SCIENTIA
Series A: *Mathematical Sciences*, Vol. 29 (2019), 11–28
Universidad Técnica Federico Santa María
Valparaíso, Chile
ISSN 0716-8446

A closed-form solution might be given by a tree. Valuations of quadratic polynomials

Leyda Almodovar[a], Alyssa N. Byrnes [b], Julie Fink[c], Xiao Guan[b], Aashita Kesarwani[b], Gary Lavigne[b], Luis A. Medina[d], Victor H. Moll[b], Isabelle Nogues[e], Senthil Rajasekaran[b], Eric Rowland[f] and Amber Yuan[g]

Abstract. The p-adic valuation of an integer x is the largest power of the prime p that divides x. It is denoted by $\nu_p(x)$. This work describes properties of the valuation $\nu_2(n^2+a)$, with $a \in \mathbb{N}$. A distinction of the behavior of these valuations for $a \equiv 7 \bmod 8$ or not is presented.

1. Introduction

The fact that the *central binomial coefficients* $C_n = \binom{2n}{n}$ are even numbers is often discussed in elementary courses. The proof usually comes from pointing out that Pascal's triangle is symmetric with respect to its centerline and that C_n is obtained by adding the two middle adjacent elements from the previous row. This yields $\binom{2n}{n} = 2\binom{2n-1}{n}$, and the problem has been solved.

The curious reader now will ask whether it is possible to find a *closed-form* for the exact power of 2 that divides C_n. This is denoted by $\nu_2(C_n)$ and is called the 2-*adic valuation* of C_n. More general, if p is a prime number and $x \in \mathbb{N}$, then $\nu_p(x)$, the p-adic valuation of x, is defined as the highest power of p that divides x.

The identity $\nu_p(C_n) = \nu_p((2n)!) - 2\nu_p(n!)$ reduces the valuation of C_n to that of factorials. For this task, the formula $\nu_p(n!) = \lfloor n/p \rfloor + \lfloor n/p^2 \rfloor + \cdots$ given by Legendre [**7**] is well-known. An alternative version can be given in terms of the expansion $n = a_0 + a_1 p + a_2 p^2 + \cdots + a_r p^r$ of n in base p. Observe that this expansion already contains the formula $\nu_p(n) = \min\{j \,:\, a_j \neq 0\}$. In the case of factorials one uses the function $s_p(n) = a_0 + a_1 + \cdots + a_r$ to write Legendre's formula as

$$\nu_p(n!) = \frac{n - s_p(n)}{p-1}. \tag{1.1}$$

2010 *Mathematics Subject Classification.* Primary 11A07, Secundary 11S05.
Key words and phrases. valuations, quadratic polynomials, congruences modulo 8.

Since the sums of digits $s_p(n)$ is comparable to $\ln n$, it follows that $\nu_p(n!) \sim n/(p-1)$ as $n \to \infty$. In the particular case $p = 2$, the formula (1.1) implies the identity

$$\nu_2(C_n) = \nu_2((2n)!) - 2\nu_2(n!) = 2s_2(n) - s_2(2n) = s_2(n), \tag{1.2}$$

where the last step follows from the fact that the binary expansion of $2n$ is obtained by appending a 0 at the end of the expansion for n. It follows from here that C_n is always even and that $C_n/2$ is odd precisely when n is a power of 2. Then $\nu_2(C_n) = s_2(n)$ deserves to be called a closed-form.

The question of what constitute a closed-form answer to a problem depends on the context. This has been discussed in [**3**] in reference to *special numbers* and recently in [**2**] for *special functions*.

This work discusses the valuation $\nu_2(n^2 + a)$ for $a \in \mathbb{N}$. This is the simplest class of polynomials and the analysis of these valuations contain all the features appearing in the general situation.

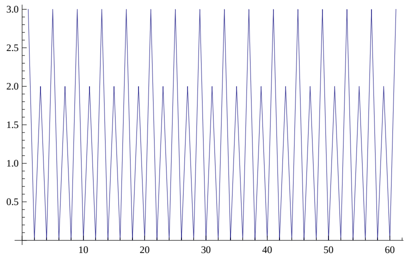

FIGURE 1. The valuation $\nu_2(n^2 + 8)$ for $0 \leqslant n \leqslant 40$

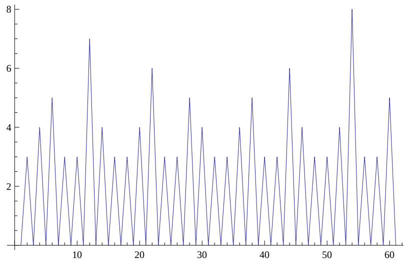

FIGURE 2. The valuation $\nu_2(n^2 + 7)$ for $0 \leqslant n \leqslant 40$

The main result is expressed in terms of sums of squares. Recall a famous theorem of Lagrange stating that every positive integer can be written as a sum of four squares [**5**]. It turns out that $\nu_2(n^2 + a)$ has a different type of behavior depending whether a needs four squares or not.

2. The construction of a tree

Let p be a prime and $f(x)$ a polynomial with integer coefficients. Then

$$f(i+mp) \equiv f(i) \bmod p. \tag{2.1}$$

Therefore the values of $f(i) \bmod p$ are determined by those in the list

$$\mathbb{L}_1 := \{f(0) \bmod p,\ f(1) \bmod p, \cdots, f(p-1) \bmod p\}. \tag{2.2}$$

Lemma 2.1. Assume $i_0 \in \{0,\, 1, \cdots, p-1\}$ satisfies $f(i_0) \not\equiv 0 \bmod p$. Then

$$\nu_p(f(i)) = 0 \text{ for any } i \equiv i_0 \bmod p. \tag{2.3}$$

Example 2.2. Let $f(x) = x^2 + 3x + 15$ and $p = 7$. Then the list in (2.2) is

$$\mathbb{L}_1 = \{1,\, 5,\, 4,\, 5,\, 1,\, 6,\, 6\} \tag{2.4}$$

so it follows that, as n runs over $\mathbb{N}$, the value $f(n)$ is never divisible by 7.

