MUIC Applied Math Seminar

Number Theory in Function Fields

Chatchawan Panraksa

Science Division
Mahidol University International College

chatchawan.pan@mahidol.edu

October 9, 2019

Theorem

Let $f(x) \in \mathbb{C}[x]$. Then $f(x)$ has at least one complex root.

Theorem (Combinatorial Nullstellensatz, Noga Alon, 1999)

Let F be a field, and let $f = f(x_1, \ldots, x_n)$ be a polynomial in $F[x_1, \ldots, x_n]$. Suppose the degree $\deg(f)$ of f is $\sum_{i=1}^{n} t_i$, where each t_i is a nonnegative integer, and suppose the coefficient of $\prod_{i=1}^{n} x_i^{t_i}$ in f is nonzero. Then, if $S_1, \ldots, S_n$ are subsets of F with $|S_i| > t_i$, there are $s_1 \in S_1, s_2 \in S_2, \ldots, s_n \in S_n$ so that

$$f(x_1, \ldots, s_n) \neq 0.$$

Cauchy-Davenport Theorem

Theorem (Cauchy-Davenport)

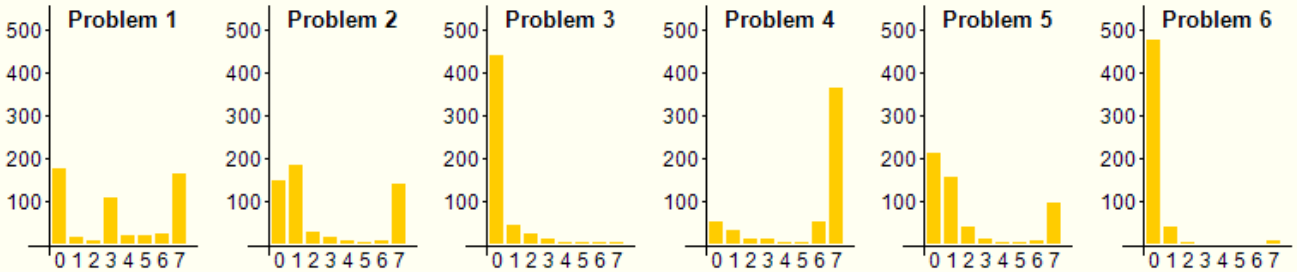
Given A, B non-empty subsets of $\mathbb{Z}_p$ for a prime p, then

$$|A + B| \geq \min\{p, |A| + |B| - 1\}.$$

(Almost) the Hardest IMO!

◀ 48TH IMO 2007 ▶

COUNTRY RESULTS • INDIVIDUAL RESULTS • **STATISTICS**

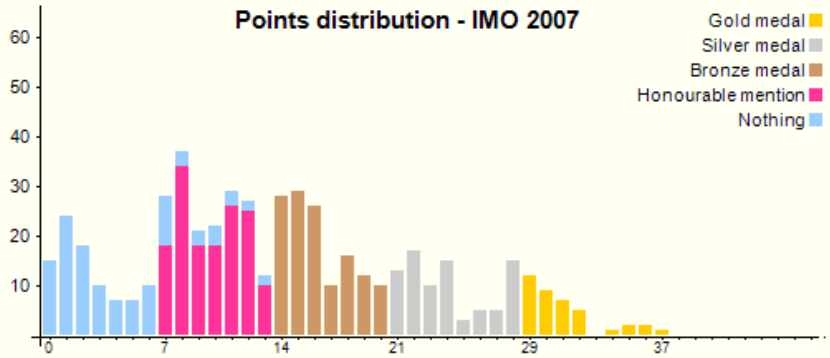


	P1	P2	P3	P4	P5	P6
Num(P# = 0)	176	147	437	51	210	473
Num(P# = 1)	13	181	42	30	155	40
Num(P# = 2)	8	26	23	9	38	2
Num(P# = 3)	105	15	11	9	10	0
Num(P# = 4)	18	5	3	3	3	0
Num(P# = 5)	18	1	1	4	4	0
Num(P# = 6)	21	8	1	51	6	0
Num(P# = 7)	161	137	2	363	94	5
Mean(P#)	3.383	2.519	0.304	5.681	1.898	0.152
Max(P#)	7	7	7	7	7	7
σ(P#)	2.916	2.851	0.868	2.456	2.592	0.735
Corr(P#, Sum)	0.747	0.767	0.452	0.632	0.767	0.361
Corr(P#, P1)		0.385	0.275	0.362	0.428	0.201
Corr(P#, P2)	0.385		0.295	0.337	0.521	0.216
Corr(P#, P3)	0.275	0.295		0.126	0.366	0.133
Corr(P#, P4)	0.362	0.337	0.126		0.288	0.110
Corr(P#, P5)	0.428	0.521	0.366	0.288		0.297
Corr(P#, P6)	0.201	0.216	0.133	0.110	0.297	

(Almost) the Hardest IMO!

