Journal of Logic & Analysis 12:4 (2020) 1–31
ISSN 1759-9008

Representation of Integers: A nonclassical point of view

BOUDAOUD ABDELMADJID
BELLAOUAR DJAMEL

Abstract: In [2], A. Boudaoud asked the following question: Which $n \in \mathbb{N}$ unlimited can be represented in the form $n = s + \omega_1\omega_2$, where $s \in \mathbb{Z}$ is limited and ω_1, $\omega_2 \in \mathbb{N}$ are unlimited? In this paper we partially answer this question, ie we present some families of unlimited positive integers which can be written as the sum of a limited integer and the product of at least two unlimited positive integers.

2010 Mathematics Subject Classification 26E35,03H05 (primary); 11A51, 11A41, 11B83. (secondary)

Keywords: Representation of integers, Internal set theory, Polynomial congruence.

1 Introduction

The study of representation of integers has a long history. By the Fundamental Theorem of Arithmetic, every positive integer has a unique prime factorization. That is, any integer $n > 1$ is represented by a product of prime powers, ie

$$n = p_1^{k_1} p_2^{k_2} \dots p_r^{k_r} \tag{F$_1$}$$

where $p_1, p_2, \dots, p_r$ are distinct primes and $k_1, k_2, \dots, k_r$ are positive integers. This representation of n, which is unique, is called the canonical factoring of n into prime powers or the standard factorization. When the numbers are sufficiently large, no efficient, non-quantum integer factorization algorithm is known even though a modification of Fermat's difference of squares method is used for factoring large integers. For further reference, we recall that $\omega(n)$ and $\Omega(n)$ are defined by $\omega(n) = r$ which is the number of distinct prime divisors of n and $\Omega(n) = k_1 + k_2 + \dots + k_r$ which is the total number of prime factors of n.

A positive integer n can be, under suitable conditions, represented as a sum of two squares (Nathanson [11, page 427]) or three squares (Mollin [13, page 252]), (for example, $13 = 3^2 + 2^2$ and $126 = 10^2 + 5^2 + 1^2$) or as the difference of two squares as in Fermat's factorization method [13, page 203]. A partition of a nonnegative integer

Published: December 2020 https://doi.org/10.4115/jla.2020.12.4

n is a representation of n as a sum of natural numbers, called parts or summands of the partitions [11, page 455]. The order of the summands does not matter. Thus, we write $n = n_1 + n_2 + \cdots + n_l$, where $n_1 \geq n_2 \geq \cdots \geq n_l$. For example, the partitions of 4 are: 4, $3+1$, $2+2$, $2+1+1$, $1+1+1+1$. We denote the number of such partitions by $p(n)$.

The classical results dealing with the subject of factorization give generally the number of positive integers n in an interval $[1, x]$ whose factorization satisfies a desired condition, which do illustrate that there is some interest in knowing whether there are numbers in some interval having a factorization with a given property. In the following we will cite some examples satisfying this fact:

1. We have the well known result that, for every integers $n \geq 0$ and $k \geq 1$, there is exactly one integer of the set $\{n+1, n+2, \ldots, n+k\}$ which is divisible by k.
2. In Nathanson [11, Theorem 8.9, page 283], we have, for $x \geq 2$,
$$\sum_{n \leq x} \omega(n) = x \log\log x + b_1 x + O\left(\frac{x}{\log x}\right)$$
where b_1 is a positive real number.
3. In Nathanson [11, Hardy–Ramanujan Theorem, page 285], we have, for every $\delta > 0$, the number of integers $n \leq x$ such that $|\omega(n) - \log\log n| \geq (\log\log x)^{(1/2)+\delta}$ is $o(x)$.
4. In Jakimczuk [9] we also have, for a fixed positive integer $k \geq 2$, the number of $2 \leq n \leq s$ having the greatest prime factor strictly greater than n/k is equivalent[1] to $C_k s/\log s$ for some constant C_k. We can cite several other results of this kind.

Notice that in the intervals indicated in these examples, we do not know which are the integers having sufficient prime factors in their canonical factorization even if the length of the interval is unlimited.

Let n be an arbitrary large positive integer. In [2, 3], Boudaoud sought to represent an integer which is in a small neighborhood of n as the product of two large positive integers. Hence the natural framework of this idea is the nonstandard mathematics (see Diener and Reeb [7], F. Diener and M. Diener [8]), because in such a language we can use the words: small, large, etc. Therefore in the framework of the nonstandard

[1] Two number-theoretic functions F and G are said to be equivalent whenever $\frac{F(s)}{G(s)} \to 1$ as s tends to ∞.

mathematics, we take n to be an unlimited positive integer and we look for a standard integer s, which is possibly equal to zero, such that $n - s = \omega_1\omega_2$, ie

$$n = s + \omega_1\omega_2 \tag{F$_2$}$$

where ω_1, ω_2 are two unlimited positive integers. Note that (F$_2$) is equivalent to $n - s = p_1^{k_1} p_2^{k_2} \cdots p_r^{k_r}$, where $\omega(n-s)$ is unlimited or $\Omega(n-s)$ is unlimited or there exists an unlimited prime factor p_{i_j} of $n - s$, ie $1 \leq i_j \leq r$, such that $k_{i_j} \geq 2$ or there exist at least two unlimited distinct prime factors $p_{i_{j_1}}$, $p_{i_{j_2}}$ of $n - s$, ie $1 \leq i_{j_1}, i_{j_2} \leq r$ with $i_{j_1} \neq i_{j_2}$. Furthermore, it raises a question concerning the uniqueness of the limited s which is involved in (F$_2$). That is, we look in an interval of limited length containing n, for integers written as the product of two unlimited integers.

Of course we can generalize the form (F$_2$), while keeping the same conditions on limited s and adding conditions on the factors ω_1 and ω_2; for example assume that an integer n is representable as

$$\begin{cases} n = s + \omega_1\omega_2 \\ m \mid \omega_1\omega_2, \end{cases} \tag{F$_3$}$$

where m is an integer greater than or equal to 2.

We study in this work the representation of integers of certain families in the form (F$_2$) and sometimes in the form (F$_3$). We also note that the problem of representing of any unlimited integer n in the form (F$_2$) is still open. Also, we deal with the representation of unlimited natural numbers as the sum of a limited integer and the product of at least three unlimited positive integers, that is,

$$n = s + \omega_1\omega_2 \cdots \omega_k \tag{F$_4$}$$

where $s \in \mathbb{Z}$ is limited and $\omega_1, \omega_2, \ldots, \omega_k$ are unlimited positive integers with $k \geq 3$.

2 Main results

2.1 General theorem of representation

Theorem 2.1 *Any unlimited positive integer n can be represented in one of the following two forms:*

I. $n = \omega_1\omega_2 + (\omega_3)^2$, *where* $\omega_1, \omega_2 \in \mathbb{Z}$ *are unlimited and* $\omega_3 \in \mathbb{N}$ *is also unlimited.*

II. $n = s + \omega_1\omega_2$, *where* $s \in \mathbb{Z}_+$ *is limited and* ω_1, ω_2 *are unlimited positive integers satisfying* $\frac{\omega_1}{\omega_2} \cong 1$.

Proof We distinguish the following cases:

A) n is a square. Then n is in form II.

B) n is not a square. In this case there exists an unlimited positive integer a with $a < n$ such that $n - a^2$ is odd and positive. Now if $n - a^2$ is limited, then $n = \left(n - a^2\right) + a^2$ and therefore n is in form II; otherwise, from Mollin [13, Exercise 6.2, page 251], $n - a^2 = b^2 - c^2$ for some $b, c > 0$ with b is unlimited, and hence $n = a^2 + b^2 - c^2$. Now we distinguish the following cases:

B.1) $t_1 = b - c$ and $t_2 = a - c$ are limited. Then $b = t_1 + c$ and $a = t_2 + c$. Hence $n = (t_2 + c)^2 + (t_1 + c)^2 - c^2 = c\,(2t_2 + 2t_1 + c) + t_1^2 + t_2^2$. In this case c must be unlimited; otherwise, n becomes limited. Then, n is in form II.

B.2) One of the numbers $t_1 = b - c$ and $t_2 = a - c$ is unlimited. In this case,

$$n = \begin{cases} (b-c)\,(b+c) + a^2, \text{ if } b - c \text{ is unlimited} \\ (a-c)\,(a+c) + b^2, \text{ if } a - c \text{ is unlimited.} \end{cases}$$

Thus, in both cases, n is in form I.

This completes the proof of Theorem 2.1. □

Corollary 2.2 *There are an infinity of values of n which can be represented simultaneously as stated in the two forms of Theorem 2.1.*

Proof Let a, b be positive integers and let $m = a^2 + b^2$. Let c, d be positive integers such that c or d is unlimited. Let us assume furthermore that $ad - bc = s'$ is limited and $ac - bd$ is unlimited. For instance, consider the numbers $a = \omega, b = \omega - 1, c = \omega - 1$ and $d = \omega - 2$ with ω is an unlimited positive integer, which satisfy our assumption.

Now, for $n = c^2 + d^2 \cong +\infty$, it follows from Lagrange's identity (Jarvis [10, Lemma 1.18, page 9]) that $mn = \left(a^2 + b^2\right)\left(c^2 + d^2\right) = (ac - bd)^2 + (ad + bc)^2 = \omega_1\omega_2 + \omega_3^2$, where $\omega_1 = \omega_2 = ac - bd$ and $\omega_3 = ad + bc$ are unlimited. On the other hand, we also have $mn = (ad - bc)^2 + (ac + bd)^2 = s + \omega_1\omega_2$, where $s = \left(s'\right)^2$ is limited and $\omega_1 = \omega_2 = ac + bd$ is unlimited. This completes the proof. □

Recall that in Boudaoud [2], the following result has been proved.

Theorem 2.3 *Assuming Dickson's conjecture (Dickson [6]), for each couple of integers q and k, there exists an infinite subset $L_{q,k} \subset \mathbb{N}$ such that, for each of the integers $n \in L_{q,k}$ and all integers s satisfying $0 < |s| \leq q$, we have $n + s = |s|\, t_1 t_2 \cdots t_k$, where $t_1 < t_2 < \cdots < t_k$ are prime integers.*

Corollary 2.4 *There exist infinitely many natural numbers n such that each of them satisfies: $\forall^{st} s \in \mathbb{Z}^* = \mathbb{Z} - \{0\} : n + s = |s|\, p$, where p is prime.*

Proof The proof follows immediately from Theorem 2.3 by taking $q \cong +\infty$ and $k = 1$. □

We deduce from the construction made in Theorem 2.3 that there exists a family formed by an infinity of unlimited natural numbers n such that each of these numbers is of the form $\omega_1\omega_2$, where ω_1, ω_2 are two unlimited positive integers, and satisfies:

$$\forall^{st} s \in \mathbb{Z}^*,\ n + s = |s|\, p$$

This means that for every limited integer $s \in \mathbb{Z}^*$ the integer $n + s$ cannot be the product of two unlimited positive integers. Then every integer n of the considered infinite family can be written in (F_2) for a unique s (in this case $s = 0$). Thereby the question that arises now is the following: Is there an unlimited positive integer n which is of the form $n = \omega_1\omega_2$, where ω_1, ω_2 are two unlimited positive integers, and at the same time n can be written in (F_2), where $s \in \mathbb{Z}^*$ is a limited integer? The answer to this question is in the following examples, where at first we deal with unlimited integers of the form n^k with $k \geq 2$.