It remains to discuss the indices i_0 with $f(i_0) \equiv 0 \bmod p$. Then (2.1) implies $\nu_p(f(i_0 + mp)) \geqslant 1$, but a larger value of the valuation is possible. In order to determine this value, observe that every number congruent to $i_0 \bmod p$ is in the set

$$\{i_0 + jp + mp^2 :\ 0 \leqslant j \leqslant p-1 \text{ and } m \in \mathbb{N}\}.$$

Moreover,

$$f(i_0 + jp + mp^2) \equiv f(i_0 + jp) \bmod p^2. \tag{2.5}$$

Therefore, the values of $f(i) \bmod p^2$ for the indices $i \equiv i_0 \bmod p$ are determined by the values

$$\mathbb{L}_2 := \left\{f(i_0) \bmod p^2,\ f(i_0+p) \bmod p^2, \cdots, f(i_0 + (p-1)p) \bmod p^2\right\}. \tag{2.6}$$

As before, if a value in the list $\mathbb{L}_1$ is not zero, then a valuation is determined.

Lemma 2.3. Let $i_0,\, i_1 \in \{0,\, 1, \cdots, p-1\}$ satisfy

$$f(i_0) \equiv 0 \bmod p \text{ and } f(i_0 + i_1 p) \not\equiv 0 \bmod p^2. \tag{2.7}$$

Then

$$\nu_p(f(i)) = 1 \text{ for any } i \equiv i_0 + i_1 p \bmod p^2. \tag{2.8}$$

Example 2.4. Let $f(x) = x^2 + 3x + 17$ and $p = 7$. The list $\mathbb{L}_1$ shows that $f(i) \not\equiv 0 \bmod 7$ if $i \equiv 0,\, 2,\, 4,\, 5,\, 6 \bmod 7$. The evaluations $f(1) = 21$ and $f(3) = 35$ imply that $f(i_0) \equiv 0 \bmod 7$ for $i \equiv 1,\, 3 \bmod 7$. The list $\mathbb{L}_2$ for $i_0 = 1$ is $\{21,\, 7,\, 42,\, 28,\, 14,\, 0,\, 35\}$. Thus the vertex corresponding to $i_1 = 5$ satisfies $f(1 + 7 \cdot 5 + 7^2 n) \equiv 0 \bmod 7^2$ and the process continues. The remaining vertices have valuation 1:

$$\nu_7(1 + 7j + 7^2 n) = 1, \text{ for } j = 0,\, 1,\, 2,\, 3,\, 4,\, 6. \tag{2.9}$$

The situation for $i_0 = 3$ is similar.

Continuing this process produces the next result.

Lemma 2.5. Assume there are indices $i_0, i_1, \cdots, i_{n-1} \in \{0, 1, \cdots, p-1\}$ satisfying

$$\begin{aligned} f(i_0) &\equiv 0 \quad \text{mod } p \\ f(i_0 + i_1 p) &\equiv 0 \quad \text{mod } p^2 \\ f(i_0 + i_1 p + i_2 p^2) &\equiv 0 \quad \text{mod } p^3 \\ \cdots & \cdots \quad \cdots \\ f(i_0 + i_1 p + i_2 p^2 + \cdots + i_n p^n) &\not\equiv 0 \quad \text{mod } p^{n+1}. \end{aligned}$$

Then any index $i \equiv i_0 + i_1 p + \cdots + i_n p^n \text{ mod } p^{n+1}$, satisfies

$$\nu_p(f(i)) = n. \tag{2.10}$$

The process described above can be explained in terms of a tree. The construction starts with a *root vertex* that forms the *zeroth level.* This is split into p vertices at the *first level* corresponding to the values $i \text{ mod } p$. The values of the polynomial f on these vertices, taken modulo p, gives the list $\mathbb{L}_1$. The vertices are joined to the root level as indicated in Figure 3.

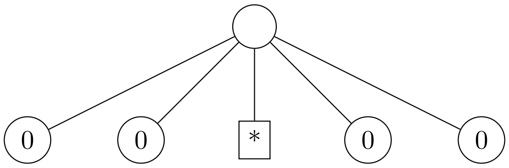

FIGURE 3. The first level of a tree

In case none of the values $f(i)$ in $\mathbb{L}_1$ are divisible by p, the process stops and $\nu_p(f(i)) = 0$ for every $i \in \mathbb{N}$. An example of this situation is given by $p = 2$ and $f(x) = x^2 + x + 1$. The other option is that there is vertex with index $i_0 \text{ mod } p$ for which $f(i_0) \equiv 0 \text{ mod } p$. This generates p descendants, simply by considering all possible remainders modulo p^2 of a number congruent to $i_0 \text{ mod } p$. They are part of the *second level.* These vertices are labelled by $i \equiv i_0 + i_1 p \text{ mod } p^2$, where $i_1 \in \{0, 1, \cdots, p-1\}$ and they are joined to the vertex i_0 as shown in Figure 4. The valuation $\nu_p(f(i))$ is completely determined for indices $i \equiv i_0 + i_1 p \text{ mod } p^2$ for which $f(i_0 + i_1 p) \not\equiv 0 \text{ mod } p^2$. Lemma 2.3 shows that, in this case, $\nu_p(f(i)) = 1$. On the other hand, each index i_1 for which $f(i_0 + i_1 p) \equiv 0 \text{ mod } p^2$, is split into p new vertices that are connected to $i_0 + i_1 P$ to form part of the *third level* and the process continues.

Now imagine that it is possible to continue the process described above indefinitely. In terms of the tree, this corresponds naturally to the notion of an *infinite branch.* But what is the arithmetic meaning of a such a phenomena? The sequence of indices generated to come an infinite brach have the form

$$i_0, \, i_0 + i_1 p, \, i_0 + i_1 p + i_2 p^2, \cdots \tag{2.11}$$

and the vertices along this branch satisfy

$$i \equiv i_0 \text{ mod } p, \, i \equiv i_0 + i_1 p \text{ mod } p^2, \;\, i \equiv i_0 + i_1 p + i_2 p^2 \text{ mod } p^3, \cdots . \tag{2.12}$$

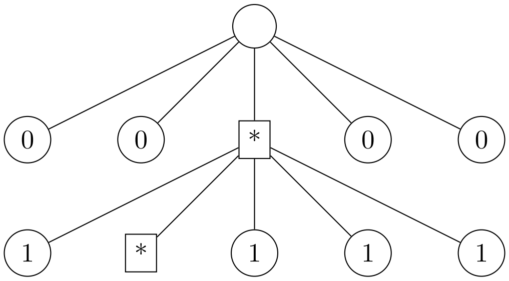

FIGURE 4. The second level of a tree

Introduce the notation

$$a_n = i_0 + i_1 p + i_2 p^2 + \cdots + i_{n-1} p^{n-1}. \tag{2.13}$$

Then the integers $a_n \to \infty$ if convergence is defined in the usual manner. On the other hand, the integers a_n satisfy

$$\begin{array}{lll} (1) & 0 \leqslant a_n < p^n & \text{for } n = 1,\, 2,\, 3,\, \cdots \\ (2) & a_n \equiv a_{n+1} \bmod p^n & \text{for } n = 1,\, 2,\, 3,\, \cdots . \end{array}$$