◀ 48TH IMO 2007 ▶

COUNTRY RESULTS • INDIVIDUAL RESULTS • STATISTICS



Contestant [♀♂][←]	Country	P1	P2	P3	P4	P5	P6	Total	Rank	Award
Peter Scholze	Germany	7	7	1	7	7	7	36	2	Gold medal
Pietro Vertechi	Italy	7	7	0	7	7	7	35	4	Gold medal
Iurie Boreico	Republic of Moldova	5	0	0	7	7	7	26	60	Silver medal
Konstantin Matveev	Russian Federation	7	7	2	7	7	7	37	1	Gold medal
Danylo Radchenko	Ukraine	7	7	0	7	7	7	35	4	Gold medal
Shayan Dashmiz	Islamic Republic of Iran	3	7	0	7	7	2	26	60	Silver medal

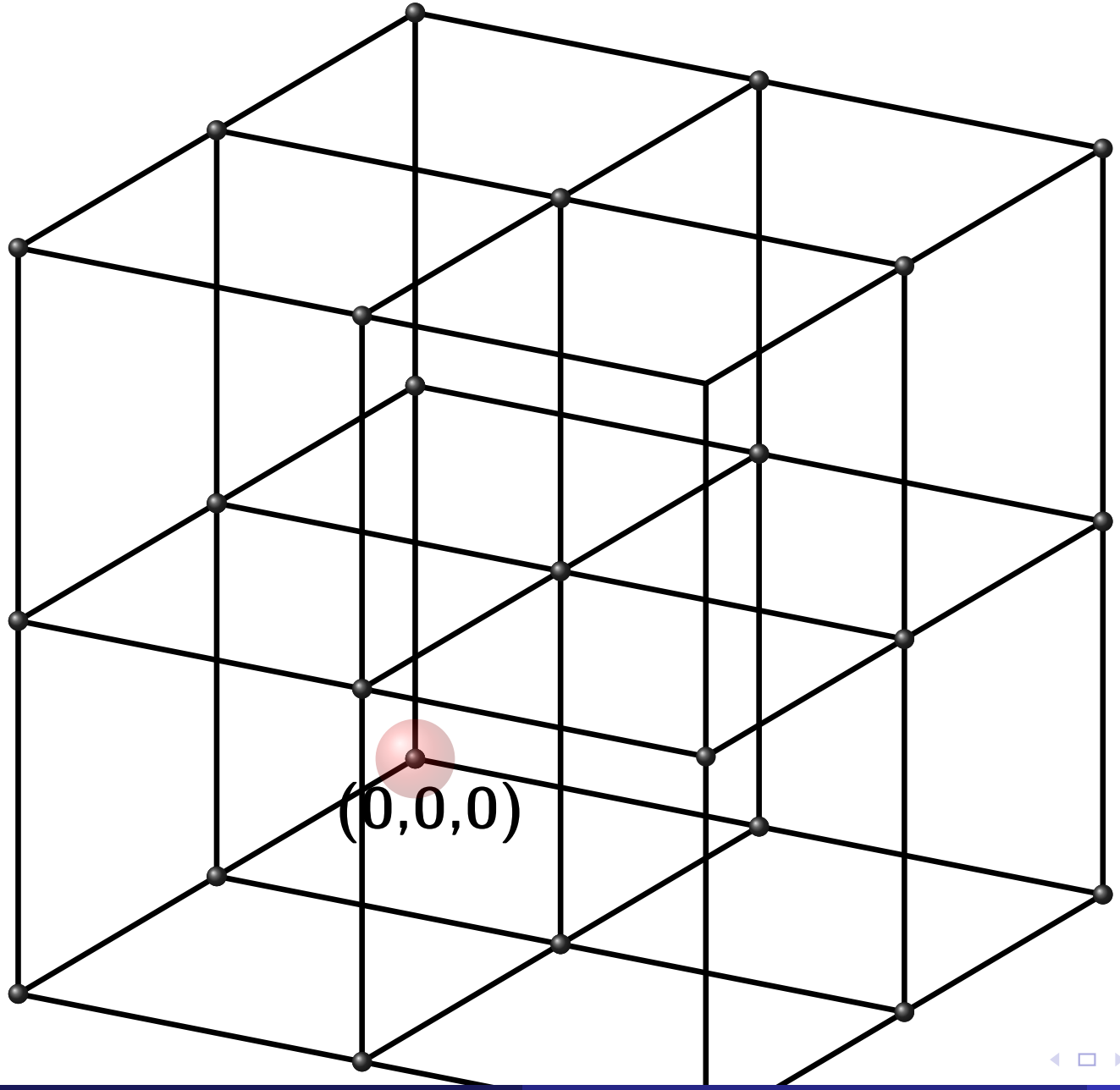
IMO 2007 Problem 6

IMO 2007 Problem 6: Let n be a positive integer. Consider

$$S = \{(x, y, z) \mid x, y, z \in \{0, 1, \ldots, n\}, x + y + z > 0\}$$

as a set of $(n+1)^3 - 1$ points in $3D$ space. Determine the smallest number of planes, the union of which contains S but does not include $(0, 0, 0)$.

3D Lattices



Definition

A **radical** of a positive integer is a product of its distinct prime factors.
NOTATION: $n = p_1^{k_1} p_1^{k_1} \dots p_m^{k_m}$
radical of n is $rad(n) = p_1 p_2 \dots p_m$.
$rad(1) := 1$

Definition

A **radical** of a positive integer is a product of its distinct prime factors.
NOTATION: $n = p_1^{k_1} p_1^{k_1} \dots p_m^{k_m}$
radical of n is $rad(n) = p_1 p_2 \dots p_m$.
$rad(1) := 1$

Example

$rad(5) = 5$

Definition

A **radical** of a positive integer is a product of its distinct prime factors.
NOTATION: $n = p_1^{k_1} p_1^{k_1} \dots p_m^{k_m}$
radical of n is $rad(n) = p_1 p_2 \dots p_m$.
$rad(1) := 1$

Example

$rad(5) = 5$
$rad(345744)$

Definition

A **radical** of a positive integer is a product of its distinct prime factors.
