MEMORIAL TO JAVIER CILLERUELO: A PROBLEM LIST

Pablo Candela[1]
Department of Mathematics, Autonomous University of Madrid, and Instituto de Ciencias Matemáticas, Madrid, Spain
pablo.candela@uam.es

Juanjo Rué[2]
Department of Mathematics, Universitat Politècnica de Catalunya and Barcelona Graduate School of Mathematics, Barcelona, Spain
juan.jose.rue@upc.edu

Oriol Serra[3]
Department of Mathematics, Universitat Politècnica de Catalunya and Barcelona Graduate School of Mathematics, Barcelona, Spain
oriol.serra@upc.edu

Received: 11/3/17, Accepted: 3/16/18, Published: 3/23/18

Abstract

This is a list of problems in combinatorial number theory gathered on the occasion of the meeting *The Music of Numbers* to honor the memory of the late Javier Cilleruelo (1961-2016).

1. Introduction

The conference *The Music of Numbers* (http://musicofnumbers.kissr.com/index.html) was held in the *Instituto de Ciencias Matemáticas – ICMAT* in Madrid on 20–22 September 2017 as a mathematical tribute to Javier Cilleruelo, who sadly passed away on May 2016. This document gathers several open problems, mostly related to his mathematical contributions in Number Theory, which were offered by his collaborators to honor his memory. We have respected the different styles and formats of the authors of the problems, which are presented in alphabetical order of the proposers. We have included problems that Javier had in his files as a research program for the future. The list of contributors is Javier Cilleruelo, Antonio Córdoba,

[1]Supported by the Spanish Ministerio de Economía y Competitividad grant MTM2017-83496-P.
[2]Supported by the Spanish Ministerio de Economía y Competitividad grants MTM2014-54745-P and MDM-2014-0445.
[3]Supported by the Spanish Ministerio de Economía y Competitividad grants MTM2014-54745-P and MDM-2014-0445.

Jean–Marc Deshouillers, Moubariz Z. Garaev, Florian Luca, Surya Ramana, Misha Rudnev, Juanjo Rué, Imre Z. Ruzsa, Oriol Serra and Igor Shparlinski.

We are grateful to the Editorial Managers of Integers, The Electronic Journal of Combinatorial Number Theory, who kindly accepted to publish this list in the journal. This will certainly contribute to broadly spreading these problems and foster research in the areas that Javier loved so much and to which he devoted his mathematical life.

2. Javier Cilleruelo

1. The probabilistic method gives the existence of an infinite sequence A which is both a B_3 sequence, namely, the sums $a+a'+a''$ with $a, a', a'' \in A$ are pairwise distinct, and has counting function $A(x) \gg x^{1/5-\epsilon}$.

   Problem 1. *Improve the exponent* $1/5$.

2. Let $f(x,y)$ be a quadratic form. We say that A is f–bounded if there is a constant g such that, for each positive integer n there are at most g pairs $(a,a') \in A \times A$ such that $f(a,a') = n$.

   Problem 2. *Prove that, for each* $\epsilon > 0$ *there is a sequence* A *which is* f*–bounded for each quadratic form* f *and such that* $A(x) \gg x^{1-\epsilon}$.

3. The set $A = \{(f(x), g(x)),\ x \in \mathbb{F}_p\}$ is a Sidon set with p elements whenever f and g are independent polynomials with $1 \le \deg(f), \deg(g) \le 2$. Reciprocally, if $A = \{(1, g(x)),\ x \in \mathbb{F}_p\}$ is a Sidon set, then g is quadratic polynomial. Prove or disprove:

   Problem 3. *Let* A *be a Sidon set in* $\mathbb{Z}_p \times \mathbb{Z}_p$ *with* p *elements. Prove that* $A = \{(f(x), g(x)) :\ x \in \mathbb{Z}_p\}$ *where* $1 \le \deg(f), \deg(g) \le 2$ *and* $\deg(\mu f(x) + \lambda g(x)) \ge 1$ *for any* $(\mu, \lambda) \ne (0,0)$.

4. Let f be a polynomial and consider $L_f(n) = \log \operatorname{lcm}\{f(1), \dots, f(n)\}$. It is well–known that, for $f(x) = x$, $L_f(n) \sim n$ which is equivalent to the prime number theorem. We proved that for an irreducible quadratic polynomial one has $L_f(n) = n \log n + Bn + o(n)$ where B is an explicit constant depending on f.