These properties may be found in Theorem 2, page 11 of [**6**] or in [**4**, page 83] where the name *coherent sequence* is used. The point is that conditions (1) and (2) guarantee that the sequence $\{a_n : n \in \mathbb{N}\}$ corresponds to a *Cauchy sequence in* $\mathbb{Q}_p$. This is the field of *p-adic numbers*, defined as the completion of $\mathbb{Q}$ under the absolute value

$$\begin{array}{rcll} |x|_p & = & p^{-\nu_p(x)} & \text{for } x \neq 0 \\ |0|_p & = & 0. & \end{array} \tag{2.14}$$

In other words, the sequence of indices corresponding to an infinite branch converges to a p-adic number $x \in \mathbb{Q}_p$. The reader unfamiliar with these concepts, should think of these numbers as analogues of real numbers. They simply come from $\mathbb{Q}$ by completion, same as $\mathbb{R}$. A nice introduction to these ideas, aside from the text already mentioned above, is the book by F. Gouvea [**4**]. Now that the limiting value of the sequence of indices has been identified as $x \in \mathbb{Q}_p$, what can be said about the limiting value of $f(a_n)$? The relation (2.10) shows that $\nu_p(f(x)) = +\infty$; that is, $f(x) = 0$. Of course, this requires f to be a continuous function in this new way of measuring convergence. *How can this not be true?* It turns out that this is a simple exercise and details are left to the reader. In summary:

Theorem 2.6. Any infinite branch in the tree associated to the polynomial f corresponds to a root of $f(x) = 0$ in the p-adic field $\mathbb{Q}_p$.

Corollary 2.7. The p-adic valuation $\nu_p(f(n))$ admits a closed-form formula if the equation $f(x) = 0$ has no solutions in $\mathbb{Q}_p$.

3. The 2-adic valuations of $n^2 + a$

The tree associated to a prime p and a polynomial f, described in the previous section, is given in detail for the case $p = 2$ and $f(x) = x^2 + a$ with fixed $a \in \mathbb{N}$. A direct computation of the values $\nu_2(n^2 + a)$ using a symbolic language, will show that this sequence admits a simple closed-form for $a \not\equiv 4, 7 \bmod 8$ and for these two remaining cases, the valuation is quite complicated. One of the goals in the next sections is to shed light on this phenomena. The reasons behind this are connected to the analysis of the equation $x^2 + a = 0$ in the ring of p-adic integers and the presence of infinite branches. This quadratic example contains all the ingredients for the analysis of $\nu_2(f(n))$ for a general polynomial.

Lemma 3.1. For $n \in \mathbb{N}$ and $a \equiv 1 \bmod 4$

$$\nu_2(n^2 + a) = \nu_2(n^2 + 1) = \begin{cases} 1 & \text{if } n \text{ is odd} \\ 0 & \text{if } n \text{ is even.} \end{cases}$$

Proof. To verify this, write $a = 4t + 1$. If n is even, then $n^2 + a$ and $n^2 + 1$ are both odd and the valuations match. In the case $n = 2m + 1$, then

$$n^2 + a = 2(2m^2 + 2m + 2t + 1) \text{ and } n^2 + 1 = 2(2m^2 + 2m + 1), \tag{3.1}$$

and the valuations also match. □

The same argument works for $a \equiv 2 \bmod 4$.

Lemma 3.2. For $n \in \mathbb{N}$ and $a \equiv 2 \bmod 4$,

$$\nu_2(n^2 + a) = \nu_2(n^2 + 2) = \begin{cases} 0 & \text{if } n \text{ is odd} \\ 1 & \text{if } n \text{ is even,} \end{cases}$$

It remains to analyze the classes $a \equiv 0,\ 3 \bmod 4$. These require to consider residues modulo 8, namely $a \equiv 0,\ 3,\ 4,\ 7 \bmod 8$. The case $a \equiv 3 \bmod 8$ is simple.

Lemma 3.3. For $n \in \mathbb{N}$ and $a \equiv 3 \bmod 8$. Then

$$\nu_2(n^2 + a) = \nu_2(n^2 + 3) = \begin{cases} 2 & \text{if } n \text{ is odd} \\ 0 & \text{if } n \text{ is even.} \end{cases}$$

Proof. Write $a = 8t + 3$. If n is even, then $n^2 + a$ and $n^2 + 3$ are both odd, therefore their valuations agree. If n is odd, say $n = 2m+1$, then $n^2+3 = 4(m^2+m+1)$ has valuation 2 and so does $n^2 + a = 4(m^2 + m + 2t + 1)$. □

The discussion of the case $a \equiv 0 \bmod 8$ is divided into two cases according to whether $a \equiv 0$ or $8 \bmod 16$. In the first case it is easy to produce a closed-form formula.

Lemma 3.4. For $n \in \mathbb{N}$ and $a \equiv 8 \bmod 16$

$$\nu_2(n^2 + a) = \nu_2(n^2 + 8) = \begin{cases} 0 & \text{if } n \equiv 1 \bmod 2 \\ 2 & \text{if } n \equiv 2 \bmod 4 \\ 3 & \text{if } n \equiv 0 \bmod 4. \end{cases} \tag{3.2}$$

Proof. Write $a = 8(2s+1)$. If n is odd, then so is $n^2 + a$ and both valuations are 0. If $n \equiv 2 \bmod 4$, write $n = 4t+2$ and use $n^2 + a = 4(4t^2 + 4t + 4s + 3)$ to conclude that $\nu_2(n^2+a) = \nu_2(n^2+8) = 2$. Finally, if $n \equiv 0 \bmod 4$, write $n = 4t$ and use $n^2 + a = 8(2t^2 + 2s + 1)$ to verify that both valuations match. □

For values of $a \equiv 0 \bmod 16$, the valuation $\nu_2(n^2+a)$ is related to $\nu_2(m^2 + a/4)$. This yields an iterative procedure.

Lemma 3.5. Let $n \in \mathbb{N}$ and $a \equiv 0 \bmod 16$. Then

$$\nu_2(n^2+a) = \begin{cases} 0 & \text{if } n \text{ is odd} \\ 2 + \nu_2\left(\left(\frac{n}{2}\right)^2 + \frac{a}{4}\right) & \text{if } n \text{ is even.} \end{cases} \tag{3.3}$$

The initial condition for this procedure is $a = 4$. A closed-form expression for $\nu_2(n^2+4)$ is presented next.

