A talk given at Combinatorial and Additive Number Theory
(Univ. of Graz, Austria, Jan. 4-8, 2016)

Some new problems and results in combinatorial and additive number theory

Zhi-Wei Sun

Nanjing University
Nanjing 210093, P. R. China
zwsun@nju.edu.cn
http://math.nju.edu.cn/∼zwsun

Jan. 6, 2016

Abstract

In this talk we introduce various new conjectures of the speaker in combinatorial and additive number theory as well as related progress. We mainly focus on additive problems related to permutations and combinatorial properties of the prime-counting function $\pi(x)$. For example, we conjecture that for any finite subset A of an abelian group G with $|A| = n > 3$. there is a numbering $a_1, \ldots, a_n$ of all the n elements of A such that

$$a_1+a_2+a_3,\ a_2+a_3+a_4,\ \ldots,\ a_{n-2}+a_{n-1}+a_n,\ a_{n-1}+a_n+a_1,\ a_n+a_1+a_2$$

are pairwise distinct, and confirm this when G is torsion-free. Our problems on the prime-counting function depend on some exact values of $\pi(x)$, in this direction we show that for any integer $m > 4$ this is a positive integer n such that $\pi(mn) = m + n$.

Part I. Additive Problems and Results involving Permutations

Erdős-Heilbronn Conjecture

Erdős-Heilbronn Conjecture (1964). Let p be a prime and let $A \subseteq \mathbb{Z}_p$. Then

$$|2^\wedge A| \geqslant \min\{p,\ 2|A|-3\},$$

where

$$n^\wedge A := \{a_1 + \cdots + a_n :\ a_1, \ldots, a_n \text{ are distinct elements of } A\}.$$

Difficulty. Unlike $\mathbb{Z}$, the field $\mathbb{Z}_p$ has no suitable ordering. Direct construction does not work!

Dias da Silva-Hamidoune Theorem [Bull. London Math. Soc., 1994]. Let F be any field and let $p(F)$ be the additive order of the multiplicative identity of F. For any finite $A \subseteq F$, we have

$$|n^\wedge A| \geqslant \min\{p(F),\ n(|A|-n)+1\}.$$

Method: Exterior algebras!

Alon-Nathanson-Ruzsa Theorem

Alon-Nathanson-Ruzsa Theorem (1996). For finite nonempty subsets $A_1, \ldots, A_n$ of a field F with $|A_1| < \cdots < |A_n|$, we have

$$|A_1 \dot{+} \cdots \dot{+} A_n| \geqslant \min\left\{p(F),\ \sum_{i=1}^{n}(|A_i| - i) + 1\right\},$$

where

$$A_1 \dot{+} \cdots \dot{+} A_n := \{a_1 + \cdots + a_n :\ a_1 \in A_1, \ldots, a_n \in A_n \text{ are distinct}\}.$$

Method: The polynomial method via Combinatorial Nullstellensatz.

Remark. In the case $|A_1| = \cdots = |A_n| = k \geqslant n$, we can choose $A_i' \subseteq A_i$ with $|A_i'| = k - n + i$ and then apply the ANR theorem to get

$$|A_1 \dot{+} \cdots \dot{+} A_n| \geqslant |A_1' \dot{+} \cdots \dot{+} A_n'|$$

$$\geqslant \min\left\{p(F),\ \sum_{i=1}^{n}(|A_i|' - i) + 1\right\} = \min\{p(F),\ (k-n)n + 1\}.$$

Linear extension of the Erdős-Heilbronn conjecture

For a prime p, $\mathbb{Z}_p$ is an additively cyclic group. On the other hand, $\mathbb{Z}_p$ is a field which involves both addition and multiplication.

A Conjecture of Z. W. Sun [Finite Fields Appl. 2008]. Let $a_1, \ldots, a_n$ be nonzero elements of a field F. If $p(F) \neq n+1$, then for any finite $A \subseteq F$ we have

$$\begin{aligned}&|\{a_1x_1 + \cdots + a_nx_n:\ x_1, \ldots, x_n \text{ are distinct elements of } A\}| \\ &\qquad \geqslant \min\{p(F) - \delta,\ n(|A| - n) + 1\},\end{aligned}$$

where

$$\delta = [\![n = 2\ \&\ a_1 + a_2 = 0]\!] = \begin{cases} 1 & \text{if } n = 2\ \&\ a_1 + a_2 = 0, \\ 0 & \text{otherwise.} \end{cases}$$

Difficulty: We cannot apply the Combinatorial Nullstellensatz directly, for, the related coefficient involving $a_1, \ldots, a_n$ might be zero. (In the case $n = 2$, the conjecture holds via a result of H. Pan and Sun [JCTA 2002].)

Prizes: I'd like to offer 200 US dollars for a complete proof.

