Journal of Logic & Analysis 12:5 (2020) 1–6
ISSN 1759-9008

On factoring of unlimited integers

KAREL HRBACEK

Abstract: Abdelmadjid Boudaoud asked whether every unlimited integer is a sum of a limited integer and a product of two unlimited integers. Assuming Dickson's Conjecture, the answer is negative.

2010 Mathematics Subject Classification 26E35 (primary); 03H05, 03H15, 11A51, 11U10 (secondary)

Keywords: factoring of integers, nonstandard analysis, unlimited integers, Dickson's conjecture

Abdelmadjid Boudaoud [1, 2, 3] asked whether every large integer is close to a product of two large integers. The question was made precise in the framework of nonstandard analysis by interpreting "large" as *unlimited* (infinite, nonstandard) and "close to" as *having a limited* (finite, standard) *difference from*:

Is every unlimited integer a sum of a limited integer and a product of two unlimited integers?

Symbolically: *If $\omega \in \mathbb{Z}$ is unlimited, is*

(*) $$\omega = s + \omega_1 \cdot \omega_2$$

where $s \in \mathbb{Z}$ is limited and $\omega_1, \omega_2 \in \mathbb{Z}$ are unlimited?

We show that the question has negative answer assuming Dickson's Conjecture about primes in arithmetic progressions. Following [1] we use the internal language of an axiomatic nonstandard set theory such as IST or BST, but the argument works, with minor modifications, in any model-theoretic framework (ultraproducts, superstructures). Only the most basic ideas of nonstandard analysis are required, and those only for understanding of conversion of the problem to an equivalent standard one.

First some simple observations. Let ω be unlimited and $\pi_1 \cdot \pi_2 \cdot \ldots \cdot \pi_\nu$ be the prime number decomposition of $|\omega|$. If at least two of the prime numbers are unlimited, or if ν is unlimited, then clearly $\omega = \omega_1 \cdot \omega_2$ for some unlimited integers ω_1, ω_2 and (*) holds with $s = 0$. Hence a counterexample to (*) has to have the form $\omega = a \cdot \pi$ where π is an unlimited prime number and $a \in \mathbb{Z}$ is limited, $a \neq 0$. Without loss of generality we can assume that $\omega > 0$ and ω is a prime number. Indeed, if every

Published: December 2020 https://doi.org/10.4115/jla.2020.12.5

unlimited prime number π could be expressed in the form (*) as $\pi = s + \omega_1 \cdot \omega_2$, then $\omega = a \cdot \pi = (a \cdot s) + (a \cdot \omega_1) \cdot \omega_2$, which would have the required form (*).

If a prime number π is a counterexample to (*), then for each limited $s \in \mathbb{Z}$ there exist an unlimited prime number π_s and a limited $a_s \in \mathbb{Z}$, $a_s > 0$, such that

$$(**) \qquad \pi - s = a_s \cdot \pi_s.$$

Noticing that $a_0 = 1$ and $\pi = \pi_0$, we rewrite (**) as

$$(***) \qquad a_s \cdot \pi_s - \pi_0 = -s.$$

It follows that, for all limited positive integers q, r, the system of Diophantine equations $a_s \cdot x_s - x_0 = -s, \quad 0 < |s| \leq q$, has a solution where all x_s are prime numbers greater than r. By Standardization, we can extend the external sequence $\langle a_s : s \in \mathbb{Z}, s \text{ limited}\rangle$ to a standard sequence $\langle a_s : s \in \mathbb{Z}\rangle$. By Transfer we deduce that the existence of a counterexample to Boudaoud's question implies the following statement $\mathcal{S}$ of standard number theory:

There is a sequence $\langle a_s : s \in \mathbb{Z}\rangle$ such that $a_0 = 1$, $a_s > 0$ for all $s \in \mathbb{Z}$, and for all positive integers q, r the system of Diophantine equations

$$(S_q) \qquad a_s \cdot x_s - x_0 = -s, \quad 0 < |s| \leq q$$

has a solution where all x_s, $|s| \leq q$, are prime numbers greater than r.