Lemma 3.6. Let $n \in \mathbb{N}$. Then

$$\nu_2(n^2+4) = \begin{cases} 0 & \text{if } n \equiv 1 \bmod 2 \\ 3 & \text{if } n \equiv 2 \bmod 4 \\ 2 & \text{if } n \equiv 0 \bmod 4. \end{cases} \tag{3.4}$$

Proof. If $n \equiv 1 \bmod 2$, then n^2+4 is odd. If $n \equiv 2 \bmod 4$, write $n = 4t+2$ and observe that $n^2 + 4 = 8(2t^2 + 2t + 1)$ to conclude that $\nu_2(n^2+4) = 3$. The case $n \equiv 0 \bmod 4$ is similar. □

Example 3.7. Consider the case $a = 16$. Lemma 3.5 gives

$$\nu_2(n^2+16) = \begin{cases} 0 & \text{if } n \text{ is odd} \\ 2 + \nu_2\left(\left(\frac{n}{2}\right)^2 + 4\right) & \text{if } n \text{ is even.} \end{cases} \tag{3.5}$$

Lemma 3.6 then shows that

$$\nu_2(n^2+16) = \begin{cases} 0 & \text{if } n \equiv 1, 3, 5, 7 \bmod 8 \\ 2 & \text{if } n \equiv 2, 6 \bmod 8 \\ 5 & \text{if } n \equiv 4 \bmod 8 \\ 4 & \text{if } n \equiv 0 \bmod 8. \end{cases} \tag{3.6}$$

The final case is $a \equiv 4 \bmod 8$.

Lemma 3.8. Let $n \in \mathbb{N}$ and $a \equiv 4 \bmod 8$. Then $\nu_2(n^2+a)$ either has a closed-form or it can be reduced to $\nu_2(m^2+7)$.

Proof. Write $a = 8t+4$ and observe that

$$\nu_2(n^2+a) = \nu_2(n^2+8t+4) = 0 \tag{3.7}$$

if n is odd. If $n = 2m$, then

$$\nu_2(n^2+a) = \nu_2(4m^2+8t+4) = 2 + \nu_2(m^2+2t+1). \tag{3.8}$$

The last function reduces to $\nu_2(m^2+a_1)$ with a_1 odd. This implies the statement since there are closed-form formulas for $a \equiv 1, 3, 5 \bmod 8$. □

Example 3.9. Let $a = 12$. Then n^2+12 is odd for n odd. Therefore $\nu_2(n^2+12) = 0$ in this case. On the other hand if n is even, say $n = 2m$, it follows that

$$\nu_2(n^2+12) = 2 + \nu_2(m^2+3) = \begin{cases} 4 & \text{if } m \equiv 1 \bmod 2, \\ 0 & \text{if } m \equiv 0 \bmod 2. \end{cases} \tag{3.9}$$

This produces

$$\nu_2(n^2+12) = \begin{cases} 2 & \text{if } n \equiv 0 \bmod 4 \\ 0 & \text{if } n \equiv 1,\, 3 \bmod 4 \\ 4 & \text{if } n \equiv 2 \bmod 4. \end{cases} \tag{3.10}$$

Example 3.10. The case $a = 20$ is similar. Clearly $\nu_2(n^2+20) = 0$ if n is odd. For n even, say $n = 2m$,

$$\nu_2(n^2+20) = 2 + \nu_2(m^2+5) \tag{3.11}$$

and the expression

$$\nu_2(n^2+20) = \begin{cases} 0 & \text{if } n \equiv 1,\, 3 \bmod 4 \\ 3 & \text{if } n \equiv 2 \bmod 4 \\ 2 & \text{if } n \equiv 0 \bmod 4 \end{cases} \tag{3.12}$$

now follows from Lemma 3.1.

Example 3.11. The final example is $a = 28$. It is clear that $\nu_2(n^2+28) = 0$ if n is odd. On the other hand, if $n = 2m$, then the valuation is reduced to the case $n = 7$ in view of

$$\nu_2(n^2+28) = 2 + \nu_2(m^2+7). \tag{3.13}$$

The final case, $a \equiv 7 \bmod 8$ is discussed in the next section. This section concludes with the formulas for $\nu_2(n^2+a)$ when $1 \leqslant a \leqslant 30$.

$a = 1, 5, 9, 13, 17, 21, 25, 29 \cdots$ (Lemma 3.1):

$$\nu_2(n^2+a) = \begin{cases} 0 & \text{if } n \equiv 0 \bmod 2 \\ 1 & \text{if } n \equiv 1 \bmod 2. \end{cases}$$

$a = 2, 6, 10, 14, 18, 22, 26, 30, \cdots$ (Lemma 3.2):

$$\nu_2(n^2+2) = \begin{cases} 0 & \text{if } n \equiv 1 \bmod 2, \\ 2 & \text{if } n \equiv 0 \bmod 2. \end{cases}$$

$a = 3, 11, 19, 27, \cdots$ (Lemma 3.3):

$$\nu_2(n^2+3) = \begin{cases} 2 & \text{if } n \equiv 1 \bmod 2, \\ 0 & \text{if } n \equiv 0 \bmod 2. \end{cases}$$

$a = 4$ (Lemma 3.6):

$$\nu_2(n^2+4) = \begin{cases} 0 & \text{if } n \equiv 1,\,3 \bmod 4 \\ 3 & \text{if } n \equiv 2 \bmod 4 \\ 2 & \text{if } n \equiv 0 \bmod 4. \end{cases}$$

$a = 8,\, 24,\, \cdots$ (Lemma 3.4):

$$\nu_2(n^2+8) = \begin{cases} 0 & \text{if } n \equiv 1,\,3 \bmod 4 \\ 2 & \text{if } n \equiv 2 \bmod 4 \\ 3 & \text{if } n \equiv 0 \bmod 4. \end{cases}$$

$a = 12$ (Example 3.9):

$$\nu_2(n^2+12) = \begin{cases} 2 & \text{if } n \equiv 0 \bmod 4 \\ 0 & \text{if } n \equiv 1,\,3 \bmod 4 \\ 4 & \text{if } n \equiv 2 \bmod 4. \end{cases}$$