Proposition 2.5 *Let n be an unlimited positive integer and let $k \geq 2$ be a limited integer. Then n^k is of the form $t^k + \omega_1\omega_2$, where $t \in \mathbb{Z}^*$ is limited and ω_1, ω_2 are two unlimited positive integers.*

Proof Let m be an unlimited positive integer such that $n - m = t \neq 0$ is limited. We see that

$$\begin{aligned} n^k &= n^k - m^k + m^k \\ &= (n-m)\left(n^{k-1} + n^{k-2}m + n^{k-3}m^2 + \cdots + nm^{k-2} + m^{k-1}\right) + m^k \\ &= t\left[(m+t)^{k-1} + (m+t)^{k-2}\, m + \cdots + (m+t)\, m^{k-2} + m^{k-1}\right] + m^k \\ &= m\left[m^{k-1} + ktm^{k-2} + c_3t^2m^{k-3} + c_4t^3m^{k-4} + \cdots + c_{k-1}t^{k-2}m + kt^{k-1}\right] + t^k \end{aligned}$$

where $c_3, c_4, \cdots, c_{k-1}$ are positive integers. □

Remark 1 We can prove Proposition 2.5 as follows: Let m be an unlimited positive integer such that $t = n - m$ with $t \in \mathbb{Z}^*$ is limited. Since $n \equiv t \pmod{m}$, it follows that $n^k \equiv t^k \pmod{m}$. Then there exists a positive integer ω such that $n^k = t^k + \omega m$. In this case, ω is unlimited; otherwise,

$$0 = n^k - \left(\omega m + t^k\right) = n\left(n^{k-1} - \omega\right) + \omega t - t^k \cong +\infty,$$

which is a contradiction.

Corollary 2.6 *Let $k \geq 1$ and let $p_k(x)$ be a standard integer-valued polynomial of degree k whose leading coefficient is positive. For any unlimited positive integer n, $np_k(n)$ is of the form $s + \omega_1\omega_2$, where $s \in \mathbb{Z}^*$ is limited and ω_1, ω_2 are two unlimited positive integers.*

Proof Since the polynomial p_k is standard, then there exists a limited integer $t_0 \in \mathbb{Z}^*$ such that $p_k(t_0) \neq 0$. Let m, n be two unlimited positive integers such that $n - m = t_0$. Since $np_k(n) \equiv t_0 p_k(t_0) \pmod{m}$, then $np_k(n) = t_0 p_k(t_0) + \omega m$, for some unlimited integer ω; otherwise,

$$0 = np_k(n) - (m\omega + t_0 p_k(t_0)) = n(p_k(n) - \omega) + t_0(\omega - p_k(t_0)) \cong +\infty$$

since $p_k(n) \cong +\infty$, which is a contradiction. □

Let $\lceil x \rceil$ denote the least integer greater than or equal to x. We have

Theorem 2.7 *Let p and q be two unlimited positive integers which are of the same parity, ie they are both odd or both even. If the difference $p - q$ is a nonzero limited integer then the number $\left\lceil \sqrt{pq} \right\rceil^2$ is of the form $s + pq$, where $s \in \mathbb{Z}^*$ is limited.*

Proof Without loss of generality assume that $p > q$. Set $A = \frac{p+q}{2}$ and $B = \frac{p-q}{2}$. Since $p - q \in \mathbb{N}^*$ is limited, $B < \sqrt{2A-1}$. Therefore,$(A-1) < \sqrt{A^2 - B^2} < A$, hence, $\left\lceil \sqrt{A^2 - B^2} \right\rceil = A$. Thus, $\left\lceil \sqrt{pq} \right\rceil = \frac{p+q}{2}$. It follows that

$$\lceil \sqrt{pq} \rceil^2 - pq = \left(\frac{p+q}{2}\right)^2 - pq$$

and so

$$\lceil \sqrt{pq} \rceil^2 = \left(\frac{p-q}{2}\right)^2 + pq.$$

Since p and q are of the same parity, $p - q$ is even, say s. That is, $s = 2\widetilde{s}$ for some $\widetilde{s} \geq 1$. Consequently, $\left\lceil \sqrt{pq} \right\rceil^2 = \left(\frac{s}{2}\right)^2 + pq = \left(\widetilde{s}\right)^2 + pq$, as required. □

Remark 2 As we stated for p and q in Theorem 2.7, we can also prove that $\lceil \sqrt{pq} \rceil = \frac{p+q}{2}$ by another method. First we recall the following well known formula

$$(1) \qquad \begin{cases} \sqrt{1+x} = 1 + \frac{1}{2}x - \frac{1}{8}x^2 + o\left(x^2\right) \\ o\left(x^2\right) = x^2\theta(x), \text{ where } \theta(x) \to 0 \text{ as } x \to 0 \end{cases}$$

for a standard function θ. Estimate $\sqrt{pq}$ for $p = q + s$. That is, $\sqrt{pq} = q\sqrt{1 + \frac{s}{q}}$. Then by (1), $\sqrt{1 + \frac{s}{q}} = \frac{p+q}{2q} + \frac{s^2}{q^2}\left(-\frac{1}{8} + \theta\left(\frac{s}{q}\right)\right)$. It follows that $\sqrt{pq} = \frac{p+q}{2} +$

$\frac{s^2}{q}\left(-\frac{1}{8}+\theta\left(\frac{s}{q}\right)\right)$. Since $\frac{s}{q}\cong 0$ and $\underset{x\to 0}{\theta(x)}\to 0$, then $\theta\left(\frac{s}{q}\right)\cong 0$. Consequently, $\frac{s^2}{q}\left(-\frac{1}{8}+\theta\left(\frac{s}{q}\right)\right)$ is infinitesimal and strictly negative. This proves the assertion.

2.2 Representation via the perturbation of the factors of n

In this section we take $n=pq$, where p and q are two unlimited positive integers linked together by the relation $p=q-t$. We aim to write n in the form (F_2), ie $n=pq=s+\omega_1\omega_2$ with $s\in\mathbb{Z}^*$ limited and ω_1, ω_2 are two unlimited positive integers. For this purpose, we put $\Delta=(p+s_1)(q+s_2)$, where s_1,s_2 are two integers not both zero. Hence, $\Delta=pq+q(s_1+s_2)+(s_1s_2-ts_2)$. Thus, $pq=\Delta+(ts_2-s_1s_2)-q(s_1+s_2)$, ie

$$n=(p+s_1)(q+s_2)+(ts_2-s_1s_2)-q(s_1+s_2). \tag{2}$$

In the following, it is required that for any choice of t, s_1 and s_2 the sums $p+s_1$ and $q+s_2$ are unlimited positive integers, and that $(ts_2-s_1s_2)-q(s_1+s_2)$ is a nonzero limited integer. We start by choosing t while the choice of the other parameters (such as s_1, s_2,...) comes after. For this reason we distinguish two cases for t.

a) t **is limited.**

Theorem 2.8 *Let n be an unlimited positive integer which is of the form $n=pq$, where $p=q-t$ and $q\cong+\infty$. Then n is written in the form $n=s+\omega_1\omega_2$, such that $s\neq 0$ is a limited integer and ω_1, ω_2 are two unlimited positive integers.*

Proof We have $n=pq=(q-t)q$. Let us take $s_1=l$ and $s_2=-l$, where l is a limited integer such that $tl-l^2\neq 0$. Thus, $\Delta=(p+l)(q-l)$; equivalently,

$$\Delta=pq-pl+lq-l^2=pq-(q-t)l+lq-l^2.$$

Hence $\Delta=pq+lt-l^2$. Consequently, $n=pq=\Delta+l^2-lt$, as required. □

Remark 3 In the case when t is limited we can prove Theorem 2.8 as follows. Let l be a limited positive integer such $l^2-lt\neq 0$. Set $m=q-l$ which is unlimited. Since q is congruent to l (mod m), then $n=q^2-qt\equiv\left(l^2-lt\right)$ (mod m), and therefore $n=l^2-lt+k(q-l)$ for some $k\geq 1$. Here, k is unlimited; otherwise,

$$0=n-\left[l^2-lt+k(q-l)\right]=q(q-t-k)+l(k-l+t)\cong+\infty$$

which is a contradiction.

Remark 4 In view of Remark 3, we can prove that $k = m + 2l - t$. In fact, let m, l be as above. Then clearly $n = (q - m)(q + m) - qt + m^2 = l^2 - lt + m(m + 2l - t)$.

b) t is unlimited.

Theorem 2.9 *Let q, t, γ be positive integers satisfying the following conditions:*

- *$\gamma \neq 0$ is limited.*
- *q, t are unlimited.*
- *$q^2 \equiv \gamma \pmod{t}$ and $q = at^2$ with $a > 0$ is a non infinitesimal real number.*

If $n = (q-t)q$, then there exist two unlimited integers ω_1 and ω_2 such that $n = \gamma + \omega_1\omega_2$.

Remark 5 By Adler and Coury [1, Theorems 5.11-5.12, page 130], we can choose t, γ and q such that $q^2 \equiv \gamma \pmod{t}$ with $q = at^2$ with $0 < a$ is a noninfinitesimal real number. For example, we can take t an unlimited prime of the form $1 + 12k$, $\gamma = 3$ and this implies, by [1, Theorem 5.13 part (ii), page 131], the existence of a solution q_0. Now if q_0 is not like we want, then we add to it a multiple of t until we get the desired value q. This implies that $q - t \cong +\infty$.

Proof of Theorem 2.9 From (2) we have $\gamma = (ts_2 - s_1s_2) - q(s_1 + s_2)$, then $s_2 = \frac{qs_1+\gamma}{t-s_1-q}$. If $s_1 = -q$. Then $s_2 = \frac{-q^2+\gamma}{t} \in \mathbb{Z}$, since by hypothesis $t \mid -q^2 + \gamma$. Now

$$n = pq = ((q - t) + s_1)(q + s_2) + \gamma = -t\left(\frac{tq - q^2 + \gamma}{t}\right) + \gamma.$$

Since $-t$ and $\frac{tq-q^2+\gamma}{t}$ are negative, then $n = \gamma + \omega_1\omega_2$ where $\omega_1 = |-t| = t \cong +\infty$, $\omega_2 = \left|\frac{tq-q^2+\gamma}{t}\right| = \frac{-tq+q^2-\gamma}{t} \cong +\infty$. The proof of Theorem 2.9 is finished. □

Theorem 2.10 *Let r, t, γ be positive integers satisfying the following conditions:*

- *γ is a limited integer different from zero.*
- *r, t are unlimited.*
- *$2t^2 \equiv \gamma \pmod{r}$.*

If $q = 2t + r$ and $n = (q - t)q$, then $n = \gamma + \omega_1\omega_2$, where ω_1, ω_2 are two unlimited integers.

Remark 6 For the choice of theses parameters we can consider the congruence $2x^2 \equiv \gamma \pmod{r}$. If we take for instance $\gamma = 2$, then this equation has a solution $x = 1 + kr$, and we can take $t = 1 + kr$ with k a positive integer.

Proof of Theorem 2.10 From (2) we have $\gamma = (ts_2 - s_1 s_2) - q(s_1 + s_2)$, then $s_2 = \frac{qs_1+\gamma}{t-s_1-q}$. If $s_1 = -t$, then $s_2 = \frac{-qt+\gamma}{2t-q}$. This is an integer, since

$$s_2 = \frac{-qt+\gamma}{2t-q} = \frac{-(2t+r)t+\gamma}{2t-2t-r} = k + r$$

where k is a positive integer. Thus,

$$n = ((q-t)+s_1)(q+k+r)+\gamma = (q-2t)(q+k+r)+\gamma.$$

Then $n = \gamma + \omega_1\omega_2$, where $\omega_1 = q - 2t \cong +\infty$, $\omega_2 = q + k + r \cong +\infty$. □

Remark 7 Other similar results can be obtained by the methods used in the proofs of Theorems 2.9 and 2.10.