On the other hand, if there is a sequence as in the statement $\mathcal{S}$, then there is a standard one, by Transfer. Given such standard sequence $\langle a_s : s \in \mathbb{Z}\rangle$, we can take unlimited q and r and the corresponding solution $\langle x_s : |s| \leq q\rangle$. For each s limited, a_s is limited and x_s is an unlimited prime number satisfying $x_0 - s = a_s \cdot x_s$; so $\omega = x_0$ is a counterexample to Boudaoud's question. Therefore it suffices to construct a sequence $\langle a_s : s \in \mathbb{Z}\rangle$ as in $\mathcal{S}$.

The system of equations (S_q) has a solution $\langle x_s : |s| \leq q\rangle$ if and only if the system of congruences

$$(R_q) \qquad x \equiv s \mod a_s, \quad 0 < |s| \leq q$$

has a solution x_0. The obvious necessary condition for solvability of (R_q) is

$$(C) \qquad (a_s, a_t) \mid t - s$$

for all $0 < |s|, |t| \leq q$. It is an easy corollary to the Chinese Remainder Theorem that the condition (C) is also sufficient for the existence of a solution to (R_q); moreover, if $\bar{x}_0$ is one solution of (R_q), then every solution is given by $x_0(k) = \bar{x}_0 + A^q \cdot k$ where $A^q = [a_{-q}, \ldots, a_q]$ is the least common multiple of $a_s, |s| \leq q$, and $k \in \mathbb{Z}$. We let

$A^q_s = A^q/a_s$; returning to the system (S_q) we see that, assuming the condition (C) is satisfied for all $0 < |s|, |t| \le q$, the system is solvable and all of its solutions are of the form

$$(F) \qquad x_s(k) = \bar{x}_s + A^q_s \cdot k, \quad |s| \le q$$

where $\langle \bar{x}_s : |s| \le q \rangle$ is a particular solution of (S_q) and $k \in \mathbb{Z}$. We note that the solutions are given by a set of arithmetic progressions. To obtain the desired result, we need to show that there are solutions where all $x_s(k)$ are prime, for arbitrarily large k.

Dickson's Conjecture was formulated by Leonard Dickson in [4]:

Let $\ell \ge 1$, $f_i(x) = a_i + b_i \cdot x$ with a_i and b_i integers, $b_i \ge 1$ (for $i = 1, \dots, \ell$). If there does not exist any integer $n > 1$ dividing all the products $\Pi^\ell_{i=1} f_i(k)$, for every integer k, then there exist infinitely many natural numbers m such that all numbers $f_1(m), \dots, f_\ell(m)$ are prime.

Dickson's Conjecture implies that in (F) there are arbitrarily large k for which all $x_s(k)$, $|s| \le q$, are prime numbers, provided the following congruence condition is satisfied:

(D) For every prime p there is k such that $p \nmid x_s(k)$ holds for all $|s| \le q$.

So it suffices to show that for every prime p there is a solution $\langle x_s : |s| \le q \rangle$ of (S_q) such that $p \nmid x_s$ holds for all $|s| \le q$.

The condition (C), which guarantees solvability of (R_q), and therefore of (S_q), does not imply (D) (consider the possibility $a_0 = a_1 = 1$, $p = 2$). We formulate a condition that does, for all q.

(E) For every prime number p and every $s \in \mathbb{Z}$:
If $a_s = p^n \cdot a'_s$ with $p \nmid a'_s$, then there is $r \in \mathbb{Z}$ such that $p^{n+1} \mid a_r$ and
$r - s = u \cdot p^n$ where $0 < u < p$.