$a = 16$ (Example 3.7):

$$\nu_2(n^2+16) = \begin{cases} 0 & \text{if } n \equiv 1,\,3,\,5,\,7 \bmod 8 \\ 2 & \text{if } n \equiv 2,\,6 \bmod 8 \\ 5 & \text{if } n \equiv 4 \bmod 8 \\ 4 & \text{if } n \equiv 0 \bmod 8. \end{cases}$$

$a = 20$ (Example 3.10):

$$\nu_2(n^2+20) = \begin{cases} 0 & \text{if } n \equiv 1,\,3 \bmod 4 \\ 3 & \text{if } n \equiv 2 \bmod 4 \\ 2 & \text{if } n \equiv 0 \bmod 4. \end{cases}$$

$a = 28$ (Example 3.11):

$$\nu_2(n^2+28) = \begin{cases} 0 & \text{if } n \text{ is odd,} \\ 2 + \nu_2\left(\left(\frac{n}{2}\right)^2 + 7\right) & \text{if } n \text{ is even.} \end{cases}$$

The only values of a, in the range $1 \leqslant a \leqslant 30$, not included in the previous list are $a = 7,\, 15,\, 23$. These are discussed in the next section.

4. The 2-adic valuation of n^2+7

Given a polynomial $f(x)$ with integer coefficients, the sequence $\{\nu_2(f(n)) : n \in \mathbb{N}\}$ has been described via a tree. This is called the *valuation tree attached to* f. The vertices correspond to some selected classes

$$C_{m,j} = \{2^m i + j : i \in \mathbb{N}\}, \tag{4.1}$$

starting with the root vertex v_0 for $C_{0,0} = \mathbb{N}$. The procedure to select the classes is explained below in the example $f(x) = x^2 + 16$. This produces an alternative way of the formula in Example 3.7. Some notation for the vertices of the tree is introduced next.

Definition 4.1. A residue class $C_{m,j}$ is called *terminal* for the tree attached to f, if the valuation $\nu_2\left(f(2^m i + j)\right)$ is independent of the index $i \in \mathbb{N}$. Otherwise it is called *non-terminal*. The same terminology is given to vertices. In the tree, terminal vertices are marked by their constant valuation and non-terminal vertices are marked with a star.

Example 4.2. The construction of the tree for $\nu_2(n^2 + 16)$ starts with the fact that $\nu_2(1^2 + 16) = 0$ and $\nu_2(2^2 + 16) = 2 \neq 0$, showing that the root node v_0 is non-terminal. This node is split into two vertices that form the first level. These correspond to $C_{1,0} = \{2i : i \in \mathbb{N}\}$ and $C_{1,1} = \{2i + 1 : i \in \mathbb{N}\}$. For the class $C_{1,0}$, the valuation

$$\nu_2((2i)^2 + 16) = 2 + \nu_2(i^2 + 4)$$

depends on i, so $C_{1,0}$ is non-terminal. For the class $C_{1,1}$,

$$\nu_2((2i + 1)^2 + 16) = \nu_2(4i^2 + 4i + 17) = 0,$$

showing that $C_{1,1}$ is a terminal class with valuation 0. Figure 5 shows the root and the first level of the tree associated to $\nu_2(n^2 + 16)$.

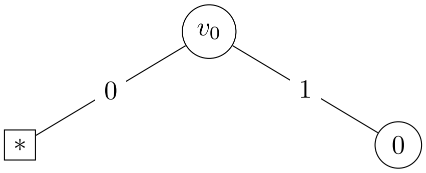

FIGURE 5. The root and the first level of the tree for $\nu_2(n^2 + 16)$

The class $C_{1,0}$ is now split into $C_{2,0} = \{4i : i \in \mathbb{N}\}$ and $C_{2,2} = \{4i + 2 : i \in \mathbb{N}\}$. These two classes form the second level. For $C_{2,0}$, the valuation

$$\nu_2((4i)^2 + 16) = 4 + \nu_2(i^2 + 1)$$

shows that this class is non-terminal. In the class $C_{2,2}$,

$$\nu_2((4i + 2)^2 + 16) = \nu_2(16i^2 + 16i + 20) = 2 + \nu_2(4i^2 + 4i + 5) = 2.$$

Therefore $C_{2,2}$ is a terminal class with valuation 2.

The third level contains the two classes $C_{3,0}$ and $C_{3,4}$ descending from $C_{2,0}$. The first class is terminal with valuation 4, since

$$\nu_2((8i)^2 + 16) = 4 + \nu_2(4i^2 + 1) = 4.$$

The second class is also terminal, with valuation 5, since

$$\nu_2((8i + 4)^2 + 16) = \nu_2(64i^2 + 64i + 32) = 5 + \nu_2(2i^2 + 2i + 1) = 5.$$

Therefore, every class in the third level is terminal and the tree is complete.

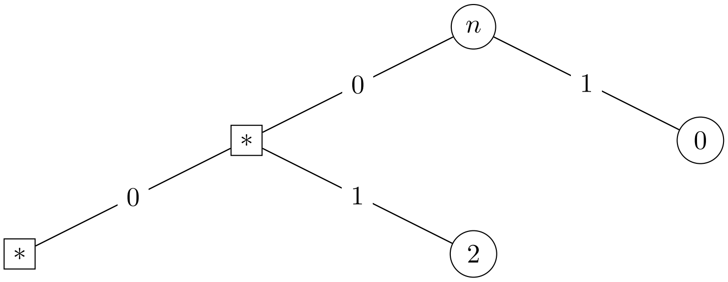

Figure 6. Two levels of the tree for $\nu_2(n^2+16)$

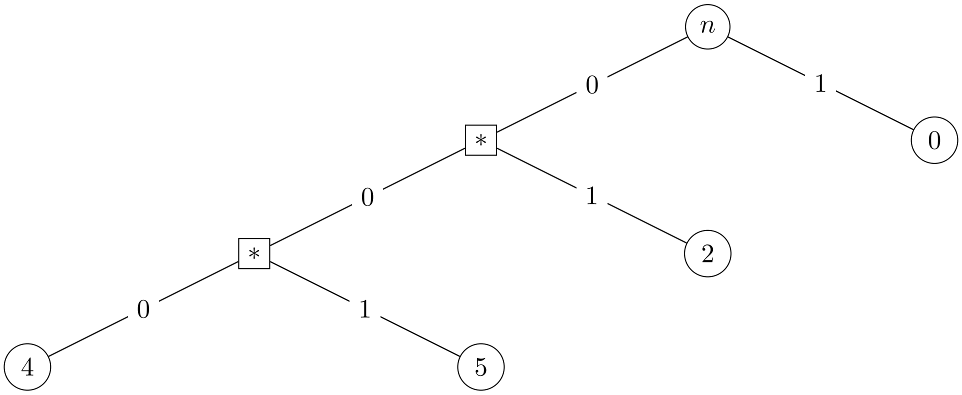

Figure 7. The complete tree for $\nu_2(n^2+16)$

Example 4.3. The valuations $\nu_2(n^2+7)$ present a more erratic behavior than the cases considered before. Perhaps it is not reasonable to expect that a simple formula, such as the one found for $\nu_2(n^2+1)$, will exist. Figure 8 gives the graph of $\nu_2(n^2+7)$ for $0 \neq n \leqslant 150$.