Linear extension of the Erdős-Heilbronn conjecture

Theorem (Z. W. Sun and L. L. Zhao, J. Combin. Theory Ser. A 119(2012)). The conjecture (posed by Sun) holds if $p(F) \geqslant n(3n-5)/2$.

Remark. Sun and Zhao also noted that the conjecture holds for $n = 3$.

Theorem. (Z.-W. Sun and L. L. Zhao, JCTA 119(2012)) Let n be a positive integer, and let F be a field with $p(F) \geqslant (n-1)^2$. Let $a_1, \ldots, a_n \in F^* = F \setminus \{0\}$, and suppose that $A_i \subseteq F$ and $|A_i| \geqslant 2n-2$ for $i = 1, \ldots, n$. Then, for the set

$$C = \{a_1x_1 + \cdots + a_nx_n :\ x_1 \in A_1, \ldots, x_n \in A_n, \text{ and } x_i \neq x_j \text{ if } i \neq j\}$$

we have

$$|C| \geqslant \min\{p(F) - [\![n = 2 \ \&\ a_1 + a_2 = 0]\!],\ |A_1| + \cdots + |A_n| - n^2 + 1\}.$$

An easy observation

Theorem (Sun, 2013-08) Let $a_1, \ldots, a_n$ be a monotonic sequence of n distinct real numbers. Then there is a permutation $b_1, \ldots, b_n$ of $a_1, \ldots, a_n$ with $b_1 = a_1$ such that

$$|b_1 - b_2|,\ |b_2 - b_3|,\ \ldots,\ |b_{n-1} - b_n|$$

are pairwise distinct.

Proof. We assume $a_1 < a_2 < \ldots < a_n$ without loss of generality. If $n = 2k$ is even, then the permutation

$$(b_1, \ldots, b_n) = (a_1, a_{2k}, a_2, a_{2k-1}, \ldots, a_{k-1}, a_{k+2}, a_k, a_{k+1})$$

meets our purpose since

$$a_{2k} - a_1 > a_{2k} - a_2 > a_{2k-1} - a_2 > \ldots > a_{k+2} - a_k > a_{k+1} - a_k.$$

When $n = 2k - 1$ is odd, the permutation

$$(b_1, \ldots, b_n) = (a_1, a_{2k-1}, a_2, a_{2k-2}, \ldots, a_{k-1}, a_{k+1}, a_k)$$

meets the requirement since

$$a_{2k-1} - a_1 > a_{2k-1} - a_2 > a_{2k-2} - a_2 > \ldots > a_{k+1} - a_{k-1} > a_{k+1} - a_k.$$

A conjecture on permutations

Corollary. There is a circular permutation $q_1, \ldots, q_n$ of the first n primes $p_1, \ldots, p_n$ with $q_1 = p_1 = 2$ and $q_n = p_n$ such that the n distances

$$|q_1 - q_2|,\ |q_2 - q_3|,\ \ldots,\ |q_{n-1} - q_n|,\ |q_n - q_1|$$

are pairwise distinct.

Conjecture (Sun, 2013-09-01). Let $a_1, a_2, \ldots, a_n$ be n distinct real numbers. Then there is a permutation $b_1, \ldots, b_n$ of $a_1, \ldots, a_n$ with $b_1 = a_1$ such that the $n-1$ numbers

$$|b_1 - b_2|,\ |b_2 - b_3|,\ \ldots,\ |b_{n-1} - b_n|$$

are pairwise distinct.

Francesco Monopoli [Electron. J. Combin. 2015]: The conjecture holds if the set $A = \{a_1, a_2, \ldots, a_n\}$ forms an arithmetic progression.

Circular permutations of quadratic residues (I)

Conjecture (Sun, 2013-09). For any prime $p = 2n + 1 > 13$, there is a circular permutation $a_1, \ldots, a_n$ of the $(p-1)/2 = n$ quadratic residues modulo p such that all the n adjacent sums

$$a_1 + a_2,\ a_2 + a_3,\ \ldots,\ a_{n-1} + a_n,\ a_n + a_1$$

are quadratic residues (or quadratic nonresidues) modulo p. Also, for any prime $p = 2n + 1 > 5$, there is a circular permutation $b_1, \ldots, b_n$ of the $(p-1)/2 = n$ quadratic residues modulo p such that all the n adjacent differences

$$b_1 - b_2,\ b_2 - b_3,\ \ldots,\ b_{n-1} - b_n,\ b_n - b_1$$

are quadratic residues (or quadratic nonresidues) modulo p.

Later this was confirmed by N. Alon and J. Bourgain in the paper *Additive patterns in multiplicative subgroups* in Geom. Funct. Anal. 24(2014), 721-739. Below is a lemma.