Lemma 1 *If the sequence $\langle a_s : s \in \mathbb{Z} \rangle$ satisfies the conditions (C) (for all $s, t \in \mathbb{Z}$) and (E), then for every $q > 0$ and every prime number p the system (S_q) has a solution $\langle x_s : |s| \le q \rangle$ such that $p \nmid x_s$ holds for all $|s| \le q$.*

Proof We fix q and p. Let n be the highest exponent such that $p^n \mid a_s$ for some $|s| \le q$. Let $q^* = q + p^{n+1}$. Let $\langle x_s : |s| \le q^* \rangle$ be a solution of the system (S_{q^*}). Since the restriction of this solution to $|s| \le q$ is a solution of (S_q), it suffices to prove that for this solution $p \nmid x_s$ holds for all $|s| \le q$.

We fix s with $|s| \leq q$, write $a_s = p^n \cdot a'_s$ with $p \nmid a'_s$, take r as in (E), and notice that $|r| \leq q^*$. The equation $a_r \cdot x_r - a_s \cdot x_s = r - s$ follows from (S_{q^*}). We thus have $p^{n+1} \cdot a'_r \cdot x_r - p^n \cdot a'_s \cdot x_s = u \cdot p^n$, and after simplifying, $p \cdot a'_r \cdot x_r - a'_s \cdot x_s = u$. If $p \mid x_s$, then $p \mid u$, a contradiction with $0 < u < p$. □

It remains to construct a sequence $\langle a_s : s \in \mathbb{Z} \rangle$ that satisfies (C) and (E). We describe its terms a_s by their prime factorization $\Pi p^{n_p(s)}$. The basic idea is to space those a_s that are divisible by p^n exactly p^n steps apart. (This can be accomplished for $s \geq 0$ by simply putting $a_s = s + 1$; however, we need a sequence that has this property and is defined for all $s \in \mathbb{Z}$.)

Definition 2 For $p > 2$ we let the *anchor*

$$s(p,n) = (p^n + 1)/2;$$

we also let

$$s(2,n) = (1 - (-2)^n)/3 = \Sigma_{i=0}^{n-1}(-2)^i.$$

Lemma 3 *If $m < n$, then $s(p,n) \equiv s(p,m) \mod p^m$.*

Proof For $p > 2$ this follows from $s(p,n) - s(p,m) = (p^n - p^m)/2 = p^m \cdot (p^{n-m} - 1)/2$. Also $s(2,n) - s(2,m) = \Sigma_{i=m}^{n-1}(-2)^i = \pm 2^m \cdot \Sigma_{i=0}^{n-m-1}(-2)^i$. □

Definition 4 For every s, we let $n_p(s)$ be the highest exponent n for which $s \equiv s(p,n) \mod p^n$. A choice of anchors is *admissible* if $n_p(s)$ exists, for all p and s.

We note that, for $p > 2$, $s(p,n) = (p^n + 1)/2 > 0$ and $s(p,n) - p^n = -(p^n - 1)/2 < 0$. Hence for all n such that $|s| < (p^n - 1)/2$ we have $s \not\equiv s(p,n) \mod p^n$, and $n_p(s) \leq \min\{n : 2|s| \leq p^n\}$. Similarly, for all n such that $|s| < |1 - (-2)^{n-1}|/3$ we have $s \not\equiv s(2,n) \mod 2^n$; hence $n_2(s) \leq \min\{n : 3|s| \leq 2^{n-1}\}$. These observations show that our choice of anchors is admissible. Taking $n = 1$ establishes that for $p > 2|s| + 1$ we have $n_p(s) = 0$, so the coefficients $a_s = \Pi p^{n_p(s)}$ are well-defined. A table of a_s for $|s| \leq 12$ is computed below.

