H \subseteq \{1, 2, \ldots, n\}$ let $a_H = \begin{cases} a_i \text{ if} & i \in H \\ 0 \text{ if} & i \notin H \end{cases}$

$$\varphi(H) = \text{see board}$$

$$\overline{\varphi}(H) = \sum_{X \subseteq H} \varphi(X)$$

$$f(x) = \sum_{H} \varphi(H) \prod_{i \in H} x_i$$

Clearly , $\overline{\varphi}(H) = F(\overline{a}_H)$

recall

$\overline{\varphi}(H) = \sum_{X \subseteq H} \varphi(X)$ and $f(x) = \sum_{H} \varphi(H) \prod_{i \in H} x_i$

recall

$\overline{\varphi}(H) = \sum_{X \subseteq H} \varphi(X)$ and $f(x) = \sum_{H} \varphi(H) \prod_{i \in H} x_i$

$$f(\overline{1}) = \sum \varphi(X) = \overline{\varphi}(\{1, \ldots, n\}) = F(\bar{a})$$

$$f(\chi(H)) = \sum_{X \subseteq H} \varphi(X) = \overline{\varphi}(H) = F(\bar{a}_H)$$

recall

$\overline{\varphi}(H) = \sum_{X \subseteq H} \varphi(X)$ and $f(x) = \sum_{H} \varphi(H) \prod_{i \in H} x_i$

$$f(\overline{1}) = \sum \varphi(X) = \overline{\varphi}(\{1, \ldots, n\}) = F(\bar{a})$$
$$f(\chi(H)) = \sum_{X \subseteq H} \varphi(X) = \overline{\varphi}(H) = F(\bar{a}_H)$$

$g(\bar{x}) = f(\bar{x}) - f(\overline{1})$
$g(\overline{1}) = 0$
$g(\chi(H)) = 0 \iff F(\bar{a}_H) = b$

Chevalley's Theorem, again

Recall

Let $A_1, \ldots, A_n$ be subsets of F_p, the p-element field, and $f \in F_p[x_1, \ldots, x_n]$ such that

$$\sum_{i=1}^{n} (|A_i| - 1) > (p-1) \deg f.$$

If the set $\{a \in A_1 \times \cdots \times A_n | f(a) = 0\}$ is not empty, then it has at least two different elements.

Chevalley's Theorem, again

Recall

Let $A_1, \ldots, A_n$ be subsets of F_p, the p-element field, and $f \in F_p[x_1, \ldots, x_n]$ such that

$$\sum_{i=1}^{n}(|A_i| - 1) > (p-1)\deg f.$$

If the set $\{a \in A_1 \times \cdots \times A_n | f(a) = 0\}$ is not empty, then it has at least two different elements.

Apply Lemma for $g(\bar{x})$ and $A_i = \{0, 1\}$. $g(\bar{1}) = 0$.
If $n > k(p-1)$, there is an other root.