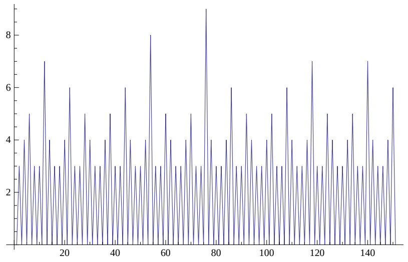

Figure 8. The valuation $\nu_2(n^2+7)$ for $0 \leqslant n \leqslant 150$

n	3	4	5	6	7	8	9	10	11	12	13	14	15	16
λ_n	1	3	5	21	11	53	75	331	843	1867	3915	8011	181	16565

FIGURE 9. The minimum index i for which $\nu_2(i^2+7)=n$

The range of $\nu_2(n^2+7)$ presents some interesting questions. It is clear that, for n even, $\nu_2(n^2+7)=0$. On the other hand, for n odd, this valuation is at least 3 since

$$\nu_2((2n+1)^2+7)=\nu_2(4n^2+4n+8)=3+\nu_2\left(\tfrac{1}{2}n(n+1)+1\right). \tag{4.2}$$

Thus, there are no values n such that $\nu_2(n^2+7)=1,$ or 2. It seems that these are the only two values omitted by this valuation. The table shows the values of λ_n defined as the minimum index i for which $\nu_2(i^2+7)=n$, in the range $3\leqslant n\leqslant 16$.

Construction of the tree. In the case of $\nu_2(n^2+7)$, the construction of the tree begins as before. The values $\nu_2(1^2+7)=3\neq\nu_2(2^2+7)=0$ show that the root vertex is non-terminal. Therefore it is split into two classes to form the first level:

$$C_{1,0}=\{2n:\, n\in\mathbb{N}\} \text{ and } C_{1,1}=\{2n+1:\, n\in\mathbb{N}\}. \tag{4.3}$$

It is easy to check that the class $C_{1,0}$ is terminal since $\nu_2((2n)^2+7)=0$. Figure 10 shows the root vertex and the first level of the tree for $\nu_2(n^2+7)$.

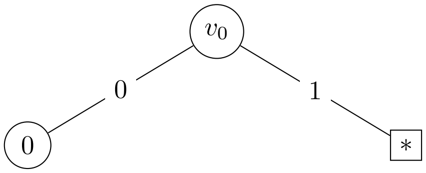

FIGURE 10. The root and the first level of the tree for $\nu_2(n^2+7)$

In the case of the class $C_{1,1}$, the congruence $(2n+1)^2+7\equiv 0 \bmod 2$ shows that every number $n\in C_{1,1}$ satisfies $\nu_2(n^2+7)\geqslant 1$. It turns out that, if $n\in C_{1,1}$, then $n=2n_1+1$ and

$$(2n_1+1)^2+7=4(n_1^2+n_1+2)\equiv 0 \bmod 8 \tag{4.4}$$

so actually $\nu_2(n^2+7)\geqslant 3$. The class $C_{1,1}$ is not-terminal, since $1,3\in C_{1,1}$ and $\nu_2(1^2+7)=3\neq\nu_2(3^2+7)=4$.

The vertex corresponding to $C_{1,1}$ is split to form part of the third level. This gives the classes $C_{2,1}$ and $C_{2,3}$; that is the sequences $4n+1$ and $4n+3$. It is easy to see that neither of these vertices is terminal. For instance, $C_{2,1}$ is not terminal, since every number in it has valuation at least 3 and the congruence

$$(4n+1)^2+7=16n^2+8n+8\equiv 0 \bmod 2^4 \tag{4.5}$$

shows that the valuation is 3 and at least 4 for n odd. A similar argument shows that $C_{2,3}$ is not terminal. Theorem 4.4 below shows the existence of two infinite branches for the tree associate to $f(x)=x^2+7$. The connection to these infinite branches and the roots of $f(x)=0$ in the 2-adic field $\mathbb{Q}_2$ is given in the next section.

Theorem 4.4. Let v be a non-terminating node at the k-th level for the valuation tree of $\nu_2(n^2+7)$. Then v splits into two vertices at the $(k+1)$-level. Exactly one of them terminates, with valuation k. The second one has valuation at least $k+1$.

PROOF. The numbers associated to the vertex v have the form

$$N_k = 2^k n + 2^{k-1} a_{k-1} + b_{k-2} \tag{4.6}$$

where

$$b_{k-2} = 2^{k-2} a_{k-2} + \cdots + 2a_1 + a_0 \tag{4.7}$$

has been determined. The induction hypothesis imply that $N_k^2+7 \equiv 0 \bmod 2^k$, so that $\nu_2(N_k^2+7) \geqslant k$. The question is whether the vertex v is terminal or not is reduced to the analysis of possible splits of v to the next level. This corresponds to the choices $a_{k-1} = 0$ or 1.

Consider now the congruence

$$N_k^2 + 7 \equiv 0 \bmod 2^{k+1} \tag{4.8}$$

that is,

$$\left[2^k n + 2^{k-1} a_{k-1} + b_{k-2} \right]^2 + 7 \equiv 0 \bmod 2^{k+1} \tag{4.9}$$

for the unknown a_{k-1}. Then (4.9) reduces to

$$2^k a_{k-1} b_{k-2} + b_{k-2}^2 + 7 \equiv 0 \bmod 2^{k+1}. \tag{4.10}$$

Observe that $b_{k-2} \equiv a_0 \bmod 2$, so (4.10) becomes

$$2^k a_{k-1} a_0 \equiv -(b_{k-2}^2 + 7) \bmod 2^{k+1}. \tag{4.11}$$

By induction $b_{k-2}^2 + 7 = 2^k m$ yielding

$$a_{k-1} \equiv -m \bmod 2 \tag{4.12}$$

as the solution to (4.9). Therefore the vertex descending from v with $a_{k-1} \not\equiv -m \bmod 2$ terminates with valuation k. The other vertex has valuation at least $k+1$. This proves that v is non-terminating (since one of its descendants has valuation k and the other has at least $k+1$). This continues the inductive process and completes the proof. □

The case $a \equiv 7 \bmod 8$ is completely similar to $a = 7$.