Let $n = q_1^{\alpha_1} q_2^{\alpha_2} \cdots q_s^{\alpha_s}$ be an unlimited positive integer with $\Omega(n) \geq 2$, where $s \geq 1$ is a limited integer and for $i = 1, 2, \ldots, s$, q_i is an unlimited prime and $\alpha_i \geq 1$ is a limited positive integer. We can now derive a representation of n in the form (F_2) using its representation as a product of prime factors:

Proposition 2.11 *If there exists an integer m such that $|q_i - m|$ is a limited positive integer for $i = 1, 2, \ldots, s$, then there exists a limited integer $t \in \mathbb{Z}^*$ such that $n = t + \omega_1\omega_2$, where ω_1 and ω_2 are two unlimited positive integers.*

Proof Setting $q_i - m = t_i$, for $i = 1, 2, \ldots, s$. Then each t_i is a limited integer. Hence, for each i, $q_i = t_i + m$. Consequently,

$$n = q_1^{\alpha_1} q_2^{\alpha_2} \cdots q_s^{\alpha_s} = \prod_{i=1}^{s} (t_i + m)^{\alpha_i} = \left(\prod_{i=1}^{s} t_i^{\alpha_i} \right) + mk.$$

Note that the number $\prod_{i=1}^{s} t_i^{\alpha_i}$ is limited since s, $(\alpha_i)_{1\leq i\leq s}$ and $(t_i)_{1\leq i\leq s}$ are also. Moreover, since $\Omega(n) \geq 2$, then m, k are two unlimited positive integers, proving the desired result. □

Proposition 2.12 *Suppose that $n = p^\alpha q^\beta$ is the product of two distinct prime powers, where α, β are unlimited and p, q are limited. Then n is of the form $s + \omega_1\omega_2$, where $s \in \mathbb{Z}^*$ is limited and $\omega_1, \omega_2 \in \mathbb{N}$ are unlimited.*

Proof We distinguish the following cases:

a) α, β are odd. In this case:

$$n = pq + pq\left(p^{\frac{\alpha-1}{2}} q^{\frac{\beta-1}{2}} - 1\right)\left(p^{\frac{\alpha-1}{2}} q^{\frac{\beta-1}{2}} + 1\right)$$

b) α is odd, β is even. In this case:

$$n = p + p\left(p^{\frac{\alpha-1}{2}}q^{\frac{\beta}{2}} - 1\right)\left(p^{\frac{\alpha-1}{2}}q^{\frac{\beta}{2}} + 1\right)$$

c) α is even, β is odd. This case is the same as (b).

d) α, β are even. It is clear that:

$$n = 1 + \left(p^{\frac{\alpha}{2}}q^{\frac{\beta}{2}} - 1\right)\left(p^{\frac{\alpha}{2}}q^{\frac{\beta}{2}} + 1\right)$$

This completes the proof. □

In the case when n is an unlimited prime power we have:

Corollary 2.13 *Let $n = q^\alpha$ be an unlimited prime power with $\alpha \geq 2$. Then n is of the form $s + \omega_1\omega_2$, where $s \in \mathbb{Z}^*$ is limited and ω_1, ω_2 are two unlimited positive integers.*

Proof There are two cases:

Case 1. q is unlimited. In this case, we see that

$$n = 1 + q^\alpha - 1^\alpha = 1 + (q-1)\left(q^{\alpha-1} + q^{\alpha-2} + \cdots + q + 1\right)$$

which is of the form $1 + \omega_1\omega_2$, where ω_1, ω_2 are two unlimited positive integers.

Case 2. q is limited. As in the proof of Proposition 2.12, we have

$$q^\alpha = \begin{cases} 1 + \left(q^{\frac{\alpha}{2}} - 1\right)\left(q^{\frac{\alpha}{2}} + 1\right) & \text{if } \alpha \text{ is even} \\ q + q\left(q^{\frac{\alpha-1}{2}} - 1\right)\left(q^{\frac{\alpha-1}{2}} + 1\right) & \text{otherwise} \end{cases}$$

as required.

□

Remark 8 Let $n = p_1^{\alpha_1}p_2^{\alpha_2}\cdots p_r^{\alpha_r}$ be an unlimited positive integer, where $p_1, p_2, \ldots, p_r$ are distinct prime numbers and $\alpha_1, \alpha_2, \ldots, \alpha_r$ are even positive integers. Set $\alpha_i = 2\beta_i$ with $\beta_i \geq 1$ for $i = 1, 2, \ldots, r$. Then for every limited integer s,

$$n = s^2 + p_1^{2\beta_1}p_2^{2\beta_2}\cdots p_r^{2\beta_r} - s^2 = s^2 + \left(p_1^{\beta_1}p_2^{\beta_2}\cdots p_r^{\beta_r} - s\right)\left(p_1^{\beta_1}p_2^{\beta_2}\cdots p_r^{\beta_r} + s\right)$$

where $p_1^{\beta_1}p_2^{\beta_2}\cdots p_r^{\beta_r} - s$ and $p_1^{\beta_1}p_2^{\beta_2}\cdots p_r^{\beta_r} + s$ are unlimited. Therefore, n can be written as the sum of a limited integer and the product of at least two unlimited positive integers.

2.3 Representation of the values of certain polynomials in the form (F_3)

In this part we consider polynomials $f(x)$ with integer coefficients. In accord with the general goal of this paper, we are looking for the integer values of x for which $f(x)$ is written in the form (F_3).

Proposition 2.14 *Let P be an odd unlimited positive integer. Let r be a positive integer, and let p_r denote the rth prime number. For every standard even integer t in $\mathbb{Z}$, and for every integer x, the polynomial $x^5 - x^3 + P$ cannot be of the form $t + \omega_1\omega_2$, where $\prod_{i=1}^{r} p_i \mid \omega_1\omega_2$.*

Proof Let $t \in \mathbb{Z}$ be an even standard integer. Consider the congruence:

$$x^5 - x^3 + P - t \equiv 0 \left(\mathrm{mod} \prod_{i=1}^{r} p_i\right)$$

We remark that $x^5 - x^3 + P$ is always odd because $x^5 - x^3$ is always even. The congruence $x^5 - x^3 + P - t \equiv 0 \pmod 2$ has no solution, since $x^5 - x^3 + P - t$ is odd. Consequently, the original congruence has no solutions. □

Example 1 Consider the polynomial congruence

$$x^{\omega} - 14x - 4 \equiv 0 \left(\mathrm{mod}\ 7^{\gamma}\right) \tag{3}$$

where ω and γ are two unlimited positive integers such that $7 \nmid \omega$. Find solutions making the value of the polynomial representable in (F_3).

Solution We first consider $f(x) = x^{\omega} - 14x - 4$ and we look for unlimited solutions that make the polynomial into form (F_3). Set $\omega = 6q + r$, where $0 \leq r \leq 5$. Since 0 is not a solution, we can use Fermat's Theorem to conclude that for any solution x, $x^6 \equiv 1 \pmod 7$ and consequently $x^{6q+r} \equiv x^r \pmod 7$. Thus, $f(x) \equiv 0 \pmod 7$ reduces to $x^r - 4 \equiv 0 \pmod 7$. Now, we distinguish the following cases:

a) $r = 0$. In this case the original congruence has no solutions, ie $\forall x\ 7^{\gamma} \nmid f(x)$.

b) $r = 1$. This means that the unique solution is $s_1 = 4$. Since $f'(4) = \omega.4^{\omega-1} - 14$ and $7 \nmid f'(4) = \omega.4^{\omega-1} - 14$, then, by Adler and Coury [1, Corollary 4.11, page 107], there exists precisely one solution $s_{\gamma}(4)$ of $f(x) \equiv 0 \pmod{7^{\gamma}}$ such that $s_{\gamma}(4) \equiv 4 \pmod 7$. Hence $f\left(s_{\gamma}(4)\right) = \left(s_{\gamma}(4)\right)^{\omega} - 14s_{\gamma}(4) - 4 \equiv 0 \pmod{7^{\gamma}}$, which implies that $f\left(s_{\gamma}(4)\right) = 0 + \omega_1\omega_2$, where ω_1 and ω_2 are two unlimited integers and $7^{\gamma} \mid \omega_1\omega_2$.

c) $r = 2$. In this case the only solutions of $f(x) \equiv 0 \pmod 7$ are -2, 2. Since $7 \nmid f'(2) = \omega.2^{\omega-1} - 14$ (respectively $7 \nmid f'(-2) = \omega.(-2)^{\omega-1} - 14$), then by [1, Corollary 4.11, page 107] 2 (respectively -2) generates a unique solution $s_\gamma(2)$ (respectively $s_\gamma(-2)$) modulo 7^γ, where $s_\gamma(2) \equiv 2 \pmod 7$ (respectively $s_\gamma(-2) \equiv -2 \pmod 7$). Hence $f\left(s_\gamma(2)\right) = \left(s_\gamma(2)\right)^\omega - 14s_\gamma(2) - 4 \equiv 0 \pmod{7^\gamma}$ (respectively $f\left(s_\gamma(-2)\right) = \left(s_\gamma(-2)\right)^\omega - 14s_\gamma(-2) - 4 \equiv 0 \pmod{7^\gamma}$), each can be written in form $\omega_1\omega_2$, where ω_1 and ω_2 are two unlimited integers and $7^\gamma \mid \omega_1\omega_2$.

d) $r = 3$. The original congruence has no solutions. Indeed, first 7 is a prime, then it has a primitive root. Since $(7,4) = 1$, we note that $(4)^{\varphi(7)/(3,\varphi(7))} = (4)^2$ which is not congruent to 1 modulo 7. Hence, by [1, Theorem 6.18, page 165], the congruence $f(x) \equiv 0 \pmod 7$ has no solution. Consequently the original congruence has no solution, ie $\forall x \ 7^\gamma \nmid f(x)$ when $r = 3$.

We are content with this, because the cases $r = 4$ and $r = 5$ are done in the same way as above. □

Example 2 Consider the polynomial congruence $x^{12} \equiv 4 \pmod{257}$. Find solutions making the value of the polynomial representable in (F_3).

Solution Since 257 is prime, 257 has a primitive root. Then, by Adler and Coury [1, Theorem 6.18, page 165], the congruence is solvable if and only if $4^{64} \equiv 1 \pmod{257}$. Since $257 = 1 + 8.32$, 2 is a quadratic residue of 257, ie $\left(2/257\right) = 1$. Hence, by Euler's Criterion (see Mollin [13, Theorem 4.2, page 179]), $1 = \left(2/257\right) \equiv 2^{128} \pmod{257}$, which implies $2^{128} \equiv 1 \pmod{257}$, ie $\left(2^2\right)^{64} = 4^{64} \equiv 1 \pmod{257}$. Consequently, the equation in question is solvable and has 4 solutions.

If x_1 is a solution then x_1 is standard and it can not be equal to zero. It is easy to see that $x_1 + 257\omega$, where $\omega \in \mathbb{N}$ is unlimited, is also a solution. Then $(x_1 + 257\omega)^{12} = x_1^{12} + 257\omega.\widetilde{\omega}$, where x_1^{12} is a limited integer and $\widetilde{\omega}$ is an unlimited positive integer. □

Remark 9 In Example 2 we can use instead of 257 a prime number of the form $2^k + 1$ with $k \geq 1$.

