The Green-Tao theorem on primes in arithmetical progressions in the positive cone of Z[X]

Elem. Math. 69 (2014) 30 – 32
0013-6018/14/010030-3
DOI 10.4171/EM/242

Elemente der Mathematik

The Green–Tao theorem on primes in arithmetical progressions in the positive cone of $\mathbb{Z}[X]$

Victor Pambuccian

Victor Pambuccian studierte von 1978 bis 1982 Mathematik an der Universität Bukarest und promovierte 1993 an der University of Michigan in Ann Arbor. Seit 1994 ist er Professor an der Arizona State University. Sein Hauptforschungsgebiet ist die axiomatische Grundlegung der Geometrie.

One version of the celebrated Green–Tao theorem [1], can be stated as:

For every positive integer k and every positive integer c, there are positive integers a and b, with b greater than c, such that $an + b$ is a prime for all $n \in \{0, 1, \ldots, k-1\}$.

Although the existing proof of this theorem is far from elementary, in that it does not stay confined within the natural numbers, but uses various properties of the reals, its statement is elementary and can be stated in the simple language of Peano Arithmetic without the induction axiom, a theory we shall refer to as PA^-, an elementary theory axiomatized in a language containing two binary operations $+$ and $\cdot$, two individual constants 0 and 1, as well as a binary relation $<$ whose axioms A1–A15 are presented in [2, pp. 16–18]. We will repeat them here for the reader's convenience, and we will omit the universal quantifiers for all universal axioms.

A1 $(x + y) + z = x + (y + z)$

A2 $x + y = y + x$

Im Zusammenhang mit dem Beweisen eines bestimmten mathematischen Satzes ist die Frage nach einem minimalen Axiomensystem, mit dessen Hilfe der entsprechende Satz hergeleitet werden kann, und damit verbunden, die Frage nach der Klasse der Bereiche, in denen der Satz gilt, ein zentrales Element mathematischen Arbeitens. Der tiefliegende zahlentheoretische Satz von Green–Tao besagt, dass es beliebig lange arithmetische Folgen gibt, mit beliebig grossem Anfangsglied, die aus lauter Primzahlen bestehen. Auf der Suche nach Strukturen, die beträchtliche Unterschiede zur Struktur der natürlichen Zahlen aufweisen, findet der Autor des vorliegenden Artikels, dass der Satz von Green–Tao seine Gültigkeit in der Menge der positiven Elemente des Ringes der Polynome mit ganzzahligen Koeffizienten behält.

A3 $(x \cdot y) \cdot z = x \cdot (y \cdot z)$

A4 $x \cdot y = y \cdot x$

A5 $x \cdot (y + z) = x \cdot y + x \cdot z$

A6 $x + 0 = x \wedge x \cdot 0 = 0$

A7 $x \cdot 1 = x$

A8 $(x < y \wedge y < z) \rightarrow x < z$

A9 $\neg x < x$

A10 $x < y \vee x = y \vee y < x$

A11 $x < y \rightarrow x + z < y + z$

A12 $(0 < z \wedge x < y) \rightarrow x \cdot z < y \cdot z$

A13 $(\forall x)(\forall y)(\exists z)\, x < y \rightarrow x + z = y$

A14 $0 < 1 \wedge (x > 0 \rightarrow (x > 1 \vee x = 1))$

A15 $x > 0 \vee x = 0$

The models of these axioms are the positive cones of discretely ordered rings, and one can state the above version of the Green–Tao theorem in this theory. To improve the readability of the statement, it is helpful to define the notion of prime inside our theory. This can be done in two ways, which are not equivalent in PA^-: by stating that a number is prime if it is irreducible, or by stating that it is prime if whenever it divides a product it must divide one of the factors. We thus have two predicates:

$$\pi_1(x) \quad :\Leftrightarrow \quad (\forall a)(\forall b)\, x = a \cdot b \rightarrow (a = 1 \vee b = 1) \tag{1}$$

$$\pi_2(x) \quad :\Leftrightarrow \quad (\forall a)(\forall b)(\forall c)(\exists d)\, x \cdot c = a \cdot b \rightarrow (x \cdot d = a \vee x \cdot d = b) \tag{2}$$

and two forms of the Green–Tao theorem (for $i \in \{1, 2\}$):

$$(\forall k)(\forall c)(\exists a)(\exists b)(\forall k')\, a > c \wedge (k' < k \rightarrow \pi_i(a + b \cdot k')). \tag{3}$$