   Problem 4. *Estimate* $L_f(n)$ *for*

   (a) $f(x) = (x^2+1)(x^2+2)$.

   (b) $f(x) = x^3 + 1$.

5. What is the largest cardinality of a set $A \subset [n] \times [n]$ which is free of three homothetic copies of a triangle? The known bounds are $n(1+o(1)) \leq |A| \ll n^{4/3}$.

3. Antonio Córdoba

1. With Javier Cilleruelo we proved that, for each $\alpha < 1/2$, there is C_α such that any arc of length R^α of a circle of radius R contains at most C_α lattice points. An elementary geometric argument based on curvature considerations yields the following result: on the sphere of radius R in the n–dimensional Euclidean space the lattice points contained inside an spherical cap of radius $R^{1/n+1}$ are located in a finite number of hyperplanes, uniformly on R.

   Problem 5. *What happens when the radius of the cap is R^α, $\frac{1}{n+1} < \alpha < 1$?*

2. Given a set $A = \{\xi_j,\ j \in J\}$ of points in the sphere $\|x\| = r$ in $\mathbb{R}^n$, $n \geq 3$ such that

   (a) $\|\xi_j - \xi_k\| \geq 1$ for $j \neq k$,

   (b) $\sup_j \#\{\xi_k : \|\xi_j - \xi_k\| \leq r^{1/2}\} = M$.

   We consider now the trigonometric sum
   $$\sum_j a_j e^{2\pi i \xi_j \cdot \mathbf{x}}.$$

   Problem 6. *Is it true that*
   $$\sup_{\|Q\|=1} \left(\int_Q |\sum_j a_j e^{2\pi i \xi \cdot x}|^{\frac{2n}{n-1}} \right)^{\frac{n-1}{2n}} \leq M^{\frac{1}{2n}} \left(\sum_j |a_j|^2 \right)^{1/2},$$
   where Q is a box? With Eric Latorre [9] we proved the truth of the above statement for $n = 2$.

4. Jean–Marc Deshouillers

1. For a positive integer s, Erdős and Rényi [15] define a random sequence of pseudo s-th powers in the following way. They first consider $(\xi_n)_n$ a sequence of random variables with values in $\{0, 1\}$ defined over a probability space Ω, satisfying
   $$\mathrm{Prob}(\xi_n = 1) = \frac{1}{sn^{1-1/s}} \quad \text{for} \quad n \geq 1 \quad \text{and} \quad \mathrm{Prob}(\xi_0 = 1) = 1.$$

Then they define the sequence $\widetilde{\mathcal{A}_s}$ through its indicator function

$$\text{For } \omega \in \Omega\colon \mathbb{I}_{\widetilde{\mathcal{A}_s(\omega)}}(n) = \xi_n(\omega).$$

From now on, we forget the reference to ω, but keep in mind that we are dealing with random variables on Ω.

For $k \geq s$, let $\widetilde{r_{s,k}}(n)$ denote the number of representations of $n \geq 0$ as the sum of k elements from $\widetilde{\mathcal{A}_s}$.

Deshouillers and Iosifescu [13] proved in 2000 that the pseudo s-th powers are almost surely an additive basis of asymptotic order $s+1$. Their main result is that there exist two positive constants $u = u(s)$ and $v = v(s)$ such that

$$\text{almost surely} \ : \ \exp(-vn^{1/s}) \leq \operatorname{Prob}(\widetilde{r_{s,s+1}}(n) = 0) \leq \exp(-un^{1/s}).$$

Problem 7. *Do we have* $\operatorname{Prob}(\widetilde{r_{s,s+1}}(n) = 0) = \exp(-w(1+o(1))n^{1/s})$ *for some* w*?*

The largest integer which is not a sum of at most $s+1$ pseudo s-th powers being a random variable which is almost surely finite, the following question is natural and would have an implication in extending the range of validity of some computations.