B. Jacobson (JCTB 1980): For each $k > 1$, any 2-connected k-regular graph with at most $3k$ vertices is Hamiltonian.

Alon and Bourgain's general result

Theorem (Alon & Bourgain). There exists a constant $c > 0$ such that for any prime power q and For any multiplicative subgroup A of the finite field $\mathbb{F}_q$ with

$$|A| = d \geq cq^{3/4} \frac{\sqrt{(\log q)(\log\log\log q)}}{\log\log q},$$

there is a numbering $a_1, a_2, \ldots, a_d$ of the elements of A such that

$$a_1 + a_2,\ a_2 + a_3,\ \ldots,\ a_{d-1} + a_d,\ a_d + a_1$$

all belong to A.

Their tools include algebraic graph theory and probability method.

A Key Lemma (Krivelevich & Sudakov). Let G be a d-regular graph with n vertices. If n is large enough, and the absolute value of each nontrivial eigenvalue of the adjacency matrix of G is smaller than $d(\log\log n)^2/(1000(\log n)\log\log\log n)$, then G is a Hamiltonian graph.

Circular permutations of quadratic residues (II)

Theorem (Sun, Oct. 2013). Let $\mathbb{F}_q$ be a finite field with $q = 2n + 1 > 2^{66}$ elements. Set

$$S = \{a^2 : \ a \in \mathbb{F}_q^* = \mathbb{F}_q \setminus \{0\}\} \ \text{ and } \ T = F_q^* \setminus S.$$

Then, there is a circular permutation $a_1, \ldots, a_n$ of all the elements of S such that

$$\{a_1 + a_2, \ a_2 + a_3, \ \ldots, \ a_{n-1} + a_n, \ a_n + a_1\} = S \ \ (\text{or } T).$$

Also, there is a circular permutation $a_1, \ldots, a_n$ of all the elements of S such that

$$\{a_1 - a_2, \ a_2 - a_3, \ \ldots, \ a_{n-1} - a_n, \ a_n - a_1\} = S \ \ (\text{or } T).$$

Circular permutations of quadratic residues (II)

Proof. Let $\varepsilon \in \{\pm 1\}$, and $R = S$ or T. Choose an element $a \in T$. By a result of Wenbao Han [Acta Math. Sinica 32(1989)], there exists a primitive root g of $\mathbb{F}_q$ such that $1 + \varepsilon g^2$ (or $a + \varepsilon a g^2$) is also a primitive root and hence an element of T. So there is a primitive root g with $1 + \varepsilon g^2 \in R$. Set $a_i = g^{2i}$ for $i = 1, \ldots, n$. Then

$$\{a_1, a_2, \ldots, a_n\} = S \quad \text{and} \quad \{a_1 + \varepsilon a_2, \ldots, a_n + \varepsilon a_1\} = R.$$

Note that

$$g^{2i} + \varepsilon g^{2(i+1)} = g^{2i}(1 + \varepsilon g^2) \in R \quad \text{for all } i = 1, \ldots, n.$$

Remark. 2^{66} in the theorem can be reduced to 13 via a complicated analysis.

Two conjectures on primitive roots

Conjecture (Z.-W. Sun, 2014-04-23). Every prime p has a primitive root $0 < g < p$ with $g - 1$ a square.

Remark. This has been verified for all primes $p < 10^{10}$.

Conjecture (joint with Q.-H. Hou, 2013-09-05) Let $\mathbb{F}_q$ be the finite field with $q > 7$ elements. Then there is a numbering $a_1, \ldots, a_q$ of the elements of $\mathbb{F}_q$ such that all the q sums

$$a_1 + a_2,\ a_2 + a_3,\ \ldots,\ a_{q-1} + a_q,\ a_q + a_1$$

are generators of the cyclic group $\mathbb{F}_q^* = \mathbb{F}_q \setminus \{0\}$ (i.e., primitive elements of $\mathbb{F}_q$).

Remark. We have verified this for all primes $q < 545$.

A conjecture related to Snevily's conjecture

Snevily's Conjecture (proved by Arsovski in 2011). Let G be any abelian group of odd order, and let A and B be finite subsets of G with $|A| = |B| = n$. Then there is a numbering $a_1, \ldots, a_n$ of the n elements of A and a numbering $b_1, \ldots, b_n$ of the n elements of B such that $a_1 + b_1,\ a_2 + b_2,\ \ldots,\ a_n + b_n$ are pairwise distinct.