NOTATION: $n = p_1^{k_1} p_1^{k_1} \dots p_m^{k_m}$
radical of n is $rad(n) = p_1 p_2 \dots p_m$.
$rad(1) := 1$

Example

$rad(5) = 5$
$rad(345744) = rad(2^4 \cdot 3^2 \cdot 7^4)$

Definition

A **radical** of a positive integer is a product of its distinct prime factors.
NOTATION: $n = p_1^{k_1} p_1^{k_1} \dots p_m^{k_m}$
radical of n is $rad(n) = p_1 p_2 \dots p_m$.
$rad(1) := 1$

Example

$rad(5) = 5$
$rad(345744) = rad(2^4 \cdot 3^2 \cdot 7^4) = 2 \cdot 3 \cdot 7$

Definition

A **radical** of a positive integer is a product of its distinct prime factors.
NOTATION: $n = p_1^{k_1} p_1^{k_1} \dots p_m^{k_m}$
radical of n is $rad(n) = p_1 p_2 \dots p_m$.
$rad(1) := 1$

Example

$rad(5) = 5$
$rad(345744) = rad(2^4 \cdot 3^2 \cdot 7^4) = 2 \cdot 3 \cdot 7 = 42$

Definition

A **radical** of a positive integer is a product of its distinct prime factors.
NOTATION: $n = p_1^{k_1} p_1^{k_1} \dots p_m^{k_m}$
radical of n is $rad(n) = p_1 p_2 \dots p_m$.
$rad(1) := 1$

Example

$rad(5) = 5$
$rad(345744) = rad(2^4 \cdot 3^2 \cdot 7^4) = 2 \cdot 3 \cdot 7 = 42$
$rad(1868347265625)$

Definition

A **radical** of a positive integer is a product of its distinct prime factors.
NOTATION: $n = p_1^{k_1} p_1^{k_1} \dots p_m^{k_m}$
radical of n is $rad(n) = p_1 p_2 \dots p_m$.
$rad(1) := 1$

Example

$rad(5) = 5$
$rad(345744) = rad(2^4 \cdot 3^2 \cdot 7^4) = 2 \cdot 3 \cdot 7 = 42$
$rad(1868347265625) = rad(3^{14} \cdot 5^8)$

Definition

A **radical** of a positive integer is a product of its distinct prime factors.
NOTATION: $n = p_1^{k_1} p_1^{k_1} \dots p_m^{k_m}$
radical of n is $rad(n) = p_1 p_2 \dots p_m$.
$rad(1) := 1$