n	-12	-11	-10	-9	-8	-7	-6	-5	-4	-3	-2	-1
a_n	5	$2 \cdot 23$	$3 \cdot 7$	$2^2 \cdot 19$	17	$2 \cdot 3 \cdot 5$	13	$2^4 \cdot 11$	3^3	$2 \cdot 7$	5	$2^2 \cdot 3$

n	0	1	2	3	4	5	6	7	8	9	10	11	12
a_n	1	2	3	$2^3 \cdot 5$	7	$2 \cdot 3^2$	11	$2^2 \cdot 13$	$3 \cdot 5$	$2 \cdot 17$	19	$2^5 \cdot 3 \cdot 7$	23

Lemma 5 *The sequence $\langle a_s : s \in \mathbb{Z}\rangle$ satisfies the condition (C) for all $s, t \in \mathbb{Z}$.*

Proof Fix $s, t \in \mathbb{Z}$ and a prime number p. By definition of $n_p(s)$, $s \equiv s(p, n_p(s)) \mod p^{n_p(s)}$, and by definition of a_s, $n_p(s)$ is the highest exponent n for which $p^n \mid a_s$. Similarly, $t \equiv s(p, n_p(t)) \mod p^{n_p(t)}$, and $n_p(t)$ is the highest exponent n for which $p^n \mid a_t$. By Lemma 2, for $m = \min(n_p(s), n_p(t))$ we have $s(p, n_p(s)) \equiv s(p, m) \equiv s(p, n_p(t)) \mod p^m$; hence $s \equiv t \mod p^m$. Thus, for every prime p the highest power of p that divides both a_s and a_t also divides $t - s$. From this the condition (C), to wit, $(a_s, a_t) \mid t - s$, readily follows. □

Lemma 6 *The sequence $\langle a_s : s \in \mathbb{Z}\rangle$ satisfies the condition (E).*

Proof Fix $s \in \mathbb{Z}$ and a prime number p so that $a_s = p^n \cdot a'_s$ and $p \nmid a'_s$; by the construction of a_s, $n = n_p(s)$. There is a unique $k \in \mathbb{Z}$ such that $s(p, n+1) + k \cdot p^{n+1} \leq s < s(p, n+1) + (k+1) \cdot p^{n+1}$; we let $r = s(p, n+1) + k \cdot p^{n+1}$. Then $p^{n+1} \mid a_r$, so in particular $r \neq s$, and $0 < s - r < p^{n+1}$. As $s(p, n+1) \equiv s(p, n) \mod p^n$, we have $r \equiv s(p, n) \equiv s \mod p^n$. Hence $s - r = u \cdot p^n$ and necessarily $0 < u < p$. This proves the condition (E). □

We restate the final result in the language of model theory.

Theorem *Let $({}^*\mathbb{Z}, <, +, \times, 0, 1)$ be an elementary extension of $(\mathbb{Z}, <, +, \times, 0, 1)$ with $\mathbb{Z} \subset {}^*\mathbb{Z}$. Assuming Dickson's Conjecture, there exist $\omega \in {}^*\mathbb{Z} \backslash \mathbb{Z}$ such that every integer in the galaxy of ω, defined as $\mathbf{G}(\omega) = \{\omega - s \mid s \text{ limited}\}$, factors as $\omega - s = a_s \cdot \pi_s$ where $a_s \in \mathbb{Z}$ and π_s is an unlimited prime number. In the example constructed above, the galaxy $\mathbf{G}(\omega)$ contains a unique prime number $\omega = \pi_0$.*

Proof The sequence $\langle a_s : s \in \mathbb{Z}\rangle$ constructed above is first-order definable in the language of $(\mathbb{Z}, <, +, \times, 0, 1)$. The elementary extension assumption is sufficient to conclude that there are $q, r \in {}^*\mathbb{Z} \setminus \mathbb{Z}$ for which the system (S_q) has a solution where all x_s are prime numbers greater than r.