Conjecture (Sun, 2013-09-03) Let A be an n-subset of a finite additive abelian group G with $2 \nmid n$ or $n \nmid |G|$.
(i) There always exists a numbering $a_1, a_2, \ldots, a_n$ of all the n elements of A such that the n sums

$$a_1 + a_2,\ a_2 + a_3,\ \ldots,\ a_{n-1} + a_n,\ a_n + a_1$$

are pairwise distinct.
(ii) In the case $3 < n < |G|$, there is a numbering $a_1, a_2, \ldots, a_n$ of all the n elements of A such that the n differences

$$a_1 - a_2,\ a_2 - a_3,\ \ldots,\ a_{n-1} - a_n,\ a_n - a_1$$

are pairwise distinct.

A conjecture involving $a_i + 2a_{i+1}$

Conjecture (2013-09-20) Let A be a finite subset of an additive abelian group G with $|A| = n > 3$.

(i) If G is finite with $|G| \not\equiv 0 \pmod 3$, then there is a numbering $a_1, \ldots, a_n$ of all the elements of A such that the n sums

$$a_1 + 2a_2,\ a_2 + 2a_3,\ \ldots,\ a_{n-1} + 2a_n,\ a_n + 2a_1$$

are pairwise distinct.

(ii) There always exist two numberings $a_1, \ldots, a_n$ and $b_1, \ldots, b_n$ of all the elements of A such that the n sums

$$a_1 + 2b_1,\ a_2 + 2b_2,\ \ldots,\ a_{n-1} + 2b_{n-1},\ a_n + 2b_n$$

are pairwise distinct.

Remark. When $A = \{a_1, \ldots, a_n\}$ forms an abelian group of the form $(\mathbb{Z}/3\mathbb{Z})^r$, the n elements

$$a_1+2a_2 = a_1-a_2,\ a_2+2a_3 = a_2-a_3,\ \ldots,\ a_{n-1}+2a_n = a_{n-1}-a_n,\ a_n+2a_1$$

cannot be pairwise distinct. We have proved part (i) for any torsion-free abelian group G, and part (ii) for $n \leqslant 4$.

A theorem involving three subsets

Motivated by Snevily's conjecture, we obtained the following result involving three subsets.

Theorem (Sun, [Math. Res. Lett. 15(2008)]). Let G be an abelian group with cyclic torsion group, and let A, B, C be subsets of G with $|A| = |B| = |C| = n$. Then, there is a numbering $a_1, \ldots, a_n$ of the n elements of A, a numbering $b_1, \ldots, b_n$ of the elements of B, and a numbering $c_1, \ldots, c_n$ of the elements of C such that $a_1 + b_1 + c_1, \ldots, a_n + b_n + c_n$ are pairwise distinct.

Corollary. Let N be any positive integer. For the $N \times N \times N$ Latin cube over Z/NZ formed by the Cayley addition table, each $n \times n \times n$ subcube with $n \leqslant N$ contains a Latin transversal.

Conjecture (Sun, [Math. Res. Lett. 15(2008)]). Every $n \times n \times n$ Latin cube contains a Latin transversal.

Remark. In 1967 Ryser conjectured that every Latin square of odd order has a Latin transversal.

A conjecture for general abelian groups

Conjecture (Sun, 2013-09-04). Let G be any abelian group, and let A be a finite subset of G with $|A| = n > 3$. Then there is a numbering $a_1, \ldots, a_n$ of all the n elements of A such that

$$a_1+a_2+a_3,\ a_2+a_3+a_4,\ \ldots,\ a_{n-2}+a_{n-1}+a_n,\ a_{n-1}+a_n+a_1,\ a_n+a_1+a_2$$

are pairwise distinct.

Remark. For a finite abelian group $G = \{a_1, a_2, \ldots, a_n\}$, it is easy to see that $2(a_1 + \cdots + a_n) = 0$.

Theorem (Sun, 2013-09-19). The conjecture holds for any *torsion-free* abelian group G.

Remark. (1) I became too tired and ill immediately after I spent the whole day to finish the proof of this theorem.
(2) The conjecture is even open for cyclic groups of prime orders. I'd like to offer a **prize** of 500 US dollars for the first complete proof of the conjecture.

Part II. Combinatorial properties of primes

The prime-counting function $\pi(x)$ and the n-th prime p_n

Primes: 2, 3, 5, 7, 11, 13, 17, 19, 23, 29, 31, 37, 41, 43, 47, ...

The prime-counting function:

$$\pi(x) = |\{p \leqslant x : \; p \text{ is prime}\}|,$$

i.e., $\pi(x)$ is the number of primes not exceeding x.

For $n = 1, 2, 3, \dots$ let p_n denote **the n-th prime**.

For example,

$$p_1 = 2, \; p_2 = 3, \; p_3 = 5, \; p_4 = 7, \; p_5 = 11, \; p_6 = 13.$$

Primes are generally *irregular*. No closed formula for $\pi(x)$ or p_n has been found.