Example

$rad(5) = 5$
$rad(345744) = rad(2^4 \cdot 3^2 \cdot 7^4) = 2 \cdot 3 \cdot 7 = 42$
$rad(1868347265625) = rad(3^{14} \cdot 5^8) = 3 \cdot 5$

Definition

A **radical** of a positive integer is a product of its distinct prime factors.
NOTATION: $n = p_1^{k_1} p_1^{k_1} \dots p_m^{k_m}$
radical of n is $rad(n) = p_1 p_2 \dots p_m$.
$rad(1) := 1$

Example

$rad(5) = 5$
$rad(345744) = rad(2^4 \cdot 3^2 \cdot 7^4) = 2 \cdot 3 \cdot 7 = 42$
$rad(1868347265625) = rad(3^{14} \cdot 5^8) = 3 \cdot 5 = 15$

How about raising the power of $rad(abc)$?

Conjecture ($abc-$Conjecture, Masser and Oestelé 1988))

For every $\epsilon > 0$, there are only finite many triple (a, b, c) of coprime positve integers with $a + b = c$ such that:

$$c > rad(abc)^{1+\epsilon}.$$

How about raising the power of $rad(abc)$?

Conjecture ($abc-$Conjecture, Masser and Oestelé 1988))

For every $\epsilon > 0$, there are only finite many triple (a, b, c) of coprime positve integers with $a + b = c$ such that:

$$c > rad(abc)^{1+\epsilon}.$$

Equivalently, we have

Conjecture ($abc-$Conjecture)

For every $\epsilon > 0$, there exists a constant K_ϵ such that for all triples (a, b, c) of coprime positve integers, with $a + b = c$ such that

$$c < K_\epsilon rad(abc)^{1+\epsilon}.$$

abc Theorem for Function Fields

Theorem (Mason-Stothers Theorem, 1981)

Let K be a field of characteristic 0. If $a(t), b(t), c(t)$ are nonzero polynomials in $K[t]$ with $a(t) + b(t) = c(t)$ and $\gcd(a(t), b(t), c(t)) = 1$, then

$$\max\{\deg a, \deg b, \deg c\} \leq rad(abc) - 1.$$

Example

$a(t) = 1, b(t) = t^n, c(t) = t^n + 1$

abc Theorem for Function Fields

Theorem (Mason-Stothers Theorem, 1981)

Let K be a field of characteristic 0. If $a(t), b(t), c(t)$ are nonzero polynomials in $K[t]$ with $a(t) + b(t) = c(t)$ and $\gcd(a(t), b(t), c(t)) = 1$, then

$$\max\{\deg a, \deg b, \deg c\} \leq rad(abc) - 1.$$

Example

$a(t) = 1, b(t) = t^n, c(t) = t^n + 1$
$\max\{\deg a, \deg b, \deg c\} = n$

abc Theorem for Function Fields

Theorem (Mason-Stothers Theorem, 1981)

Let K be a field of characteristic 0. If $a(t), b(t), c(t)$ are nonzero polynomials in $K[t]$ with $a(t) + b(t) = c(t)$ and $\gcd(a(t), b(t), c(t)) = 1$, then

$$\max\{\deg a, \deg b, \deg c\} \leq rad(abc) - 1.$$

Example

$a(t) = 1, b(t) = t^n, c(t) = t^n + 1$
$\max\{\deg a, \deg b, \deg c\} = n$
$rad(abc) = t(t^n + 1),$

abc Theorem for Function Fields

Theorem (Mason-Stothers Theorem, 1981)

Let K be a field of characteristic 0. If $a(t), b(t), c(t)$ are nonzero polynomials in $K[t]$ with $a(t) + b(t) = c(t)$ and $\gcd(a(t), b(t), c(t)) = 1$, then

$$\max\{\deg a, \deg b, \deg c\} \leq rad(abc) - 1.$$

Example

$a(t) = 1, b(t) = t^n, c(t) = t^n + 1$
$\max\{\deg a, \deg b, \deg c\} = n$
$rad(abc) = t(t^n + 1)$, $\deg rad(abc) = n + 1$

Fermat's Last Theorem for Polynomials

Theorem

There are no nonzero polynomials $x(t), y(t), z(t) \in \mathbb{C}[t]$ *such that*

$$x(t)^n + y(t)^n = z(t)^n, \text{ for } n > 2.$$

"Mathematicians are like Frenchmen: whatever you say to them they translate into their own language and forthwith it is something entirely different."

Johann Wolfgang von Goethe, 1749 – 1832

Thank You!