Problem 8. *What is the law of the largest integer which is not a sum of at most* $s+1$ *pseudo-s powers?*

Cilleruelo, Deshouillers, Lambert and Plagne [4] proved the following:

Let $\lambda_s = \Gamma(1/s)/(s^s s!)$ and $c > (\lambda_s(1-2\lambda_s))^{-1}$. Almost surely, a sequence of pseudo s-th powers $\widetilde{\mathcal{A}}$ has the following property: any large enough integer n can be written in the form

$$n = a_1 + \cdots + a_{s+1}, \quad \text{with} \quad a_i \in \widetilde{\mathcal{A}} \quad \text{and } a_{n+1} < (c \log n)^s.$$

Problem 9. *Can one replace* $c > (\lambda_s(1-2\lambda_s))^{-1}$ *by* $c > (\lambda_s)^{-1}$*?*

Problem 10. *Show that the above statement does not hold any longer if* $c < \lambda_s^{-1}$.

The Erdős-Rényi model for the pseudo s-th powers only takes care of the "infinite valuation". Around 2000, Deshouillers, Hennecart and Landreau [10] developed probabilistic models which also take care of the distribution of the pseudo s-th powers in arithmetic progressions. For fixed K, they forced the pseudo s-th powers to be distributed as the real s-th powers in all the arithmetic progressions modulo any integer less than K. For example, this leads almost surely to a density $\delta_s(K)$ for the sums of s pseudo s-th powers. Moreover, when K tends to infinity, $\delta_s(K)$ tends to 0 when $s = 2$ and to a positive limit when $s \geq 3$. They also made some numerical experiments for $s = 3$ [12] and $s = 4$ [11] which turned out to be consistent with the arithmetico-random model.

Problem 11. *Find an arithmetico-probabilistic model for squares in which Landau asymptotics for sums of two squares (i.e. their number up to x is equivalent to $Cx/\sqrt{\log x}$) is almost surely valid for sums of 2 pseudo-squares.*

Finally, in their numerical exploration of sums of three cubes, Deshouillers, Hennecart and Landreau [12] noticed that the density of sums of three cubes seems to have a minimal value around 10^{14}.

Problem 12. *Give some (heuristical) explanation of the fact that the density of the sums of three cubes is minimal around 10^{14}.*

5. Moubariz Z. Garaev

1. Let p be a sufficiently large prime number. In the joint work with Javier Cilleruelo [5] we have shown that there is an absolute constant $c > 0$ such that the number J of solutions of the congruence

   $$x^n \equiv \lambda \pmod p; \quad x \in \mathbb{N}, \quad L < x < L + p/n,$$

   satisfies $J < p^{\frac{1}{3}-c}$ uniformly over positive integers n, λ and L.

   The method of [5] is effective and the constant c can easily be made explicit, however it will be small. Heuristically one believes that $J < p^{o(1)}$. Here we pose the following question.

   Problem 13. *Prove that $J < p^{3/10}$.*

   In other words, prove that one can take $c = 1/30$.

6. Florian Luca

1. An integer n is a *palindrome* in base g if the coefficients of n in its expansion $n = \sum_{i=0}^{l} d_i g^i$ in base g satisfy $d_i = d_{l-i}$ for each i. With Javier Cilleruelo and Lewis Baxter [6] we proved that, for each $g \geq 5$, the set $P_g = \{n \in \mathbb{N} :$ n is a palindrome in base $g\}$ is an additive basis of order 3. $P_g + P_g + P_g = \mathbb{N}$.

   Problem 14. *Let $s(k, g)$ be the smallest number s such that in every coloring of P_g with k colors every integer is the sum of at most s monochromatic palindromes in P_g. Is $s(k, g)$ independent of g?*

7. Surya Ramana

1. The two questions given below are due to Javier Cilleruelo and are stated on page 53 of [7]. This paper studies $|A \cdot A|$ and $|A/A|$, both when A is a random subset of $[1, n]$ and when A is an "interesting" set such as shifted primes or shifted sums of two squares.

   Let $A \subset [1, n]$ be a set of integers, with $n \to +\infty$.

   Problem 15. *Is it true that* $|A \cdot A| \sim \frac{|A|^2}{2}$ *implies* $|A| = o(\frac{n}{\sqrt{\log n}})$*?*

   Problem 16. *Is it true that if* $|A \cdot A| \sim |[1, n] \cdot [1, n]|$ *then* $|A| \sim n$*?*

8. Misha Rudnev

1. Let A be a finite set in a field F and let $D = A - A$. We can prove by using crosss ratios that there is $\epsilon > 0$ such that

   $$|D \cdot D| > |D|^{1+\epsilon}.$$

   Problem 17. *Show that, for each* $N \geq 2$ *there is* $M = f(N)$ *such that* $|D^M| \geq |A|^N$.