By the Prime Number Theorem,

$$\pi(x) \sim \frac{x}{\log x} \quad \text{and} \quad p_n \sim n \log n.$$

An easy result on $\pi(x)$

Proposition. For any positive integer m, there is a positive integer $n \leqslant m$ such that $\pi(m+n) = n$.

Proof. Let $f(n) = \pi(m+n) - n$. Clearly,

$$f(1) = \pi(m+1) - 1 \geqslant 0, \; f(m) = \pi(2m) - m \leqslant 0,$$

and

$$\begin{aligned} f(n) - f(n+1) =& \pi(m+n) - n - (\pi(m+n+1) - (n+1)) \\ =& \pi(m+n) + 1 - \pi(m+n+1) \in \{0, 1\}. \end{aligned}$$

So, for some $1 \leqslant n \leqslant m$ we have $f(n) = 0$, i.e., $\pi(m+n) = n$.

An easy result on $\pi(x)$

Proposition. For any positive integer m, there is a positive integer $n \leqslant m$ such that $\pi(m+n) = n$.

Proof. Let $f(n) = \pi(m+n) - n$. Clearly,

$$f(1) = \pi(m+1) - 1 \geqslant 0, \ f(m) = \pi(2m) - m \leqslant 0,$$

and

$$\begin{aligned} f(n) - f(n+1) =& \pi(m+n) - n - (\pi(m+n+1) - (n+1)) \\ =& \pi(m+n) + 1 - \pi(m+n+1) \in \{0, 1\}. \end{aligned}$$

So, for some $1 \leqslant n \leqslant m$ we have $f(n) = 0$, i.e., $\pi(m+n) = n$.

Another Proof. Let n be the number of primes not exceeding the m-th composite number q. Then $m+n = q-1$ and hence $\pi(m+n) = \pi(q-1) = \pi(q) = n$.

Golomb's Theorem

Theorem (S. Golomb, 1962). For any integer $m > 1$, there is an integer $n > 1$ such that $n/\pi(n) = m$.
Proof. If $m = 2$ we may take $n = 2$. Below we assume $m > 2$. By the Prime Number Theorem,

$$\frac{n}{\pi(n)} \sim \log n \to +\infty \quad \text{as } n \to +\infty.$$

Take the least integer $n > 1$ such that $n/\pi(n) \geqslant m$. As $m > 2$, we have $n > 2$. Thus

$$\frac{n}{\pi(n)} \geqslant m > \frac{n-1}{\pi(n-1)}.$$

If n is prime, then

$$\frac{n}{\pi(n)} = \frac{(n-1)+1}{\pi(n-1)+1} \leqslant \frac{n-1}{\pi(n-1)}.$$

So n is composite and hence $n \geqslant m\pi(n) > n-1$. Thus $n/\pi(n) = m$.

My result on $\pi(x)$

Theorem (Sun, Ramanujan J.). (i) Let m be any positive integer. For the set

$$S_m := \left\{ a \in \mathbb{Z} :\ \pi(n) = \frac{n+a}{m} \text{ for some integer } n > 1 \right\},$$

we have

$$S_m = \{\ldots, -2, -1, \ldots, S(m)\},$$

where

$$S(m) = \max\{km - p_k :\ k \in \mathbb{Z}^+\} = \max\{km - p_k :\ k = 1, \ldots, \lfloor e^{m+1} \rfloor\}.$$

(ii) We have

$$(m-1)S(m+1) > mS(m) \quad \text{for any } m \in \mathbb{Z}^+.$$

Also,

$$\frac{e^{m-1}}{m-1} < S(m) < (m-1)e^{m+1} \quad \text{for all } m = 3, 4, \ldots,$$

and hence

$$\lim_{m \to +\infty} \sqrt[m]{S(m)} = e.$$

Consequences of the theorem

Corollary 1. Let $m > 0$ and $a \leqslant m^2 - m - 1$ be integers. Then there is an integer $n > 1$ with $\pi(n) = (n + a)/m$, i.e.,

$$\pi(mn - a) = n \quad \text{for some } n \in \mathbb{Z}^+.$$

Corollary 2. For any integer $m > 4$, there is a positive integer n such that $\pi(mn) = m + n$.

Corollary 3. For any integer $m > 3$, there is a positive integer n such that $\pi(mn) = F_m + n$, where $\{F_k\}_{k \geqslant 0}$ is the Fibonacci sequence.

Examples.

$$\pi(21 \times 179992154) = 21 + 179992154$$

and

$$\pi(16 \times 1600659) = F_{16} + 1600659.$$

On representations of positive rational numbers

Conjecture (Z.-W. Sun, 2015-07-03) The set

$$\left\{\frac{m}{n}:\ m,n\in\mathbb{Z}^+ \text{ and } p_m+p_n \text{ is a square}\right\}$$

contains any positive rational number r.