Proposition 2.15 *For all unlimited integers ω, there exist an unlimited prime number p and a positive integer n (n is minimal) such that $\omega^n = 1 + \lambda p$, for some unlimited positive integer λ.*

Proof By Bertrand's Postulate (Mollin [13, page 69]), there exists a prime number p such that $\omega < p \leq 2\omega$. Then p is an unlimited and $(p, \omega) = 1$. Let us denote by n the order of ω modulo p, ie $n = ord(\omega)$, so by the minimality of $ord(\omega)$, n is the smallest one. Therefore,

$$\omega^{ord(\omega)} = \omega^n = 1 + \lambda p \tag{4}$$

for some positive integer λ. Since $\omega < p$, then $2 \leq ord(\omega) = n$. Moreover, it follows from (4) that

$$1 = \frac{1}{\omega^n} + \frac{\lambda p}{\omega^n} \tag{5}$$

which implies that λ must be an unlimited positive integer. Otherwise, the right hand side of (5) would be infinitesimal and this is a contradiction. □

Example 3 Let p be an unlimited prime number. Then:

a) If p is of the form $1 + 4k$, then according to Adler and Coury [1, Theorem 5.11, page 130] there exists an integer $\widetilde{x}$ such that $\widetilde{x}^2 = -1 + \lambda_0 p$, for some positive integer λ_0. Since $\widetilde{x} + \lambda p$ is also a solution for every $\lambda \geq 1$, then there exists an unlimited integer x such that $x^2 = -1 + \omega p$, for some unlimited $\omega \in \mathbb{N}$.

b) If p is of the form $\pm 1 + 8k$, then according to the previous example there exists an unlimited integer x such that $x^2 = 2 + \omega p$, where $\omega \in \mathbb{N}$ is unlimited.

c) If p is of the form $\pm 3 + 8k$, then there is no integer x satisfying the equation $x^2 = 2 + \omega p$, where $\omega \in \mathbb{N}$ is unlimited.

Example 4 Consider the congruence $x^2 \equiv 50 \pmod{p}$, where p is an unlimited prime of the form $p = 1 + 8k$. Since $50 = 5^2 \cdot 2$, then $\left(50/p\right) = \left(5^2 \cdot 2/p\right) = \left(2/p\right) = 1$ by Adler and Coury [1, Theorem 5.12, page 130]. Thus, there exists an unlimited integer x such that $x^2 = 50 + \omega p$, where ω is an unlimited positive integer.

Proposition 2.16 *Let $f(x, y) = ax^2 + bxy + cy^2$ be a binary quadratic form with integer coefficients a, b, c such that $a > 0$, $\gcd(a, b, c) = 1$ and the discriminant of f is $\triangle(f) = b^2 - 4ac = d^2$ with $d \in \mathbb{N}$. Let $p \cong +\infty$ be a prime number such that $(a, p) = 1$. Then there are infinitely many couples $(x, y) \in \mathbb{N}^2$ such that $f(x, y) = s + \omega_1\omega_2$ and $p \mid \omega_1\omega_2$, where s is a limited integer and ω_1, ω_2 are two unlimited positive integers. That is, $f(x, y)$ can be written in the form (F_3).*

Proof By Buchmann and Vollmer [4, Formula 1.25, page 17], since $\frac{b+d}{2}$ and $\frac{b-d}{2}$ are integers then

$$f(x, y) = \left(\frac{a}{d_1}x + \frac{1}{d_1}\left(\frac{b+d}{2}\right)y\right)\left(\frac{a}{d_2}x + \frac{1}{d_2}\left(\frac{b-d}{2}\right)y\right) \tag{6}$$

where $d_1 = gcd\left(a, \frac{b+d}{2}\right)$ and $d_2 = gcd\left(a, \frac{b-d}{2}\right)$. Let y be any positive integer such that $(yd, p) = 1$.

Now we prove that the quadratic congruence

$$ax^2 + bxy + cy^2 \equiv 0 \pmod{p} \tag{7}$$

has an infinity of solutions $x \in \mathbb{N}$. Indeed, since $(4a, p) = 1$, we multiply the congruence by $4a$ to get the equivalent congruence $(2ax)^2 + 4abxy + 4acy^2 \equiv 0 \pmod{p}$; that is, $(2ax + by)^2 \equiv y^2\left(b^2 - 4ac\right) \pmod{p}$, and so, $(2ax + by)^2 \equiv (yd)^2 \pmod{p}$. Since $\left((yd)^2/p\right) = 1$, the last congruence has a solution $\widetilde{x}$ which is a solution for the congruence (7). Since $\widetilde{x} + kp$ is a solution of congruence (7) for every integer $k \geq 1$, then (7) has infinitely many positive solutions. Hence the original congruence $f(x, y) \equiv 0 \pmod{p}$ has infinitely many solutions $(x, y) \in \mathbb{N}^2$.

Let us finish the proof. By (6) and (7), we have for every solution (x, y),

$$f(x, y) = \left(\frac{a}{d_1}x + \frac{1}{d_1}\left(\frac{b+d}{2}\right)y\right)\left(\frac{a}{d_2}x + \frac{1}{d_2}\left(\frac{b-d}{2}\right)y\right) = lp \tag{8}$$

where l is a positive integer. Let (x_0, y) be a solution such that for every solution (x, y) with $x \geq x_0$, the factors $\frac{a}{d_1}x + (\frac{b+d}{2d_1})y$ and $\frac{a}{d_2}x + (\frac{b-d}{2d_2})y$ are unlimited positive integers. Note that such x_0 exists because we have an infinity of values of x for which (x, y) is a solution. Hence for $x \geq x_0$: $f(x, y) = 0 + \left(\frac{a}{d_1}x + \frac{1}{d_1}(\frac{b+d}{2})\right)\left(\frac{a}{d_2}x + \frac{1}{d_2}(\frac{b-d}{2})y\right) = \omega_1\omega_2$, where by (8) $\omega_1\omega_2 = lp$. That is, $p \mid \omega_1\omega_2$. □

Remark 10 Each y satisfying the condition $(yd, p) = 1$ allows us to obtain an infinite family of solutions.

Next we look at another problem that actually generalizes (F_2) and (F_3).

2.4 Representation of integers in the form (F_4)

We begin with the following propositions:

Proposition 2.17 *Let $k \geq 2$ be limited. Let n be an unlimited positive integer of the form $s + \omega_1\omega_2$ where $s \in \mathbb{Z}^*$ is limited and $\omega_1, \omega_2 \in \mathbb{N}$ are unlimited. Then n^k can be written in the form $s^k + \omega_1\omega_2\omega_3$ such that $\omega_3 \in \mathbb{N}$ is also unlimited.*

Proof Since $n \equiv s \pmod{\omega_1\omega_2}$, then $n^k \equiv s^k \pmod{\omega_1\omega_2}$. Thus, there exists a positive integer ω_3 such that $n^k = s^k + \omega_1\omega_2\omega_3$, where ω_3 is unlimited; otherwise,

$$0 = n^k - \left(s^k + \omega_1\omega_2\omega_3\right) = (s + \omega_1\omega_2)^k - \left(s^k + \omega_1\omega_2\omega_3\right) \cong +\infty,$$

which gives us the required contradiction. □

We will prove that, for $k \geq 3$, the value of ω_3 in Proposition 2.17 depends on k as follows: $\omega_3 = w_k + n^{k-1}$, where w_k is uniquely determined. More precisely:

Proposition 2.18 *Let n be an unlimited positive integer of the form $s + \omega_1\omega_2$, where $s \in \mathbb{Z}^*$ is limited and ω_1, ω_2 are two unlimited positive integers and let $k \geq 3$ be limited. Then there exists an unlimited positive integer ω_3 such that $n^k = s^k + \omega_1\omega_2\left(w_k + n^{k-1}\right)$, where:*

$$w_k = \begin{cases} s\omega_3, \text{ for } k = 3 \\ s^{k-2}\omega_3 + s^{k-3}n^2 + s^{k-4}n^3 + \cdots + s^2n^{k-3} + sn^{k-2}, \text{ for } k \geq 4 \end{cases}$$

Proof The proof is by induction on k. Assume that $k = 3$. Since $n \equiv s \pmod{(\omega_1\omega_2)}$, then by Proposition 2.17 there exist two unlimited positive integers ω_3, ω_3' such that:

$$\begin{cases} n^2 = s^2 + \omega_1\omega_2\omega_3, \\ n^3 = s^3 + \omega_1\omega_2\omega_3' \end{cases} \tag{9}$$

Therefore, $n^3 = s^3 + s^2\omega_1\omega_2 + s\omega_1\omega_2\omega_3 + \omega_1^2\omega_2^2\omega_3$. Hence by (9), $\omega_3' = s\omega_3 + n^2$. That is,

$$n^3 = s^3 + \omega_1\omega_2\left(s\omega_3 + n^2\right) = s^3 + \omega_1\omega_2\left(w_3 + n^2\right),$$

where $w_3 = s\omega_3$.

If the statement holds for $k \geq 3$, then

$$\begin{aligned} n^{k+1} = n.n^k &= (s + \omega_1\omega_2)\left[s^k + \omega_1\omega_2\left(w_k + n^{k-1}\right)\right] \\ &= s^{k+1} + s\omega_1\omega_2\left(w_k + n^{k-1}\right) + s^k\omega_1\omega_2 + \omega_1^2\omega_2^2\left(w_k + n^{k-1}\right). \end{aligned}$$

Since $n^{k+1} = s^{k+1} + \omega_1\omega_2\omega_3''$ for some unlimited positive integer ω_3'', it follows that

$$\begin{aligned} \omega_3'' &= s\left(w_k + n^{k-1}\right) + s^k + \omega_1\omega_2\left(w_k + n^{k-1}\right) \\ &= s\left(w_k + n^{k-1}\right) + n^k \end{aligned}$$

and hence $n^{k+1} = s^{k+1} + \omega_1\omega_2\left(w_{k+1} + n^k\right)$, where:

$$\begin{aligned} w_{k+1} &= s\left(w_k + n^{k-1}\right) \\ &= s\left(s^{k-2}\omega_3 + s^{k-3}n^2 + s^{k-4}n^3 + \cdots + s^2n^{k-3} + sn^{k-2} + n^{k-1}\right) \\ &= s^{k-1}\omega_3 + s^{k-2}n^2 + s^{k-3}n^3 + \cdots + s^2n^{k-2} + sn^{k-1} \end{aligned}$$

This completes the proof of Proposition 2.18. □

Theorem 2.19 *Let $(t_1, t_2) \in (\mathbb{Z}^*)^2$ be a system of limited integers. Let q be an unlimited positive integer, and let $n = q(q-t_1)(q-t_2)$. If there exists a system of limited integers $(a,b,c) \in (\mathbb{Z}^*)^3$ such that*

$$\text{(10)} \qquad \begin{cases} a+b+c=0 \\ ab+ac+bc=(a+c)t_1+(b+c)t_2 \\ act_1+bct_2-ct_1t_2-abc \neq 0, \end{cases}$$

then n can be written in the form (F_4) with $s \neq 0$.