9. Juanjo Rué

1. In a joint work with Cilleruelo, Rué, Sarka and Zumalacárregui [8] we studied the behavior of $\log \operatorname{lcm}(A)$, where A is a subset of $\{1, \ldots, n\}$ in which each element is chosen independently with probability p. In particular, precise estimates for the expected value and variance of $\log \operatorname{lcm}(A)$ were obtained.

   Problem 18. *Is there a scaling limit for the random variable* $\log \operatorname{lcm}(A)$*?*

   Javier conjectured that the answer is a normal limit law.

10. Imre Z. Ruzsa

1. Let p be an odd prime. The size of the largest Sidon set in $\mathbb{Z}_p^{2k}$ is p^k.

   Problem 19. *What happens in* $\mathbb{Z}_p^{2k+1}$*?*

   Problem 20. *What if* p *is composite?*

2. Let f be a completely multiplicative function such that

$$\sum_{n<x} f(n) = cn + O(1)$$

with $c \neq 0$.

Problem 21. *Is it true that for every prime p either $f(p) = 1$ or $|f(p)| < 1$?*

Assuming an affirmative answer it is not difficult to describe all such functions.

Problem 22. *Formulate at least a plausible conjecture for the case $c = 0$.*

3. Let A be a finite set of integers.

Problem 23. *Is there another set B such that*

$$|B| \approx |A|, \;\; |B+B| \approx |A-A|?$$

Problem 24. *Is there another set C such that*

$$|C-C| \approx |A+A|, \;\; |C+C| \approx |A-A|?$$

The meaning of $\approx$ in the above two problems is up to a factor of $|A|^{\varepsilon}$.

All known inequalities involving the sumset and the difference set are symmetric (a positive answer to the above problem would explain why). However, typically the difference set is bigger; constructing sets with more sums than differences is more difficult and the excess is smaller than in the opposite direction.

4. Let $A \subset \mathbb{N}$ be a set of positive density.

Problem 25. *Is it true that $A - A$ has a nonempty interior in the Bohr topology, that is, it contains a set of the form*

$$\{n : \|\alpha_1(n-a)\| < \varepsilon, \ldots, \|\alpha_k(n-a)\| < \varepsilon\}$$

with an integer a and real $\alpha_1, \ldots, \alpha_k$?

11. Oriol Serra

1. Let $f(n)$ be the minimum number of monochromatic solutions of the Sidon equation $x + y = z + t$ in a 2–coloring of $\mathbb{Z}/n\mathbb{Z}$.

Problem 26. *Give an estimation of a lower bound for $f(n)$. Is there a 2–coloring with fewer monochromatic solutions than a random 2–coloring?*

This is a particular instance of the general problem of finding the minimum number of monochromatic solutions to linear equations posed by Ron Graham. For 3–term arithmetic progressions in the integers Parrilo, Robertson and Saracino [17] showed that random colorings are not the ones which minimize the number of monochromatic patterns. An analogous result was obtained by J. Wolf [20] for 4–term arithmetic progressions. In Cameron, Cilleruelo and Serra [1] we gave some formulas relating the counting of different color patterns of solutions to linear equations in a coloring of a group. Stating precisely the problem for the Sidon equation was a question that Javier particularly liked.

12. Igor Shparlinski

1. About seven years ago, Javier [2] gave an asymptotic formula for the least common multiple of the first N values of a quadratic polynomial

   $$f(x) = ax^2 + bx + c \in \mathbb{Z}[x] : \log \operatorname{lcm}[f(1), \cdots, f(N)] = N \log N + B_f N + o(N)$$

   where B_f depends only on f.

   In 2013, J. Rué, P. Sarka and A. Zumalacárregui [18] obtained in the case of $f(x) = x^2 + 1$ a more explicit bound on the error term, with a logarithmic saving. Their method can also be applied to more general quadratic polynomials.

   The obstacle for further improvements and generalisations is in our poor knowledge of the distribution of roots of polynomial congruences modulo primes. In fact the only known results are that of W. Duke, J. Friedlander and H. Iwaniec [14] and its extensions by Á. Tóth [19] and K. Homma [16].

   On the other hand, in the case of polynomials in two variables, we know lots more: For counting roots in large boxes, one can use the Bombieri bound, for small boxes, one can use a large variety of results of several authors, including Javier Cilleruelo himself. This naturally leads to the following:

   Problem 27. *Given a polynomial $f(x, y) \in \mathbb{Z}[x, y]$, obtain an asymptotic formula for*

   $$\log \operatorname{lcm}[f(m, n), 1 \leq m, n \leq N]$$

   with a power saving in the error term.