Remark. We have verified this for all those rational numbers $r=a/b$ with $a,b\in\{1,\ldots,200\}$. For example, $2=20/10$ with $p_{20}+p_{10}=71+29=10^2$ a square.

Conjecture (Z.-W. Sun, 2015-07-03) Any positive rational number r can be written as m/n with $m,n\in\mathbb{Z}^+$ such that $\pi(m)\pi(n)$ is a positive square.

Remark. We have verified this for $r=a/b$ with $a,b\in\{1,\ldots,60\}$. For example, $49/58=1076068567/1273713814$ with

$$\pi(1076068567)\pi(1273713814)=54511776\times63975626=59054424^2.$$

A conjecture related to additive chains

A (finite or infinite) strictly increasing sequence with the initial term 1 is called an **addition chain** if each term after the initial one can be written as the sum of two earlier (not necessarily distinct) terms. For example,

$$a(1)=1,\ a(2)=1+1=2,\ a(3)=2+2=4,$$
$$a(4)=4+2=6,\ a(5)=4+4=8,\ a(6)=8+6=14$$

is an addition chain for 14.

Conjecture (Sun, 2015-09-23). The sequence

$$f(n)=\pi\left(\frac{n(n+1)}{2}+1\right)\quad (n=1,2,3,\ldots)$$

is an additive chain.

Remark. I have verified that for each $n=2,\ldots,10^5$ we can write $f(n)$ as $f(k)+f(m)$ for some $k,m\in\mathbb{Z}^+$.

A curious conjecture on $\varphi(n)\pi(n^2)$ and $\sigma(n)\pi(n^2)$

For any positive integer n, define

$$\varphi(n) = |\{1 \leqslant a \leqslant n : (a, n) = 1\}| \text{ and } \sigma(n) = \sum_{d|n} d.$$

Conjecture (Sun, 2014-10-14). All the numbers

$$\varphi(n)\pi(n^2) \quad (n = 1, 2, 3, \ldots)$$

are pairwise distinct. Also, all the numbers

$$\sigma(n)\pi(n^2) \quad (n = 1, 2, 3, \ldots)$$

are pairwise distinct.

Remark. I have verified that all the numbers $\varphi(n)\pi(n^2)$ (or $\sigma(n)\pi(n^2)$) ($n = 1, 2, \ldots, 4 \times 10^5$) are indeed pairwise distinct! The conjecture suggests that the exact values of $\pi(n^2)$ ($n \in \mathbb{Z}^+$) might be related to multiplicative functions.

On representations involving $\pi(x^2)$

By the Prime Number Theorem,

$$\pi(x^2) \sim \frac{x^2}{\log x^2} = \frac{x^2}{2\log x} \text{ for } x \geqslant 2.$$

Conjecture (Sun, 2015-10-09). (i) Any positive integer n can be written as $\pi(x^2) + \pi(y^2/2)$, where x and y are positive integers.

(ii) Any positive integer n can be written as $\pi(x^2/2) + \pi(3y^2/2)$, where x and y are positive integers.

Remark. I have verified this for n up to 4×10^5. For example,

$$28 = 11 + 17 = \pi(6^2) + \pi\left(\frac{11^2}{2}\right)$$

and

$$100407 = 7554 + 92853 = \pi\left(\frac{392^2}{2}\right) + \pi\left(\frac{3 \times 894^2}{2}\right).$$

A conjecture on unit fractions involving primes

It is well known that any positive rational number can be written as the sum of some distinct unit fractions (via the simple fact $1/n = 1/(n+1) + 1/(n(n+1))$). For example,

$$\frac{2}{3} = \frac{1}{3} + \frac{1}{3} = \frac{1}{3} + \left(\frac{1}{4} + \frac{1}{3 \times 4}\right) = \frac{1}{3} + \frac{1}{4} + \frac{1}{12}.$$

As Euler proved, the series $\sum_p 1/p$ diverges, where p runs over all the primes.

Conjecture (Z.-W. Sun, 2015-09-09). Let r be any positive rational number. For $d = \pm 1$, there are finitely many distinct primes $q_1, \ldots, q_k$ such that $r = \sum_{j=1}^{k} 1/(q_j + d)$.

Remark. On Nov. 4, 2015 I announced a prize of 1000 US dollars for the first correct proof. The conjecture has been verified for all those rational numbers $r \in (0, 1]$ with denominators not exceeding 100. (`http://math.nju.edu.cn/∼zwsun/UnitFraction.pdf`.)