One would expect the theorem to be true in PA (which is PA^- together with an axiom schema corresponding to the induction principle), which would mean that it has an elementary proof, one that can be written down without any appeal to the real numbers. We know that none of the two versions hold in PA^-, as there are models of PA^- (see [5]) in which the set of all primes (and thus of all irreducibles) is bounded from above (very few results of number theoretic interest hold in PA^- (one such example is presented in [3]), so it is no surprise that the Green–Tao theorem does not hold in PA^-). The weakest theory in which (3) could hold is $\mathrm{PA}^- \cup \{\mathrm{A16}\}$, where A16 is an axiom stating that the primes (or irreducibles) are cofinal, in the sense that

A16 $(\forall x)(\exists p)\, \pi_i(p) \wedge p > x$.

The question whether $\mathrm{PA}^- \cup \{\mathrm{A16}\} \vdash (3)$ is very likely hard to settle. The aim of our note is only to show that (3) holds in one particular model of $\mathrm{PA}^- \cup \{\mathrm{A16}\}$, namely in the positive cone of $\mathbb{Z}[X]$, i.e., in the set $C(\mathbb{Z}[X]) := \{p(X) \in \mathbb{Z}[X] \mid p(X) \geq 0\}$, where the order is defined by setting $p(X) = a_n X^n + a_{n-1} X^{n-1} + \cdots + a_0 > 0$ if and only if the

leading coefficient $a_n > 0$. Before proceeding with the proof, we remind the statement of Eisenstein's criterion for the irreducibility of a primitive polynomial in $\mathbb{Z}[X]$: If a polynomial $f(X) = X^n + a_{n-1}X^{n-1} + \cdots + a_1X + a_0$ is such that $p|a_i$ for all $i \in \{0, \ldots, n-1\}$ and $p^2 \nmid a_0$, for some prime number p, then $f(X)$ is irreducible in $\mathbb{Z}[X]$. We will thus show that

Theorem. *The Green–Tao theorem* (3) *holds in* $C(\mathbb{Z}[X])$.

Proof. First, notice that, in $\mathbb{Z}[X]$, an element is irreducible if and only if it is prime, i.e., $\pi_1(x) \leftrightarrow \pi_2(x)$ holds in $C(\mathbb{Z}[X])$. It is thus enough to show that (3) with $i = 1$ holds in $C(\mathbb{Z}[X])$. To prove (3) with $i = 1$, notice that, given c and k in $C(\mathbb{Z}[X])$, we can choose a to be $X^n + 2$ and b to be $2X$, where $n = 2(\max\{\deg(c), \deg(k)\} + 1)$, where by $\deg(f)$ we have denoted the degree of the polynomial f. To see that $a + b \cdot k'$, i.e., the polynomial $X^n + 2 \cdot k' \cdot X + 2$, is irreducible for all $0 \leq k' < k$, first notice that $\deg(2 \cdot k' \cdot X) \leq \deg(k) + 1 \leq \frac{n}{2}$, so the conditions of the Eisenstein criterion for irreducibility are satisfied for the prime number 2, given that the leading coefficient is 1, the free term is 2, and the other coefficient is a multiple of 2. □

Interest in the validity in $C(\mathbb{Z}[X])$ of sentences originally stated for $\mathbb{N}$ has been expressed outside of the "models of arithmetic" context as well. A. Schinzel [4] has shown that the Erdős-Straus conjecture, stating the representability of $4/n$ as the sum of three unit fractions, is false in $C(\mathbb{Z}[X])$.

References

[1] B. Green, T. Tao, The primes contain arbitrarily long arithmetic progressions. Ann. of Math. (2) 167 (2008), 481–547.

[2] R. Kaye, Models of Peano Arithmetic, vol. 15 of Oxford Logic Guides, The Clarendon Press, New York, 1991.

[3] V. Pambuccian, The sum of irreducible fractions with consecutive denominators is never an integer in PA^-. Notre Dame J. Form. Log. 49 (2008), 425–429.

[4] A. Schinzel, On sums of three unit fractions with polynomial denominators. Funct. Approx. Comment. Math. 28 (2000), 187–194.

[5] J.C. Shepherdson, A non-standard model for a free variable fragment of number theory. Bull. Acad. Polon. Sci. Sér. Sci. Math. Astronom. Phys. 12 (1964), 79–86.

Victor Pambuccian
School of Mathematical and Natural Sciences
Arizona State University – West Campus
P.O. Box 37100
Phoenix, AZ 85069-7100, USA
e-mail: pamb@asu.edu