2-ADIC BEHAVIOR OF NUMBERS OF DOMINO TILINGS

HENRY COHN
DEPARTMENT OF MATHEMATICS, HARVARD UNIVERSITY
CAMBRIDGE, MA 02138, USA
cohn@math.harvard.edu

Dedicated to my grandparents Garnette Cohn (1907–1998) and Lee Cohn (1908–1998)

Abstract. We study the 2-adic behavior of the number of domino tilings of a $2n \times 2n$ square as $n$ varies. It was previously known that this number was of the form $2^n f(n)^2$, where $f(n)$ is an odd, positive integer. We show that the function $f$ is uniformly continuous under the 2-adic metric, and thus extends to a function on all of $\mathbb{Z}$. The extension satisfies the functional equation $f(-1 - n) = \pm f(n)$, where the sign is positive iff $n \equiv 0, 3 \pmod{4}$.

Kasteleyn [K], and Temperley and Fisher [TF], proved that the number of tilings of a $2n \times 2n$ square with $1 \times 2$ dominos is

$$\prod_{i=1}^{n} \prod_{j=1}^{n} \left( 4 \cos^2 \frac{\pi i}{2n+1} + 4 \cos^2 \frac{\pi j}{2n+1} \right).$$

Although it is by no means obvious at first glance, this number is always a perfect square or twice a perfect square (see [P]). Furthermore, it is divisible by $2^n$ but no higher power of 2. This fact about 2-divisibility was independently proved by several people (see [JSZ], or see [P] for a combinatorial proof), but there seems to have been little further investigation of the 2-adic properties of these numbers, except for [JS].

Write the number of tilings as $2^n f(n)^2$, where $f(n)$ is an odd, positive integer. In this paper, we study the 2-adic properties of the function $f$. In particular, we will prove the following theorem, which was conjectured by James Propp:

Theorem 1. The function $f$ is uniformly continuous under the 2-adic metric, and its unique extension to a function from $\mathbb{Z}_2$ to $\mathbb{Z}_2$ satisfies the functional equation

$$f(-1 - n) = \begin{cases} f(n) & \text{if } n \equiv 0, 3 \pmod{4}, \\ -f(n) & \text{if } n \equiv 1, 2 \pmod{4}. \end{cases}$$

John and Sachs [JS] have independently investigated the 2-adic behavior of $f$, and explicitly determined it modulo $2^6$. Their methods, as well as ours, can be used to write formulas for $f$ modulo any power of 2, but no closed form is known.

The proof of Theorem 1 will not make any use of sophisticated 2-adic machinery. The only non-trivial fact we will require is that the 2-adic absolute value extends uniquely to each finite extension of $\mathbb{Q}$. For this fact, as well as basic definitions and concepts, the book [G] by Gouvêa is an excellent reference.

Theorem 1 is in essence a statement about the divisibility properties of $f(n)$ modulo $2^k$, for all integers $k$. It is helpful to keep this in mind when thinking about the proof of Theorem 1. It is also helpful to keep in mind the more elementary description of what it means for $f$ to be uniformly continuous 2-adically: for every $k$, there exists an $\ell$ such that if $n \equiv m \pmod{2^\ell}$, then $f(n) \equiv f(m) \pmod{2^k}$. In particular, we will see that for our function $f$, the condition $n \equiv m \pmod{2}$ implies that $f(n) \equiv f(m) \pmod{2}$, and $n \equiv m \pmod{4}$ implies that $f(n) \equiv f(m) \pmod{4}$.

Date: Submitted December 17, 1998; accepted February 18, 1999.

1991 Mathematics Subject Classification. 05A15, 11A07.
The author was supported by an NSF Graduate Research Fellowship.
As a warm-up in using 2-adic methods, and for the sake of completeness, we will prove that that number of tilings of a $2n \times 2n$ square really is of the form $2^n f(n)^2$, assuming Kasteleyn’s theorem. To do so, we will make use of the fact that the 2-adic metric extends to every finite extension of $\mathbb{Q}$, in particular the cyclotomic extensions, which contain the cosines that appear in Kasteleyn’s product formula. We can straightforwardly determine the 2-adic valuation of each factor, and thus of the entire product.