Proof As in the proof of Theorem 2.8, we set

$$\Delta = (q-t_1+(q-t_1)\phi_1)(q-t_2+(q-t_2)\phi_2)(q+q\phi_3),$$

where $\phi_1 = \frac{a}{q-t_1}, \phi_2 = \frac{b}{q-t_2}$ and $\phi_3 = \frac{c}{q}$. It is not difficult to see that Δ is the product of three unlimited positive integers. Moreover, we see that:

$$\begin{aligned} n &= q(q-t_1)(q-t_2) \\ &= \Delta - q(q-t_1)(q-t_2)[\phi_1+\phi_2+\phi_3+\phi_1\phi_2+\phi_1\phi_3+\phi_2\phi_3+\phi_1\phi_2\phi_3] \\ &= \Delta - (q-t_1)(q-t_2)q[\phi_1+\phi_2+\phi_3+\phi_1\phi_2+\phi_1\phi_3+\phi_2\phi_3] \\ &\quad - q(q-t_1)(q-t_2)\phi_1\phi_2\phi_3 \end{aligned}$$

Using (10), we obtain

$$\begin{aligned} n &= \Delta - \big[abq+ac(q-t_1)+bc(q-t_2)+a(q-t_1)q+b(q-t_2)q \\ &\qquad + c(q-t_1)(q-t_2)\big] - abc \\ &= \Delta - (a+b+c)q^2 + [-at_1-bt_2-(t_1+t_2)c+ab+ac+bc]q \\ &\qquad - act_1-bct_2+ct_1t_2-abc \\ &= \Delta - act_1-bct_2+ct_1t_2-abc \\ &= \Delta - s \end{aligned}$$

where $s = act_1+bct_2-ct_1t_2+abc \neq 0$ is limited. This completes the proof. □

Example 5 Let q be an unlimited positive integer and let $n = q^3+23q^2+42q$. We would like to write n in the form (F_4) with $s \neq 0$. Note also that $n = q(q+2)(q+21)$. By taking $(t_1,t_2) = (-2,-21)$ and $(a,b,c) = (-1,4,-3)$, the equations stated in (10) hold. As in the proof of Theorem 2.19, by computation we see that

$$\Delta = (q-t_1+a)(q-t_2+b)(q+c) = (q-3)(q+6)(q+20),$$

and so $s = -act_1-bct_2+ct_1t_2+abc = -360 \neq 0$. Thus,

$$n = \Delta - s = (q-3)(q+6)(q+20)+360,$$

which is similar to the form (F_4) with $s \neq 0$.

Remark 11 Let n be as above, ie $n = q(q-t_1)(q-t_2)$, where t_1, t_2 are limited integers. If there exist limited integers $a, b, c \in \mathbb{Z}^*$ such that

$$\begin{cases} t_1 + t_2 = a + b + c \\ t_1 t_2 = ab + ac + bc \end{cases} \tag{11}$$

then n can be written in the form (F_4), where $s = abc \in \mathbb{Z}^*$ is limited. In fact, the conditions stated in (11) follow immediately from the equation $n = s+(q-a)(q-b)(q-c)$.

Proposition 2.20 *Let $(t_1, t_2, t_3) \in (\mathbb{Z}^*)^3$ be a system of limited integers. Let q be an unlimited positive integer, and let $n = q\left(q^3 + t_1 q^2 + t_2 q + t_3\right)$. If there exists a system $(a, b, c, d) \in (\mathbb{Z}^*)^4$ of limited integers such that*

$$\begin{cases} t_1 = -a - b - c - d \\ t_2 = ab + ac + ad + bc + bd + cd \\ t_1 t_2 t_3 = -abc - abd - acd - bcd, \end{cases} \tag{12}$$

then n can be written in the form $n = s + \omega_1\omega_2\omega_3\omega_4$, where $s \in \mathbb{Z}^*$ is limited integer and $\omega_1, \omega_2, \omega_3, \omega_4$ are four unlimited positive integers.

Proof The proof follows immediately from the equations stated in (12), since by computation we have $n = (q-a)(q-b)(q-c)(q-d) + s$, where $s = -abcd \in \mathbb{Z}^*$. □

Example 6 Let q be an unlimited positive integer and let $n = q\left(q^3 - 4q^2 - 42q - 36\right)$. Setting $(t_1, t_2, t_3) = (-4, -42, -36)$ and $(a, b, c, d) = (1, -3, -3, 9)$, then equations (12) hold. By Proposition 2.20, n can be written in the form $s + \omega_1\omega_2\omega_3\omega_4$, where $s \in \mathbb{Z}^*$ is limited and ω_i is unlimited for $1 \le i \le 4$. In fact, we see that:

$$\begin{aligned} (q-a)(q-b)(q-c)(q-d) + (-abcd) &= (q-1)(q+3)(q+3)(q-9) + (-81) \\ &= q\left(q^3 - 4q^2 - 42q - 36\right) = n \end{aligned}$$

The following remark generalizes Proposition 2.20.

Remark 12 Let $k \ge 3$ and let $\left(t_1, t_2, \ldots, t_{k-1}\right) \in (\mathbb{Z}^*)^{k-1}$ be a system of limited integers satisfying the following equations

$$\begin{cases} t_1 = \displaystyle\sum_{i=1}^{k-1} a_i \\ t_2 = -\displaystyle\sum_{i<j} a_i a_j \\ \quad \vdots \\ t_{k-1} = (-1)^k \displaystyle\sum_{1 \le i_1 < i_2 < \cdots < i_{k-1} \le k-1} a_{i_1} a_{i_2} \cdots a_{i_{k-1}} \end{cases} \tag{13}$$

for some limited integers $(a_1, a_2, \ldots, a_k)$. Let q be an unlimited positive integer, and let $n = q\left(q^{k-1} + t_1 q^{k-2} + \cdots + t_{k-2}q + t_{k-1}\right)$. Then n has a decomposition $n = s + \omega_1\omega_2\cdots\omega_{k+1}$ such that $s \in \mathbb{Z}^*$ is limited and $\omega_1, \omega_2, \ldots, \omega_{k+1}$ are $(k+1)$ unlimited positive integers. Indeed, by using the equations stated in (13) we can show that $n = (q-a_1)(q-a_2)\cdots(q-a_k) + s$, where $s = (-1)^k a_1 a_2 \cdots a_k$.

Proposition 2.21 *Let $n = s_1 + \omega_1\omega_2$, where $s_1 \in \mathbb{Z}^*$ is a limited integer, ω_1 and ω_2 are two unlimited positive integers. Then $\forall^{st} k \geq 1$, there exist a limited integer s and $k+2$ unlimited positive integers λ_1, $\lambda_2, \ldots, \lambda_{k+1}, \lambda_{k+2}$ such that*

$$n^{2^k} = s + \lambda_1\lambda_2\cdots\lambda_{k+1}\lambda_{k+2}.$$

Proof Let us define the following external formula for $k \geq 1$: $F(k) \equiv$ " $\forall^{st} k \geq 1$, there exist a limited integer s and $k+2$ unlimited positive integers $\lambda_1, \lambda_2, \ldots, \lambda_{k+1}, \lambda_{k+2}$ such that $n^{2^k} = s + \lambda_1\lambda_2\cdots\lambda_{k+1}\lambda_{k+2}$". We will use the external induction principle (F. Diener and M. Diener [8]). For $k = 1$, we have $n^{2^1} = s_1^2 + 2\omega_1\omega_2(s_1 + \omega_1\omega_2)$. Hence $n^2 = s + \lambda_1\lambda_2\lambda_3$, where $s = s_1^2$ is limited and $\lambda_1 = 2\omega_1$, $\lambda_2 = \omega_2$ and $\lambda_3 = s_1 + \omega_1\omega_2$ are unlimited. Assume $F(k)$ for a standard integer $k \geq 1$. We prove $F(k+1)$. Indeed, from the fact that $n^{2^k} = s + \lambda_1\lambda_2\cdots\lambda_{k+1}\lambda_{k+2}$ we have:

$$\begin{aligned} n^{2^{k+1}} &= \left(n^{2^k}\right)^2 = \left(s + \lambda_1\lambda_2\cdots\lambda_{k+1}\lambda_{k+2}\right)^2 \\ &= s^2 + \lambda_1\lambda_2\cdots\lambda_{k+1}\lambda_{k+2}\left(2s + \lambda_1\lambda_2\cdots\lambda_{k+1}\lambda_{k+2}\right) \end{aligned}$$

Then $n^{2^{k+1}}$ is written in the required form, which completes the proof. □

Proposition 2.22 *Let $q \geq 2$ be an integer and t be an unlimited positive integer. For every limited integer $k \geq 1$, the natural number q^{2^t} is of the form $1 + \omega_1\omega_2\cdots\omega_k\omega_{k+1}$, where $\omega_i \cong +\infty$ for $1 \leq i \leq k+1$ and $\omega_{k+1} = q^{2^{t-k}} - 1$.*

Proof Let $F(k)$ be the assertion

$$\begin{aligned} F(k): \quad q^{2^t} &= 1 + \omega_1\omega_2\cdots\omega_k\omega_{k+1}, \text{ where } \omega_i \cong +\infty \text{ for } 1 \leq i \leq k+1 \\ &\text{and } \omega_{k+1} = q^{2^{t-k}} - 1. \end{aligned}$$

For $k = 1$, we have

$$q^{2^t} = 1 + q^{2^t} - 1 = 1 + \left(q^{2^{t-1}} + 1\right)\left(q^{2^{t-1}} - 1\right) = 1 + \omega_1\omega_2,$$

where ω_1, ω_2 are two unlimited positive integer and $\omega_2 = q^{2^{t-1}} - 1$. Hence $F(1)$.

Assume $F(k)$ for a limited integer $k \geq 1$ and prove $F(k+1)$. By $F(k)$ we have $q^{2^t} = 1 + \omega_1\omega_2\cdots\omega_k\omega_{k+1}$, where $\omega_i \cong +\infty$ for $1 \leq i \leq k+1$ and $\omega_{k+1} = q^{2^{t-k}} - 1$. Then $\omega_{k+1} = q^{2^{t-k}} - 1 = \left(q^{2^{t-(k+1)}} + 1\right)\left(q^{2^{t-(k+1)}} - 1\right)$. Hence:

$$q^{2^t} = 1 + \omega_1\omega_2\cdots\omega_k\omega_{k+1} = 1 + \omega_1\omega_2\cdots\omega_k\left(q^{2^{t-(k+1)}} + 1\right)\left(q^{2^{t-(k+1)}} - 1\right)$$

We put $\omega_{k+1} = q^{2^{t-(k+1)}} + 1$ and $\omega_{k+2} = q^{2^{t-(k+1)}} - 1$. Then ω_{k+1} and ω_{k+2} are two unlimited positive integers, and

$$q^{2^t} = 1 + \omega_1\omega_2\cdots\omega_k\omega_{k+1}\omega_{k+2}.$$

Hence $F(k+1)$. Consequently $\forall^{st}k \geq 1\ F(k)$, and this end the proof. □

Let $f(x)$ be a standard integer-valued polynomial of degree k whose leading coefficient is positive and let q be an unlimited positive integer. In general, $f(q)$ can not be written as

$$f(q) = s + \prod_{i=0}^{k}(q - x_i) \tag{14}$$

where x_i are limited integers for $i = 0, 1, \ldots, k$. In the rest of this section we give some examples of such polynomials which do not satisfy (14).