According to the construction, the coefficient a_s is divisible by an odd prime p if and only if $s = (p+1)/2 + k \cdot p$ for some $k \in \mathbb{Z}$ if and only if $2s - 1 = p \cdot (2k+1)$ for some $k \in \mathbb{Z}$. Thus at least one such p exists, except when $s = 1$ and $s = 0$. The coefficient $a_1 = 2$. We conclude that all $\omega_s - s = a_s \cdot \pi_s \in \mathbf{G}(\omega)$ are composite except for $\omega_0 = \pi_0$. □

The proofs that the sequence $\langle a_s : s \in \mathbb{Z}\rangle$ satisfies (C) and (E) go through for every admissible choice of anchors $s(p,n)$. The anchors can be chosen so as to make the galaxy $\mathbf{G}(\omega)$ contain (1) no prime numbers or (2) infinitely many prime numbers.

(1) The following values of $s(p,n)$ guarantee that $a_s \neq 1$ holds for all $s \in \mathbb{Z}$, and hence that $\mathbf{G}(\omega)$ contains no prime numbers. Let $p_1, p_2, \ldots, p_i, \ldots$ be the increasing enumeration of odd primes. We set $s(2,0) = 1$, $s(2,1) = 0$, $s(2,n) = 2^{n-1}$ for $n > 1$; $s(p_i, 0) = 1$, $s(p_{2i}, 1) = i$, $s(p_{2i+1}, 1) = -i$, and $s(p,n) = s(p,1) + p^{n-1}$ for all odd p and all $n > 1$. It is easy to verify that this choice of anchors is admissible.

(2) Dickson's Conjecture implies that there exist sequences of prime numbers of the form

$$\langle c + i \cdot (i+1) : 0 \leq i < \ell\rangle$$

for any ℓ. For $\ell = 2$ they are just the prime twins $\langle c, c+2\rangle$. A remarkable example is the sequence $\langle 41 + i \cdot (i+1) : 0 \leq i < 40\rangle$ of 40 primes. We construct $\mathbf{G}(\omega)$ where $\omega + i \cdot (i+1)$ is a prime number for every $i \in \mathbb{Z}$, $i \geq 0$. This requires a choice of anchors such that, for every prime number p, $s(p,1) \not\equiv -i \cdot (i+1) \mod p$ holds for all $i \geq 0$. As $i \cdot (i+1)$ is even, the requirement is guaranteed for $p = 2$ by choosing $s(2,1) = 1$. For odd primes p the requirement is equivalent to $(2i+1)^2 \not\equiv 1 - 4s(p,1) \mod p$, and thus holds for all $i \geq 0$ whenever $1 - 4s(p,1)$ is a quadratic nonresidue mod p. As there are $(p-1)/2$ equivalence classes $\mod p$ of quadratic nonresidues, and hence also of possible values for $s(p,1)$, we can choose $s(p,1)$ so that $(p-1)/4 \leq s(p,1) \leq (p-1)/2$. This last condition guarantees that the choice of anchors is admissible [if we also let $s(2,n) = (1 - (-2)^n)/3$ and $s(p,n) = s(p,1) + p^{n-1}$ for $n > 1$].

References

[1] **A Boudaoud**, *La conjecture de Dickson et classes particulières d'entiers*, Ann. Math. Blaise Pascal 13 (2006), 103 – 109; https://doi.org/10.5802/ambp.215

[2] **A Boudaoud**, *Decomposition of terms in Lucas sequences*, J. Log. Anal. 1:4 (2009), 1 – 23; https://doi.org/10.4115/jla.2009.1.4

[3] **A Boudaoud**, **D Bellaouar**, *Representation of integers: A nonclassical point of view*, J. Log. Anal. 12:4 (2020) 1{-31; https://doi.org/10.4115/jla.2020.12.4

[4] **L E Dickson**, *A new extension of Dirichlet's theorem on prime numbers*, Messenger of Mathematics 33 (1904), 155 - 161.

Department of Mathematics, City College of CUNY
New York, NY 10031,
khrbacek@icloud.com

Received: 9 October 2019 Revised: 21 October 2020