   A natural starting point could the case of polynomials of the form $f(x, y) = q(x, y) - a$ with a quadratic form q and an integer a. In this case, there are results of A. Zumalacárregui which give nontrivial information about the distribution of solutions in boxes of any size.

References

[1] P. Cameron, J. Cilleruelo and O. Serra, On monochromatic solutions of equations in groups, *Rev. Mat. Iberoam.* **23** (2007), 385-395.

[2] J. Cilleruelo, The least common multiple of a quadratic sequence, *Compos. Math.* **147** (2011), 1129-1150.

[3] J. Cilleruelo and J-M. Deshouillers, Gaps in sumsets of s pseudo s-th power sequences, *Ann. Inst. Fourier (Grenoble)* **67** (2017), 1725-1738.

[4] J. Cilleruelo, J-M. Deshouillers, V. Lambert, and A. Plagne, Additive properties of pseudo s-th power sequences, *Math. Z.* **284** (2016), 175-193.

[5] J. Cilleruelo and M. Z. Garaev, Congruences involving product of intervals and sets with small multiplicative doubling modulo a prime and applications, *Math. Proc. Cambridge Philos. Soc.* **160** (2016), no. 3, 477-494.

[6] J. Cilleruelo, F. Luca, and L. Baxter, Every positive integer is a sum of three palindromes, *Math. Comp.*, published electronically (2017), https://doi.org/10.1090/mcom/3221.

[7] J. Cilleruelo, D.S. Ramana, and O. Ramaré, Quotients and product sets of thin subsets of the positive integers, *Proc. Steklov Inst. Math.* **296** (2017), 52-64.

[8] J. Cilleruelo, J. Rué, P. Sarka, and A. Zumalacárregui, The least common multiple of random sets of positive integers, *J. Number Theory* **144** (2014), 92-104.

[9] A. Córdoba, E. Latorre, Radial multipliers and restriction to surfaces of the Fourier transform in mixed-norm spaces, *Math. Z.* **286** (2017), 1479-1493.

[10] J-M. Deshouillers, F. Hennecart, and B. Landreau, Sums of powers: an arithmetic refinement to the probabilistic model of Erdős and Rényi, *Acta Arith.* **85** (1998), 13-33.

[11] J-M. Deshouillers, F. Hennecart, and B. Landreau, Do sums of 4 biquadrates have a positive density?, *Algorithmic number theory*, 196-203, Lecture Notes in Comput. Sci. **1423**, Springer, Berlin, 1998.

[12] J-M. Deshouillers, F. Hennecart, and B. Landreau, On the density of sums of three cubes, *Algorithmic number theory*, 141-155, Lecture Notes in Comput. Sci. **4076**, Springer, Berlin, 2006.

[13] J-M. Deshouillers and M. Iosifescu, Sommes de $s+1$ pseudo-puissances s-ièmes, *Rev. Roumaine Math. Pures Appl.* **45** (2000), 427-435.

[14] W. Duke, J. Friedlander, and H. Iwaniec, Equidistribution of roots of a quadratic congruence to prime moduli, *Ann. of Math.* (2) **141** (1995), no. 2, 423-441.

[15] P. Erdős and A. Rényi, Additive properties of random sequences of positive integers, *Acta Arith.* **6** (1960), 83-110.

[16] K. Homma, On the discrepancy of uniformly distributed roots, *J. Number Theory* **128** (2008), 500-508.

[17] P. A. Parrilo, A. Robertson, and D. Saracino, On the asymptotic minimum number of monochromatic 3-term arithmetic progressions, *J. Combin. Theory Ser. A* **115** (2008), 185-192.

[18] J. Rué, P. Sarka, A. Zumalacárregui, On the error term of the logarithm of the lcm of quadratic sequences, *J. Théor. Nombres Bordeaux* **25** (2) (2013) 457-470.

[19] Á. Tóth, Roots of quadratic congruences, *Internat. Math. Res. Notices 2000*, no. 14, 719-739.

[20] J. Wolf, The minimal number of monochromatic 4-term progressions in $\mathbb{Z}_p$, *J. Comb.* **1** (2010), 53-68.