Examples:

$$1 = \frac{1}{2-1} = \frac{1}{3-1} + \frac{1}{5-1} + \frac{1}{7-1} + \frac{1}{13-1},$$

$$1 = \frac{1}{2+1} + \frac{1}{3+1} + \frac{1}{5+1} + \frac{1}{7+1} + \frac{1}{11+1} + \frac{1}{23+1},$$

$$\begin{aligned}\frac{1}{19} =& \frac{1}{37-1} + \frac{1}{137-1} + \frac{1}{191-1} + \frac{1}{229-1} \\ &+ \frac{1}{331-1} + \frac{1}{397-1} + \frac{1}{761-1} + \frac{1}{1021-1} \\ =& \frac{1}{37+1} + \frac{1}{107+1} + \frac{1}{227+1} + \frac{1}{239+1} \\ &+ \frac{1}{311+1} + \frac{1}{359+1} + \frac{1}{701+1} + \frac{1}{911+1} \text{ (Z.-W. Sun).}\end{aligned}$$

$$\begin{aligned}\frac{6}{29} =& \frac{1}{7-1} + \frac{1}{29-1} + \frac{1}{281-1} + \frac{1}{2437-1} + \frac{1}{2521-1} + \frac{1}{7309-1} \\ =& \frac{1}{5+1} + \frac{1}{29+1} + \frac{1}{271+1} + \frac{1}{509+1} + \frac{1}{1217+1} \\ &+ \frac{1}{4079+1} + \frac{1}{7307+1} + \frac{1}{17747+1} \text{ (Qing-Hu Hou, Nov. 6).}\end{aligned}$$

Part III. Universal Representations involving Mixed Powers

Mixed Sums of Squares and Triangular Numbers

Gauss-Legendre Theorem:
$\{x^2 + y^2 + z^2 : \ x, y, z \in \mathbb{N}\} = \mathbb{N} \setminus \{4^k(8l + 7) : \ k, l \in \mathbb{N}\}$.

Euler's Observation:

$$8n + 1 = (2x)^2 + (2y)^2 + (2z + 1)^2 \text{ with } x \equiv y \pmod 2$$

$$\Longrightarrow n = \frac{x^2 + y^2}{2} + \frac{z(z + 1)}{2} = \left(\frac{x + y}{2}\right)^2 + \left(\frac{x - y}{2}\right)^2 + \frac{z(z + 1)}{2}.$$

Lionnet's Assertion (proved by Lebesgue & Réalis in 1872). Any $n \in \mathbb{N}$ is the sum of two triangular numbers and a square.

B. W. Jone and G. Pall [Acta Math. 1939]. Every $n \in \mathbb{N}$ is the sum of a square, an *even* square and a triangular number.

Theorem (i) [Z. W. Sun, Acta Arith. 2007] Any $n \in \mathbb{N}$ is the sum of an *even* square and two triangular numbers.

(ii) (Conjectured by Z. W. Sun and proved by B. K. Oh and Sun [JNT, 2009]). Any positive integer n can be written as the sum of a square, an *odd* square and a triangular number.

Some new conjectures

Conjecture (Z. W. Sun, Oct. 2, 2015). Any positive integer n can be written as $x^2 + y^2 + p(p \pm 1)/2$ with p prime and $x, y \in \mathbb{Z}$.

For example, 97 has a unique representation $97 = 1^2 + 9^2 + 5(5+1)/2$ with 5 prime, and 538 has a unique representation $538 = 3^2 + 8^2 + 31(31-1)/2$ with 31 prime.
Let φ denote Euler's totient function. It is easy to see that all the numbers

$$\varphi(n^2) = n\varphi(n) \ (n = 1, 2, 3, \ldots)$$

are pairwise distinct.
My following conjecture seems novel and curious.

Conjecture (Sun, Oct. 1, 2015). Any integer $n > 1$ can be written as $x^2 + y^2 + \varphi(z^2)$, where x, y and z are integers with $0 \leqslant x \leqslant y$ and $z > 0$ such that y or z is prime.

For example, 13 has a unique representation $13 = 1^2 + 2^2 + \varphi(4^2)$ with 2 prime, and 94415 has a unique representation $94415 = 115^2 + 178^2 + \varphi(223^2)$ with 223 prime.

Some new conjectures

In Jan. 2015, using q-series I proved that any positive integer can be represented as the sum of two squares and a *positive* triangular number. Below is a variant of this involving cubes.

Conjecture (Sun, Oct. 3, 2015). Any positive integer n can be written as the sum of a nonnegative cube, a square and a positive triangular number.

I have verified this for $n \leqslant 10^5$. For example, 306 has a unique representation: $306 = 1^3 + 13^2 + 16 \times 17/2$.

In contrast with Largrange's theorem on sums of four squares, my following conjecture seems difficult.