Proposition 2.23 *Let $q \in \mathbb{N}$ be unlimited. The natural number $q\left(q^2 + q + 1\right)$ is not of the form $s + (q-x)(q-y)(q-z)$, where $x, y, z \in \mathbb{Z}^*$ are limited and $s = xyz$.*

Proof Assume, by way of contradiction, that $q\left(q^2 + q + 1\right) = s + (q-x)(q-y)(q-z)$ for some limited integers $x, y, z \in \mathbb{Z}^*$ with $s = xyz$. Since q is unlimited, $1 \cong -x - y - z$, and hence

$$-x - y - z = xy + xz + yz = 1. \tag{15}$$

From (15), it follows that

$$-y^2 - yz - y - z^2 - z - 1 = 0. \tag{16}$$

Now, assume that (y_0, z) is a solutions of the equation (16). Then $-z^2 - (y_0 + 1)z - y_0^2 - y_0 - 1 = 0$. The later equation has no integer solutions because its discriminant $\Delta = -3y_0^2 - 2y_0 - 3$ is negative. This is a contradiction. □

Proposition 2.24 *Let $q \in \mathbb{N}$ be unlimited. The natural number $q\left(q^3 + q^2 + q + 1\right)$ is not of the form $s + (q-x)(q-y)(q-z)(q-t)$, where $x, y, z, t \in \mathbb{Z}^*$ are limited and $s = -xyzt$.*

Proof Assume, by way of contradiction, that

$$q\left(q^3+q^2+q+1\right)=s+(q-x)(q-y)(q-z)(q-t) \tag{17}$$

for some limited integers $x,y,z,t\in\mathbb{Z}^*$ with $s=-xyzt$. Set:

$$\begin{aligned} l_1 &= -t-x-y-z \\ l_2 &= tx+ty+tz+xy+xz+yz \\ l_3 &= -txy-txz-tyz-xyz \end{aligned}$$

In the case when the equality $l_1=l_2=l_3=1$ is not true, we use the relation (17) to obtain:

$$(l_1-1)q^2+(l_2-1)q+l_3-1=0 \tag{18}$$

There are two cases:

- If $l_1\neq 1$, then $(l_1-1)+\frac{(l_2-1)}{q}+\frac{l_3-1}{q^2}=0$. By this, $l_1-1\cong 0$ and therefore $l_1-1=0$, which is absurd.
- If $l_1=1$, then $l_2\neq 1$; otherwise, $l_3=1$. In this case $q=\frac{1-l_3}{l_2-1}$, which is impossible since q is unlimited.

Thus, we have shown that $l_1=l_2=l_3=1$. It follows from (17) that

$$-x^2-xy-xz-x-y^2-yz-y-z^2-z-1=0. \tag{19}$$

Assume that (x_0,y_0,z) is a solutions of the equation (19). Then $-z^2-(x_0+y_0+1)z-x_0^2-x_0y_0-x_0-y_0^2-y_0-1=0$. The later equation has the discriminant $\Delta=-3x_0^2-3y_0^2-2x_0y_0-2x_0-2y_0-3$, which is negative since $\Delta=-2x_0^2-2x_0-2y_0^2-(x_0+y_0)^2-2y_0-3$. Thus, (17) is not valid. □

Next, we shall prove the following result which is a generalization of Propositions 2.23 and 2.24.

Theorem 2.25 *Let $k\geq 2$ be limited and let q be an unlimited positive integer. The natural number $n=q\left(q^k+q^{k-1}+\cdots+q+1\right)$ is not of the form $s+(q-x_0)(q-x_1)\cdots(q-x_k)$, where $x_0,x_1,\ldots,x_k\in\mathbb{Z}^*$ are limited and $s=(-1)^k x_0x_1\cdots x_k$.*

Proof Suppose the contrary. That is,

$$n=q\left(q^k+q^{k-1}+\cdots+q+1\right)=s+(q-x_0)(q-x_1)\cdots(q-x_k), \tag{20}$$

where $x_0, x_1, \ldots, x_k \in \mathbb{Z}^*$ are limited integers and $s = (-1)^k x_0 x_1 \cdots x_k$. By computation, we see that:

$$\begin{aligned} n &= [(q-x_0)(q-x_1)](q-x_2)\cdots(q-x_k)+s \\ &= \left[q^2-(x_0+x_1)q+x_0x_1\right](q-x_2)\cdots(q-x_k)+s \\ &= \left[q^3-(x_0+x_1+x_2)q^2+(x_0x_1+x_0x_2+x_1x_2)q-x_0x_1x_2\right] \\ &\qquad \cdot(q-x_3)\cdots(q-x_k)+s \\ &\vdots \\ &= q^{k+1}-\left(\sum_{i=0}^{k}x_i\right)q^k+\left(\sum_{0\le i<j\le k}x_ix_j\right)q^{k-1}-\left(\sum_{0\le i<j<s\le k}x_ix_jx_s\right)q^{k-1} \\ &\qquad +\cdots+s \end{aligned}$$

Since q is unlimited and $x_0, x_1, \ldots, x_k$ are limited, then by (20), $1 \cong -\sum_{i=0}^{k} x_i$, and therefore:

$$1 = -\sum_{i=0}^{k} x_i \tag{21}$$

Moreover, using (20) once again, $1 \cong \sum_{0\le i<j\le k} x_ix_j$, and therefore:

$$1 = \sum_{0\le i<j\le k} x_ix_j \tag{22}$$

From (21), $x_0 = -x_1 - x_2 - \cdots - x_k - 1$, and by replacing in (22) we obtain:

$$\begin{aligned} 0 &= \sum_{1\le i<j\le k} x_ix_j - 1 \\ &= \left(-\sum_{i=1}^{k}x_i - 1\right)\sum_{i=1}^{k}x_i + \sum_{1\le i<j\le k}x_ix_j - 1 \\ &= -x_k^2 - \left(\sum_{i=1}^{k-1}x_i+1\right)x_k - \sum_{i=1}^{k-1}x_i^2 - 2\sum_{1\le i<j\le k-1}x_ix_j - \sum_{i=1}^{k-1}x_i \\ &\qquad + \sum_{1\le i<j\le k-1}x_ix_j - 1 \\ &= -x_k^2 - \left(\sum_{i=1}^{k-1}x_i+1\right)x_k - \sum_{i=1}^{k-1}x_i^2 - \sum_{1\le i<j\le k-1}x_ix_j - \sum_{i=1}^{k-1}x_i - 1 \end{aligned}$$

That is,

$$-x_k^2-\left(\sum_{i=1}^{k-1}x_i+1\right)x_k-\sum_{i=1}^{k-1}x_i^2-\sum_{1\le i<j\le k-1}x_ix_j-\sum_{i=1}^{k-1}x_i-1=0.$$

Let $\left(x_{1,0},x_{2,0},\ldots,x_{k-1,0}\right)$ be a system of $(k-1)$ limited integers and consider the following quadratic equation:

$$-x^2-\left(\sum_{i=1}^{k-1}x_{i,0}+1\right)x-\sum_{i=1}^{k-1}x_{i,0}^2-\sum_{1\le i<j\le k-1}x_{i,0}x_{j,0}-\sum_{i=1}^{k-1}x_{i,0}-1=0 \tag{23}$$

The later equation has the discriminant

$$\begin{aligned}\Delta&=\left(\sum_{i=1}^{k-1}x_{i,0}+1\right)^2-4(-1)\left[-\left(\sum_{i=1}^{k-1}x_{i,0}^2\right)-\left(\sum_{1\le i<j\le k-1}x_{i,0}x_{j,0}\right)\right.\\&\quad\left.-\left(\sum_{i=1}^{k-1}x_{i,0}\right)-1\right]\\&=-3\sum_{i=1}^{k-1}x_{i,0}^2-2\sum_{1\le i<j\le k-1}x_{i,0}x_{j,0}-2\left(\sum_{i=1}^{k-1}x_{i,0}\right)-3\\&=-2\sum_{i=1}^{k-1}\left(x_{i,0}^2+x_{i,0}\right)-\left(\sum_{i=1}^{k-1}x_{i,0}\right)^2-3\end{aligned}$$

which is negative. Thus, (23) is not valid for every $x\in\mathbb{Z}$. That is, there is no limited value x_k to achieve the equation (23), and therefore (20) is not true. □

Corollary 2.26 *Let $k\ge 3$ be limited and let q be an unlimited positive integer. The natural number $n=q^k$ is not of the form $(q-x_1)(q-x_2)\cdots(q-x_k)+s$, where $x_1,\ldots,x_k\in\mathbb{Z}^*$ are limited and $s=(-1)^k x_1\cdots x_k$.*

Proof As in the proof of Theorem 2.25 if $q^k=(q-x_1)(q-x_2)\cdots(q-x_k)+s$, where $x_1,x_2,\ldots,x_k\in\mathbb{Z}^*$ are limited and $s=(-1)^k x_1x_2\cdots x_k$, we have:

$$0=\sum_{i=1}^{k}x_i \tag{24}$$

$$0=\sum_{1\le i<j\le k}x_ix_j \tag{25}$$

It follows from (24) and (25) that

$$-\sum_{i=2}^{k} x_i^2 - \sum_{2\le i<j\le k} x_i x_j = 0$$

and so
$$-x_k^2 - \left(\sum_{i=2}^{k-1} x_i\right) x_k - \sum_{i=2}^{k-1} x_i^2 - \sum_{2\le i<j\le k-1} x_i x_j = 0.$$

Consider the following quadratic equation,

$$-x^2 - \left(\sum_{i=2}^{k-1} x_i\right) x - \sum_{i=2}^{k-1} x_i^2 - \sum_{2\le i<j\le k-1} x_i x_j = 0, \tag{26}$$

which has no integer solutions since

$$\begin{aligned}\Delta &= \left(\sum_{i=2}^{k-1} x_i\right)^2 - 4(-1)\left(-\sum_{i=2}^{k-1} x_i^2 - \sum_{2\le i<j\le k-1} x_i x_j\right)\\ &= -3\sum_{i=2}^{k-1} x_i^2 - 2\sum_{2\le i<j\le k-1} x_i x_j = -2\sum_{i=2}^{k-1} x_i^2 - \left(\sum_{i=2}^{k-1} x_i\right)^2 < 0.\end{aligned}$$

Thus, there are no limited values $x_2, \ldots, x_k \in \mathbb{Z}^*$ to satisfy the equation (26), and hence the corollary is proved. □

2.5 Examples of the natural numbers of the form $\pm 1 + \omega_1\omega_2$ where ω_1, ω_2 are unlimited

There are several identities of the form $F \equiv \pm 1 \pmod{n}$, where n may or may not be a prime. For example, Fermat's Little Theorem, Wilson's Theorem and its consequences, Unique Sums of Two Squares (Nathanson [11, Theorem 13.4, page 407]), Criterion for Power Residue Congruences (Mollin [13, Theorem 3.10, page 155]) and many others. For this purpose, we survey some examples of families of unlimited positive integers which can be written in the form $\pm 1 + \omega_1\omega_2$, where ω_1, ω_2 are two unlimited positive integers. That is, we give unlimited integers n satisfying $n \equiv \pm 1 \pmod{\omega_1\omega_2}$, where $\omega_1, \omega_2 \in \mathbb{N}$ are unlimited.

1. Let n be an unlimited positive integer and let $k \ge 2$. Since $n^k = (-1 + (n+1))^k$, n^k is of the form $(-1)^k + \omega(n+1)$, for some unlimited positive integer ω.