Theorem 4.5. Assume $a \equiv 7 \bmod 8$. Then the valuation $\nu_2(n^2+a)$ is determined by a tree with two infinite branches.

Note 4.6. The proof presented before is simply an adaptation of the Hensel's lemma, the version of Newton's method for solving polynomial equations in $\mathbb{Q}_2$. The reader will find more information in Section 3.4 of [**4**].

5. The solutions to $ax^2 + c = 0$ in the 2-adic field $\mathbb{Q}_2$

The existence of two infinite branches in the tree for $f(x) = x^2 + 7$ is connected to solutions to the equation $f(x) = 0$ in the 2-adic field $\mathbb{Q}_2$. This section explores the slightly more general question of $\nu_2(an^2 + c)$, where $a,\, c \in \mathbb{Z}$. It is assumed that $\gcd(a, c) = 1$, since any common divisor just produces a shift in the valuation. The case a even and c odd is simple: $\nu_2(an^2 + c) = 0$. Therefore, it is assumed that a is odd and c is even. It turns out to be convenient to write

$$c = 4^i b, \quad \text{with} \quad b \not\equiv 0 \bmod 4. \tag{5.1}$$

Then the solutions to

$$f_{a,c}(x) = ax^2 + c = 0 \tag{5.2}$$

are given by

$$x = \pm 2^i \sqrt{-\frac{b}{a}}. \tag{5.3}$$

The problem has been reduced to the study of square roots in the field $\mathbb{Q}_2$.

The classical binomial theorem

$$(1-x)^{-s} = \sum_{k=0}^{\infty} \frac{(s)_k}{k!} x^k \tag{5.4}$$

gives the identity

$$\begin{aligned} \sqrt{-\frac{b}{a}} &= \sum_{k=0}^{\infty} \frac{\left(-\frac{1}{2}\right)_k}{k!} \left(1 + \frac{b}{a}\right)^k \\ &= 1 - \sum_{k=1}^{\infty} \frac{1 \cdot 3 \cdots (2k-3)}{2^k k! a^k} (a+b)^k. \end{aligned} \tag{5.5}$$

It remains to verify that this last series converges in $\mathbb{Q}_2$.

This is the point in the argument where a remarkable property of p-adic numbers simplifies things. Recall that the norm in $\mathbb{Q}_2$ defined in (2.14) satisfies a stronger version of the triangle inequality:

$$||x + y||_2 \leqslant \text{Max}\{||x||_2, ||y||_2\}. \tag{5.6}$$

The extension to more summands

$$||\sum_{k=1}^{n} x_k||_2 \leqslant \text{Max}\{||x||_j \,:\, 1 \leqslant j \leqslant n\} \tag{5.7}$$

has the remarkable consequence stated below. This appears as Corollary 4.1.2 in [**4**].

Theorem 5.1. Let $a_k \in \mathbb{Q}_2$. Then the series $\sum_{k=1}^{\infty} a_k$ converges in $\mathbb{Q}_2$ if and only if the general term a_k converges to 0 in $\mathbb{Q}_2$.

The relation $\|x\|_2 = 2^{-\nu_2(x)}$ shows that the series in (5.5) converges if and only if

$$\lim_{k\to\infty} \nu_2 \left(\frac{1\cdot 3 \cdots (2k-3)}{2^k k! a^k} (a+b)^k \right) = +\infty. \tag{5.8}$$

Legendre's relation (1.1) and the fact that a is odd, converts (5.8) into

$$\lim_{k\to\infty} \left(\nu_2(a+b) - 2\right) k + s_2(k) = +\infty. \tag{5.9}$$

The next result now follows from the estimate $s_2(k) = O(\log k)$ as $k \to \infty$.

Theorem 5.2. Let a, c be integers with a odd and c even. Write $c = 4^i b$ with $b \not\equiv 0 \bmod 4$. Then the equation $f_{a,c}(x) = ax^2 + c = 0$ has a solution in the 2-adic field $\mathbb{Q}_2$ if and only if $\nu_2(a+b) \geqslant 3$.

This result is expressed in terms of trees.

Corollary 5.3. Let b be as in the previous theorem. Then the tree associated to the polynomial $f_{a,c}(x) = ax^2 + c$ has infinite branches if and only if $a + b \equiv 0 \bmod 8$.

In particular, the number b must be odd. Therefore, infinite branches appear precisely when $c = 4^i b$, with b an odd number with $a+b \equiv 0 \bmod 8$. In the case $a = 1$, this gives $b \equiv 7 \bmod 8$.

6. A random walk coming from the valuation of $n^2 + 7$

The sequence N_k constructed in the previous section has the form

$$N_k = 2^k n + 2^{k-1} a_{k-1} + \cdots + 2a_1 + a_0, \tag{6.1}$$

with $a_j = 0$ or 1. The two sequences start with $\{1, 0\}$ and $\{1, 1\}$, respectively. The numbers a_j are chosen in order to satisfy the congruence

$$N_k^2 + 7 \equiv 0 \bmod 2^{k+1}. \tag{6.2}$$

It is clear that N_k satisfy the consistency condition

$$N_k \equiv N_{k-1} \bmod 2^{k-1}. \tag{6.3}$$

This is precisely the definition of a 2-*adic integer*; see F. Gouvea [**4**] for more details. It turns out that $\{N_k\}$ are precisely the two roots, denoted by x_1 and x_2, of the equation $x^2 + 7 = 0$ in the 2-adic numbers $\mathbb{Q}_2$.

For p prime, the p-adic numbers $\mathbb{Q}_p$ are defined as the completion of $\mathbb{Q}$ with respect to the metric

$$|x|_p = p^{-\nu_p(|x|)}, \text{ for } x \in \mathbb{Q} \tag{6.4}$$

where $\nu_p(x)$ is the p-adic valuation described in the introduction. Recall that a complete space is one where the notions of Cauchy and convergent are one and the same. Thus, $\mathbb{Q}_p$ should be thought of a variation of the usual real numbers $\mathbb{R}$. A theorem of Ostrowski [**4**] shows that, aside from $\mathbb{R}$, these are the only natural ways to complete $\mathbb{Q}$.