Conjecture (Sun, Oct. 3, 2015). Any $n \in \mathbb{N}$ can be written as

$$w^2 + x^3 + y^4 + 2z^4 \text{ with } w, x, y, z \in \mathbb{N}.$$

For example, 1248 has a unique representation

$$1248 = 31^2 + 5^3 + 0^4 + 2 \times 3^4.$$

Write integers as $x^a + y^b - z^c$ with $x, y, z \in \mathbb{Z}^+$

Conjecture (Sun, Dec. 2015). If $\{a, b, c\}$ is among the multisets

$\{2, 2, p\}$ (p is prime or a product of some primes congruent to 1 mod 4),

$$\{2, 3, 3\},\ \{2, 3, 4\} \text{ and } \{2, 3, 5\},$$

then any integer m can be written as $x^a + y^b - z^c$, where x, y and z are positive integers.

I have verified that $\{x^4 - y^3 + z^2 :\ x, y, z \in \mathbb{Z}^+\}$ contains all integers m with $|m| \leqslant 10^5$. For example,

$$0 = 4^4 - 8^3 + 16^2,\quad -1 = 1^4 - 3^3 + 5^2,$$

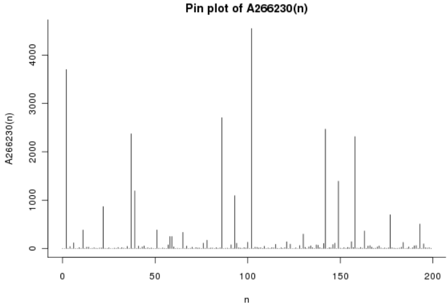
$$-20 = 32^4 - 238^3 + 3526^2,\quad 11019 = 4325^4 - 71383^3 + 3719409^2.$$

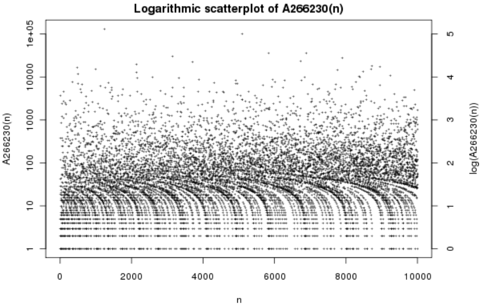
Other Examples.

$$394 = 2283^3 + 128^4 - 110307^2,\quad 570 = 546596^2 + 8595^3 - 983^4,$$

$$445 = 9345^3 + 34^5 - 903402^2,\quad 435 = 475594653^2 + 290845^3 - 3019^5.$$

Fountain Graph for $a(n) = \min\{x \in \mathbb{Z}^+ : \ n + x^2 = y^3 + z^3 \text{ for some } y, z \in \mathbb{Z}^+\}$





Why is the conjecture reasonable?

If $m \equiv 6 \pmod 8$, then for $a = 4, 6, 8, \ldots$ we have $m + x^a \equiv 6, 7 \pmod 8$ and hence $m + x^a$ can never be the sum of two squares.

For any prime $p \equiv 3 \pmod 4$ and odd integer $n > 1$, I have proved that $x^{pn} + (2p)^p$ cannot be the sum of two squares.

Heuristic Arguments (not rigorous): As

$$\{1 \leqslant n \leqslant N: \ n = x^a + y^b \text{ for some } x, y \in \mathbb{Z}^+\}$$

$$\sim C_0 N^{1/a+1/b} = C_0 \int_0^N \left(\frac{1}{a} + \frac{1}{b}\right) t^{1/a+1/b-1} dt,$$

we think that $t \in \mathbb{Z}^+$ has the form $x^a + y^b$ $(x, y \in \mathbb{Z}^+)$ with probability $C_1 t^{1/a+1/b-1}$ (where C_0 and C_1 are positive constants). Note that the series $\sum_{z=1}^{\infty}(m + z^c)^{1/a+1/b-1}$ diverges if $c(1 - 1/a - 1/b) < 1$. Thus, when $1/a + 1/b + 1/c > 1$, we might expect that there are infinitely many triples (x, y, z) of positive integers with $m = x^a + y^b - z^c$. If $2 \leqslant a < b \leqslant c$, then

$$\frac{1}{a} + \frac{1}{b} + \frac{1}{c} > 1 \iff a = 2, \ b = 3, \text{ and } c \in \{3, 4, 5\}.$$

Concluding remarks

For sources of most conjectures mentioned in this talk, you may loot at my following papers

1. Zhi-Wei Sun, *Some new problems in additive combinatorics*, preprint, `arXiv:1309.1679`. Available from `http://arxiv.org/abs/1402.6641`.]

2. Zhi-Wei Sun, *A new theorem on the prime-counting function*, Ramanujan J., in press. Available from `Doi 10.1007/s11139-015-9702-z`.

3. Zhi-Wei Sun, *Conjectures on representations involving primes*, in: Combinatorial and Additive Number Theory (edited by M. B. Nathanson), Springer, to appear. [This paper contains 100 conjectures.]

Thank you!