2. Let n be an unlimited positive integer. Then n^5+n^4 is of the form $-1+\omega_1\omega_2$, where ω_1,ω_2 are two unlimited positive integers[2]. In fact, we see that $n^5+n^4 = -1+\left(n^2+n+1\right)\left(n^3-n+1\right)$.
3. Let m,n be two unlimited positive integers with $m\leq n$. If $(m+n)|(m-1)(n-1)$ then mn is of the form $-1+\omega_1\omega_2$, where ω_1,ω_2 are two unlimited positive integers. In fact, we see that $mn = -1+\left(\frac{(m-1)(n-1)}{m+n}+1\right)(m+n)$, where $\frac{(m-1)(n-1)}{m+n}\geq\frac{(m-1)(n-1)}{2n}\cong+\infty$. As an example, $m=n^2-n-1$ with $n\cong+\infty$.
4. Let ω be an unlimited positive integer. From Nathanson [11, Theorem 3.9, page 95], $5^{2^\omega}\equiv 1+3\cdot 2^{\omega+2}\pmod{2^{\omega+4}}$. Then 5^{2^ω} is of the form $1+\omega_1\omega_2$, where ω_1,ω_2 are two unlimited positive integers.
5. If there exists an unlimited prime number p such that $2p-1$ is a perfect square, then p is of the form $1+\omega_1\omega_2$, where ω_1,ω_2 are two unlimited positive integers. In fact, assume that $2p-1=n^2$ for some odd n. Setting $\omega=\frac{n-1}{2}$, hence $n=2\omega+1$ and therefore,
$$p=\frac{1+n^2}{2}=\frac{1+(2\omega+1)^2}{2}=1+2\omega+2\omega^2=1+2\omega(\omega+1).$$
This completes the proof.
6. Let n be an unlimited positive integer and let k be an unlimited integer with $k\leq n+2$. Since $(k-1)$ divides $(n+1)!+k-1$, the expression $(n+1)!+k$ is of the form $1+\omega_1\omega_2$, where ω_1,ω_2 are two unlimited positive integers.

Example 7 Let ω be an unlimited positive integer and let $k\geq 2$. Using different ways we show that k^{2^ω} can be written as $\pm 1+\omega_1\omega_2$, where ω_1,ω_2 are two unlimited positive integers.

Form 1. It is clear that $k^{2^\omega}=1+\left(k^{2^\omega/2}-1\right)\left(k^{2^\omega/2}+1\right)$.

Form 2. Assume that k is odd. By induction on n, we prove that 2^{n+2} divides $k^{2^n}-1$. If $n=1$, then 8 divides $k^2-1=(k-1)(k+1)$ since 2 divides both $k-1$ and $k+1$, and 4 divides one of the numbers $k-1$ and $k+1$ (set $k=2s+1$ for some $s\geq 1$; if s is even, then 4 divides $k-1$ and if s is odd, then 4 divides $k+1$). Assume that 2^{n+2} divides $k^{2^n}-1$. As $k^{2^n}+1$ is even, we have $2^{n+3}=2\cdot 2^{n+2}$ divides $\left(k^{2^n}-1\right)\left(k^{2^n}+1\right)$. Thus, $k^{2^\omega}=1+r\cdot 2^{\omega+2}$ for some unlimited positive integer r, which is different from those of $k^{2^\omega/2}-1$ and $k^{2^\omega/2}+1$.

[2]Let n be an unlimited integer. Using some properties of congruence or the Euclidean algorithm, we can write n^k+n^{k-1} in the form $2+\omega_1\omega_2$ for every $k\geq 2$, where ω_1,ω_2 are two unlimited positive integers.

Form 3. Assume that k is unlimited. Then:

$$\begin{aligned} k^{2^\omega} &= 1+(k-1)\left(k^{2^\omega-1}+k^{2^\omega-2}+\cdots+k+1\right) \\ &= -1+(k+1)\left(k^{2^\omega-1}-k^{2^\omega-2}+\cdots-k+1\right) \end{aligned}$$

Theorem 2.27 *Let $k \geq 1$. Let $p = 2n+1$ be an unlimited prime number and let $d_i = i$, for $i = 1, 2, \ldots, 2n$. Define the polynomial of degree $2n-1$ by:*

$$p(x) = \left(\sum d_i\right) x^{2n-1} - \left(\sum_{i<j} d_i d_j\right) x^{2n-2} + \left(\sum_{i<j<k} d_i d_j d_k\right) x^{2n-2} - \cdots - d_1 d_2 \cdots d_{2n}$$

Let $k \geq 2$ and $s \leq 2n$. For every $a \in \{2, 3, \ldots, kp-s\}$ with a and p relatively prime, $p(a)$ is of the form $1+\omega_1\omega_2$, where ω_1, ω_2 are two unlimited positive integers with $p \mid \omega_1\omega_2$.

Proof Using a result stated in Adler and Coury [1, Problem 4.11, page 114] we can write:

$$\begin{aligned} -p(x)+1 &= -x^{2n} + x^{2n} - \left(\sum d_i\right) x^{2n-1} + \left(\sum_{i<j} d_i d_j\right) x^{2n-2} \\ &\quad - \left(\sum_{i<j<k} d_i d_j d_k\right) x^{2n-2} + \cdots + (-1)^{2n} d_1 d_2 \cdots d_{2n} + 1 \\ &= x^{2n} - \left(\sum d_i\right) x^{2n-1} + \left(\sum_{i<j} d_i d_j\right) x^{2n-2} \\ &\quad - \left(\sum_{i<j<k} d_i d_j d_k\right) x^{2n-2} + \cdots + d_1 d_2 \cdots d_{2n} + 1 - x^{2n} \\ &= (1-x)(2-x)(3-x)\cdots(2n-x) + 1 - x^{2n} \end{aligned}$$

Assume that $2 \leq a \leq p-1$. Since $(a, p) = 1$, it follows from Fermat's little theorem that $-p(a)+1 = 1-a^{2n} = 1-a^{p-1} \equiv 0 \pmod{p}$. Assume that $p < a \leq kp-s$ with $2 \leq s \leq p-1$. Let $F(x) = (1-x)(2-x)(3-x)\cdots(2n-x)$. From Fermat's little theorem once again, we obtain $-p(a)+1 \equiv F(a) \pmod{p} \equiv 0 \pmod{p}$, since p divides $F(a)$. In both cases, $p(a) = 1+\omega p$ for some unlimited positive integer ω. □

We end this section by giving a sequence of positive integers of the form $1+\omega_1\omega_2$ such that the product of its first $k-$terms can be written uniquely in the form $-1+\omega_1\omega_2$, where ω_1, ω_2 are two unlimited positive integers.

Proposition 2.28 *Consider the sequence given in De Koninck and A Mercier [5, pages 56-57] by* $x_0 = 2$ *and* $x_k = x_0x_1\cdots x_{k-1} + 1$ *for* $k \geq 1$. *The first few terms are* $2, 3, 7, 43, 1807, 3263443, \ldots$. *For each unlimited positive integer* n, $x_0x_1\cdots x_{n-2}x_n$ *is of the form* $-1 + \omega_1\omega_2$, *where* ω_1, ω_2 *are two unlimited positive integers*[3].

Proof Since $\frac{1}{x_0} + \frac{1}{x_1} + \cdots + \frac{1}{x_n} + \frac{1}{x_0x_1\cdots x_n} = 1$, it follows that

$$x_1x_2\cdots x_n + x_0x_2\cdots x_n + \cdots + x_0x_1\cdots x_{n-2}x_n + x_0x_1\cdots x_{n-1} + 1 = x_0x_1\cdots x_n$$

that is,

$$\begin{aligned} x_0x_1\cdots x_{n-2}x_n = &-1 + x_0x_1\cdots x_n - x_1x_2\cdots x_n - x_0x_2\cdots x_n - \cdots - x_0x_1\cdots x_{n-2}x_n \\ &- x_0x_1\cdots x_{n-1} = -1 + x_{n-1}\omega \end{aligned}$$

where

$$\omega = x_0x_1\cdots x_{n-2}x_n - x_1x_2\cdots x_{n-2}x_n - x_0x_2\cdots x_{n-2}x_n - \cdots - x_0x_2\cdots x_{n-2}$$

is unlimited since $\frac{x_0x_1\cdots x_{n-2}x_n}{x_{n-1}}$ is also. □

2.6 In classical terms

Finally, we give the classical equivalent statement to the fact that every unlimited positive integer can be written in the form (F_2). Unfortunately, we could not prove it in the general case. The nonclassical statement can be written as

$$\forall N \left(\forall^{st} i\, (i < N)\right) \Rightarrow \exists^{st} s\ \exists \omega_1, \omega_2\ \forall^{st} r\ \ (N = s + \omega_1\omega_2\ \&\ \min(\omega_1, \omega_2) > r)$$

where $N, i, r, \omega_1, \omega_2 \in \mathbb{N}$ and $s \in \mathbb{Z}$. By using the idealization principle (I), the last formula is equivalent to

$$\begin{aligned} \forall N \Big[&\left(\forall^{st} i (i < N)\right) \Rightarrow \\ &\exists^{st} s\ \forall^{st\,fin} R\ \exists\, (\omega_1, \omega_2)\ \ \forall r \in R\ \ (N = s + \omega_1\omega_2\ \&\ \min(\omega_1, \omega_2) > r) \Big] \end{aligned}$$

where R belongs to the set of finite parts of $\mathbb{N}$. This last formula is equivalent to:

$$\begin{aligned} \forall N\ \exists^{st}(i, s)\ \ \forall^{st\,fin} R\ \big[&(i < N) \Rightarrow \\ &\exists\, (\omega_1, \omega_2)\ \ \forall r \in R\ \ (N = s + \omega_1\omega_2\ \&\ \min(\omega_1, \omega_2) > r) \big] \end{aligned}$$

[3] For each unlimited n and for each limited $k \geq 1$, by definition, the term x_n is of the form $1 + \omega_1\omega_2\cdots\omega_k$, where $\omega_1, \omega_2, \ldots, \omega_k$ are k unlimited positive integers.

By the extension principle, this last formula is equivalent to

$$\forall N\ \forall^{st}\widetilde{R}\ \exists^{st}(i,s)\ \big[(i<N)\Rightarrow \exists(\omega_1,\omega_2)\ \forall r\in\widetilde{R}(i,s)\ \ (N=s+\omega_1\omega_2\ \&\ \min(\omega_1,\omega_2)>r)\big]$$

where $\widetilde{R}$ is a mapping from $\mathbb{N}\times\mathbb{Z}$ to the set of finite parts of $\mathbb{N}$. Then:

$$\forall^{st}\widetilde{R}\ \forall N\ \exists^{st}(i,s)\ \big[(i<N)\Rightarrow \exists(\omega_1,\omega_2)\ \forall r\in\widetilde{R}(i,s)\ \ (N=s+\omega_1\omega_2\ \&\ \min(\omega_1,\omega_2)>r)\big]$$

By using the idealization principle (I), the last formula is equivalent to

$$\forall^{st}\widetilde{R}\ \exists^{st\,fin}S\ \forall N\ \exists(i,s)\in S\ \big[(i<N)\Rightarrow \exists(\omega_1,\omega_2)\ \forall r\in\widetilde{R}(i,s)\ \ (N=s+\omega_1\omega_2\ \&\ \min(\omega_1,\omega_2)>r)\big]$$

where S belongs to the set of finite parts of $\mathbb{N}\times\mathbb{Z}$. By the transfer principle (T), this last formula is equivalent to:

$$\forall\widetilde{R}\ \exists^{fin}S\ \forall N\ \exists(i,s)\in S\ \big[(i<N)\Rightarrow \exists(\omega_1,\omega_2)\ \forall r\in\widetilde{R}(i,s)\ \ (N=s+\omega_1\omega_2\ \&\ \min(\omega_1,\omega_2)>r)\big] \tag{27}$$

Let us look at what (27) means by considering the following illustration. Let ω be a positive integer large enough. Define the function $\widetilde{R}$ from $\mathbb{N}\times\mathbb{Z}$ to the set of finite parts of $\mathbb{N}$ by:

$$\widetilde{R}(m,n)=\left\{\left(m+|n|+\omega\right)^{\omega}\right\}$$

It follows from (27) that:

$$\exists^{fin}S\ \forall N\ \exists(i,s)\in S\ \big[(i<N)\Rightarrow \exists(\omega_1,\omega_2)\ \ \left(N=s+\omega_1\omega_2\ \&\ \min(\omega_1,\omega_2)>\left(i+|s|+\omega\right)^{\omega}\right)\big] \tag{28}$$

The formula (28) is valid for any $N>\max\{\mathrm{Pr}_1(S)\}$, where $\mathrm{Pr}_1(S)$ means the first projection of S. Also we notice from (28) the smallness of s compared to ω_1 and ω_2.