The discussion presented in the previous sections show that the tree associated with $\nu_2(n^2+7)$ has the feature that, starting at level 2, it contains two infinite branches. The branch is labeled by a sequence $\{a_k : k \in \mathbb{N}\}$, where $a_k = 0$ indicates that the left branch of the tree at level k continues to level $k+1$ and $a_k = 1$ that the right one does. One of these branches with $\{1, 0\}$, that corresponds to the vertex v_2 and the continues with

$$\mathbb{L} = \{1,0,1,0,1,1,0,1,0,0,0,0,0,0,1,1,0,0,0,1,1,0,0,1,0,0,1,1,1,0\}.$$

The sequence $\mathbb{L}$ naturally corresponds to the first digits of the root x_1 of $x^2+7=0$.

The questions stated below are of statistical nature and they will be discussed in future work.

• Assume you are sitting at vertex at the k-th level of the branch. Is there an equal chance to move left or right at the next level?
• Are the choices of left/right at one level independent of the previous one?
• Is there a natural way to scale the sum $a_1 + a_2 + \cdots + a_n$, in order to obtain a meaningful result for the behavior of the sequence as $n \to \infty$?
• Is it possible to consider $\{a_j\}$ as a sequence of random variables taking values $\{0, 1\}$ and to determine their properties?
• Introduce the notation

$$x_k = a_k - \tfrac{1}{2} \tag{6.5}$$

and consider x_k to be a random variable taking values $\pm\frac{1}{2}$. If the values taken by $\{x_k\}$ were equally likely and the random variables were independent, then $\mathbb{E}x_k = 0$ and the central limit theorem would imply

$$\frac{1}{\sqrt{n}}\sum_{k=1}^{n} x_k \to N(0,1) \tag{6.6}$$

where $N(0,1)$ is a normal distribution. Does this happen in this situation?

The next figures show the sum $x_1 + \cdots + x_n$ for $n \leqslant 1500$ and $n \leqslant 50000$, respectively.

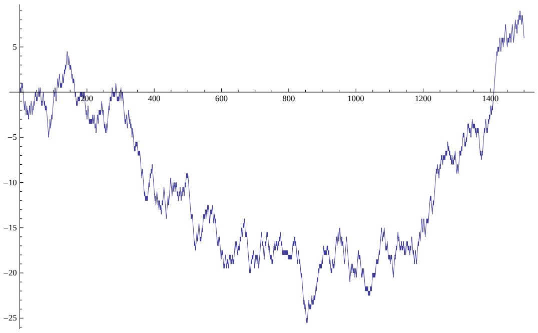

Figure 11. The walk coming from $a = 7$

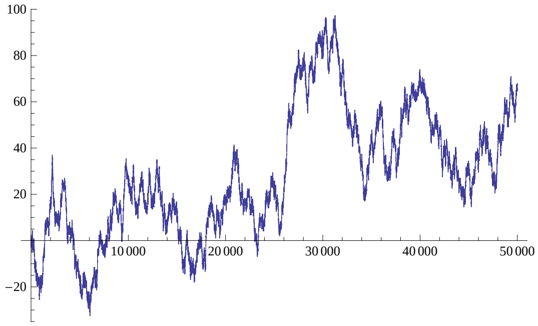

Figure 12. The walk coming from $a = 7$

Acknowledgments. The work of the last author is partially supported by NSF-DMS 1112656. The work of A. Byrnes, J. Fink, G. Lavigne and S. Rajasekaran, undergraduate students at Tulane University was partially funded by an REU Program at Tulane University funded by the same grant and also by the Newcomb-Tulane College funds. The work of X. Guan and A. Kesarwani, graduate students at Tulane University, was partially funded by the NSF-DMS 1112656 mentioned above. The last part of this work was carried out during the 2014 Mathematical Sciences Research Institute Undergraduate Program (MSRI-UP) which is funded by the National Science Foundation (grant No. DMS-1156499) and the National Security Agency (grant No. $H{-}98230 - 13 - 1 - 0262$). A. Byrnes, I. Nogues and A. Yuan were undergraduates at this program, L. Almodovar is a graduate student working as an assistant and E. Rowland was a postdoctoral advisor at the MSRI-UP program.

References

[1] F. Aragon, D. Bailey, J. Borwein, and P. Borwein. Walking on real numbers. *Mathematical Intelligencer*, 35:42–60, 2013.

[2] J. M. Borwein and R. Crandall. Closed forms: what they are and why we care. *Notices Amer. Math. Soc.*, 60:50–65, 2013.

[3] T. Chow. What is a closed-form number? *Amer. Math. Monthly*, 106:440–448, 1999.

[4] F. Gouvea. *p-adic numbers.* Springer-Verlag, 2nd edition, 1997.

[5] G. H. Hardy, D. R. Wright, E. M.; revised by Heath-Brown, and J. Silverman. *An Introduction to the Theory of Numbers.* Oxford University Press, 6th edition, 2008.

[6] N. Koblitz. *p-adic Numbers, p-adic Analysis, and Zeta functions*, volume 58 of *Graduate Texts in Mathematics.* Springer Verlag, New York, 1984.

[7] A. M. Legendre. *Théorie des Nombres.* Firmin Didot Frères, Paris, 1830.

Received 04 05 2019 revised 08 06 2019

[a] Department of Mathematics, University of Iowa ,
Iowa City, IA 52242, U.S.A.
E-mail address: leida-almodovar@uiowa.edu

[b] Department of Mathematics, Tulane University, New Orleans, U.S.A.
E-mail address: abyrnes1@tulane.edu
E-mail address: xguan1@tulane.edu
E-mail address: akesarwa@tulane.edu
E-mail address: glavigne@tulane.edu
E-mail address: vhm@tulane.edu

[c] 330 Hudson St, 7th Floor, New York, NY 10013, U.S.A.
E-mail address: jfink@money-media.com

[d] Departamento de Matematicas, Universidad de Puerto Rico, Ri0 Piedras, San Juan, PR 00936-8377
E-mail address: luis.medina17@upr.edu

[e] Department of Mathematics, Princeton University, Princeton, NJ 08544, U.S.A.
E-mail address: inogues@princeton.edu

[f] Laboratoire de Combinatoire et d'informatique Mathématique (LaCIM), Universite du Quebec á Montreal, CP 8888, Succ. Centre-ville, Montréal (Quebec) $H3C\,3P8$, CANADA.
E-mail address: rowland@lacim.ca

[g] Department of Mathematics, University of Chicago, Chicago, IL 60637, U.S.A.
E-mail address: amberyuan@uchicago.edu