2.7 Open questions and final thoughts

We conclude with a (very non-exhaustive) list of open questions which have arisen along the way. As we mentioned earlier in the introduction, if we consider an unlimited positive integer we do not know whether it is possible to factorize it into a product of smaller unlimited integers. Also if we consider an unlimited positive integer which is the product of two unlimited integers, that is $n=\omega_1\omega_2$ where $\omega_1,\omega_2\in\mathbb{N}$ are unlimited,

we do not know whether it can be written as the sum of a nonzero limited integer and the product of at least two unlimited positive integers, for example, $n = s + \omega_1'\omega_2'$ where $s \in \mathbb{Z}^*$ is limited and $\omega_1', \omega_2' \in \mathbb{N}$ are unlimited. Even if this last representation is possible, we do not have valuable information whether the factors ω_1', ω_2' are coprime, semiprime, squarefree,. . . ; or neither. Also this work may develop a generalization of the factoring of unlimited Gaussian integers and unlimited matrices with integer entries. For these reasons, all of the following questions are worth pursuing.

1. Let n be an unlimited positive integer of the form $s + \omega_1\omega_2$, where $s \in \mathbb{Z}^*$ is limited and ω_1, ω_2 are two unlimited positive integers and let d be a limited divisor of n. We ask if n/d is of the form $s' + \omega_1'\omega_2'$, where $s' \in \mathbb{Z}^*$ is limited and ω_1', ω_2' are two unlimited positive integers.[4]

2. Let q be an unlimited positive integer and let $(a_i)_{0\leq i\leq k-1}$ be limited integers, where $k \geq 2$ is limited. Then $q\left(a_{k-1}q^{k-1} + \cdots + a_1q + a_0\right)$ is of the form $s + \omega_1\omega_2\cdots\omega_k$, where $s \in \mathbb{Z}^*$ is limited and ω_j is unlimited for $1 \leq j \leq k$. This problem is solvable for $k = 2$ by congruences.

3. Let p be an unlimited prime number of the form $a\omega + b$, where $a, b \geq 1$ are limited. We ask if p is of the form $s + \omega_1\omega_2$, where $s \in \mathbb{Z}^*$ and ω_1, ω_2 are two unlimited positive integers.

4. Let n be an unlimited positive integer of the form $1 + \omega_1\omega_2$. We ask if n is also of the form $-1 + \omega_1'\omega_2'$. In fact, assume that $n = 1 + \omega_1\omega_2 = -1 + \omega_1'\omega_2'$ for some unlimited positive integers $\omega_1, \omega_2, \omega_1', \omega_2'$. Let $\omega_1' = \omega_1 + x$ and $\omega_2' = \omega_2 + y$, where $x, y \in \mathbb{Z}^*$. We must have $\omega_1 y + \omega_2 x + xy = 2$. Generally, it is not so easy to solve this nonlinear equation.

5. Let n be an unlimited positive integer of the form $s + \omega_1\omega_2$, where $s \in \mathbb{Z}^*$ is limited and ω_1, ω_2 are two unlimited positive integers. We ask if n is also of the form $s' + \omega_1'\omega_2'$, where $s' \in \mathbb{Z}^*$ is limited and $\omega_1', \omega_2' \in \mathbb{N}$ are unlimited and relatively prime.

6. Let n be an unlimited positive integer. First, we ask if n can be written in the form $s + \omega_1\omega_2$, where $s \in \mathbb{Z}^*$ is unlimited and ω_1, ω_2 are two unlimited positive integers satisfying the condition $\frac{s}{\omega_1} \cong \frac{s}{\omega_2} \cong 0$. Second, we ask if n can be written in the form $s + \omega_1\omega_2$, where $s \in \mathbb{Z}^*$ is unlimited and ω_1, ω_2 are two unlimited positive integers satisfying the condition $\frac{s}{\omega_1\omega_2} \cong 0$. As an example concerning the second part of this question, we have the following proposition:

[4] In the case when d divides both n and s, then n/d is of the form $s' + \omega_1'\omega_2'$, *where* $s' \in \mathbb{Z}^*$ *is limited and* ω_1', ω_2' *are also two unlimited positive integers.*

Proposition 2.29 *Let n be an unlimited positive integer and let $\pi(n)$ be the number of primes not exceeding n. Then $n\pi(n-1)$ is of the form $s+\omega_1\omega_2$, where $s \in \mathbb{Z}^*$ and ω_1, ω_2 are two unlimited positive integers satisfying the condition $s/(\omega_1\omega_2) \cong 0$.*

Proof Setting $s = n\pi(n-1) - (n-1)\pi(n)$, we show that $\frac{s}{(n-1)\pi(n)} \cong 0$. In fact, since $\frac{\pi(n-1)}{\pi(n)} \cong \frac{n-1}{n} \cong 1$, we have $\frac{s}{n\pi(n)} = \frac{\pi(n-1)}{\pi(n)} - \frac{n-1}{n} \cong 0$. Let $\frac{s}{n\pi(n)} = \phi \cong 0$. It follows that $n-1 = \frac{s-\pi(n)\phi}{\pi(n)\phi}$, and therefore

$$\frac{s}{(n-1)\pi(n)} = \frac{s\phi}{s-\pi(n)\phi} = \frac{n-1}{n}\phi \cong 0,$$

as claimed. □

7. Let $S(x)$ be the sum of the digits of the positive integer x in its decimal representation. It is clear that we can find at least two unlimited positive integers n, m such that $S(n)$ is limited, $S(m)$ is unlimited and $S(nm) = s+\omega_1\omega_2$, where $\omega_1, \omega_2 \in \mathbb{N}$ are unlimited. For example, $n = 10^t$ with $t \geq 0$, and:

$$m = \underbrace{11\ldots1}_{\omega_1\omega_2\text{-times}}$$

Here, $S(n) = 1$, $S(m) \cong +\infty$ and $S(nm) = \omega_1\omega_2$. But, it is not so easy to find two unlimited positive integers n, m such that $S(n) \cong S(m) \cong +\infty$, $|S(n) - S(m)| = 1$ and $S(nm)$ can be written in the form $s+\omega_1\omega_2$.

8. Recall that several factoring algorithms has been generalized using Gaussian integers. First, we need to the following definition:

Definition 2.30 Let $\alpha = a+bi \in \mathbb{Z}[i]$ be a Gaussian integer and let $N(\alpha)$ be its norm. If either a or b is unlimited, α is said to be unlimited. Otherwise, α is said to be limited. Thus, $\alpha \in \mathbb{Z}[i]$ is unlimited if and only if $N(\alpha)$ is also. If both a and b are unlimited, α is said to be completely unlimited.

In view of the above definition, is it possible to characterize unlimited Gaussian integers $z \in \mathbb{Z}[i]$ which can be written in the form $s+\omega_1\omega_2$, where $s \in \mathbb{Z}[i]$ is limited and $\omega_1, \omega_2 \in \mathbb{Z}[i]$ are unlimited (respectively completely unlimited)?

9. Let A be an $m \times n$ matrix with integer entries. If one of its entries is unlimited, then A is said to be unlimited; otherwise, A is said to be limited. Given an $m \times n$ unlimited matrix A with integer entries, we ask if there are two unlimited matrices $\Omega_1(u \times k)$ and $\Omega_2(k \times v)$ such that

$$A = S + \Omega_1\Omega_2,$$

where $S(m \times n)$ is a nonzero limited matrix with integer entries.

Acknowledgements. The authors would like to thank the Referees and Editor for valuable comments on refinements of an earlier version of the present paper. This research work is supported by The General Direction of Scientific Research and Technological Development (DGRSDT)-Algeria.

References

[1] **A Adler**, **J E Coury**, *The theory of numbers:* A text and source book of problems, Jones and Bartlett Publ., Boston (1995); ISBN-10:0867204729

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

[3] **A Boudaoud**, *Decomposition of terms in Lucas sequences*, J. Log. Anal. 1:4 (2009), 1-23; Published: 16 April 2009; https://doi.org/10.4115/jla.2009.1.4

[4] **J Buchmann, U Vollmer,** *Binary quadratic forms*. In Binary Quadratic Forms (pp. 9-20). Springer, Berlin, Heidelberg (2007); https://doi.org/10.1007/978-3-540-46368-9_2

[5] **J M De Koninck**, **A Mercier**, *1001 problems in classical number theory*, Ellipses Edition Marketing S.A, Paris (2004)

[6] **L E Dickson**, *History of the Theory of Numbers*, Vol. 1, Chelsea, New York (1992); https://archive.org/details/historyoftheoryo01dick

[7] **F Diener**, **G Reeb**, *Analyse non-standard,* Hermann Éditeurs des Sciences et des Arts (1989)

[8] **F Diener**, **M Diener**, *Nonstandard analysis in practice*, Springer Science & Business Media (1995); https://doi.org/10.1007/978-3-642-57758-1

[9] **R Jakimczuk**, *A note on the greatest prime factor*, Notes on Number Theory and Discrete Mathematics, Vol. 20 (2014), No. 4, 77–80; ISSN 1310–5132

[10] **F Jarvis**, *Algebraic Number Theory*, Springer (2014); https://doi.org/10.1007/978-3-319-07545-7

[11] **M B Nathanson**, *Elementary methods in number theory*, Springer-Verlag, New York (2000); https://doi.org/10.1007/b98870

[12] **E Nelson**, *Internal set theory*: *A new approach to nonstandard analysis*. Bull. Am. Math. *Soc*. 83 (1977), 1165–1198; https://doi.org/10.1090/S0002-9904-1977-14398-X

[13] **R A Mollin**, *Fundamental number theory with applications*. Second Edition, Chapman & Hall/Crc (2008); https://doi.org/10.1201/b15895

[14] **R L Rivest**, **A Shamir, L Adleman**, *A method for obtaining digital signature and public key cryptosystems*, Comm. ACM, vol 21 (1978), 120-126; https://doi.org/10.1145/359340.359342

[15] **I P Van den Berg, V Neves (eds.)**, *The Strength of Nonstandard Analysis*. Springer, Wien (2007); https://doi.org/10.1007/978-3-211-49905-4

[16] **I P Van Den Berg**, *Extended use of IST*, Ann. Pure Appl. Logic. *58* (1992), 73-92; https://doi.org/10.1016/0168-0072(92)90035-X

Laboratory of Pure and Applied Mathematics (LMPA), University of M'sila, B.P. 166, Ichbilia, 28000 M'sila, Algeria.

University 08 Mai 1945 Guelma, Department of Mathematics, B.P. 401 Guelma 24000, Algeria.

abdelmadjid.boudaoud@univ-msila.dz, bellaouar.djamel@univ-guelma.dz
bellaouardj@yahoo.fr

Received: 15 April 2019 Revised: 1 November 2020