Let $\zeta$ be a primitive $(2n + 1)$-st root of unity, and define

$$\alpha_{i,j} = \zeta^i + \zeta^{-i} + \zeta^j + \zeta^{-j}.$$ 

Then the number of domino tilings of a $2n \times 2n$ square is

$$(1) \quad \prod_{i=1}^{n} \prod_{j=1}^{n} (4 + \alpha_{i,j}).$$

To determine the divisibility by 2, we look at this number as an element of $\mathbb{Q}_2(\zeta)$. Because $2n + 1$ is odd, the extension $\mathbb{Q}_2(\zeta)/\mathbb{Q}_2$ is unramified, so 2 remains prime in $\mathbb{Q}_2(\zeta)$. We will use $| \cdot |_2$ to denote the unique extension of the 2-adic absolute value to $\mathbb{Q}_2(\zeta)$.

**Lemma 2.** For $1 \leq i, j \leq n$, we have

$$|4 + \alpha_{i,j}|_2 = \begin{cases} 1 & \text{if } i \neq j, \\
1/2 & \text{if } i = j. \end{cases}$$

**Proof.** The number $4 + \alpha_{i,j}$ is an algebraic integer, so its 2-adic absolute value is at most 1. To determine how much smaller it is, first notice that

$$\alpha_{i,j} = (\zeta^i + \zeta^j)(\zeta^{i+j} + 1)\zeta^{-i}\zeta^{-j}.$$ 

In order for $4 + \alpha_{i,j}$ to reduce to 0 modulo 2, we must have

$$\zeta^i \equiv \zeta^{i+j} \pmod{2}.$$ 

However, this is impossible unless $i \equiv \pm j \pmod{2n+1}$, because $\zeta$ has order $2n+1$ in the residue field. Since $1 \leq i, j \leq n$, the only possibility is $i = j$.

In that case, $4 + \alpha_{i,i} = 2(2 + \zeta^i + \zeta^{-i})$. In order to have $|4 + \alpha_{i,i}|_2 < 1/2$, the second factor would need to reduce to 0. However, that could happen only if $\zeta^i \equiv \zeta^{-i} \pmod{2}$, which is impossible. \qed

By Lemma 2, the product (1) is divisible by $2^n$ but not $2^{n+1}$. The product of the terms with $i = j$, divided by $2^n$, is

$$(2) \quad \prod_{i=1}^{n} (2 + \zeta^i + \zeta^{-i}),$$

which equals 1, as we can prove by writing

$$\prod_{i=1}^{n} (2 + \zeta^i + \zeta^{-i}) = \prod_{i=1}^{n} (1 + \zeta^i) = \prod_{i=1}^{n} (1 + \zeta^i)(1 + \zeta^{2n+1-i}) = \prod_{i=1}^{2n} (1 + \zeta^i) = 1;$$

the last equality follows from substituting $z = -1$ in

$$z^{2n+1} - 1 = \prod_{i=0}^{2n} (z - \zeta^i).$$ 

Thus, the odd factor of the number of tilings of a $2n \times 2n$ square is

$$f(n)^2 = \prod_{1 \leq i < j \leq n} (4 + \alpha_{i,j})^2.$$
We are interested in the square root of this quantity, not the whole odd factor. The positive square root is
\[ f(n) = \prod_{1 \leq i < j \leq n} (4 + \alpha_{i,j}) \]
(notice that every factor is positive). It is clearly an integer, since it is an algebraic integer and is invariant
under every automorphism of \( \mathbb{Q}(\zeta)/\mathbb{Q} \). Thus, we have shown that the number of tilings is of the form
\[ 2^n f(n)^2, \]
where \( f(n) \) an odd integer.

In determining the 2-adic behavior of \( f \), it seems simplest to start by examining it modulo 4. In that
case, we have the formula
\[ f(n) \equiv \prod_{1 \leq i < j \leq n} \alpha_{i,j} \pmod{4}, \]
and the product appearing in it can actually be evaluated explicitly.

**Lemma 3.** We have
\[ \prod_{1 \leq i < j \leq n} \alpha_{i,j} = \begin{cases} 1 & \text{if } n \equiv 0, 1, 3 \pmod{4}, \\ -1 & \text{if } n \equiv 2 \pmod{4}. \end{cases} \]

*Proof.* In this proof, we will write \( \zeta^* \) to indicate an unspecified power of \( \zeta \). Because the product in question
is real and the only real power of \( \zeta \) is 1, we will in several cases be able to see that factors of \( \zeta^* \) equal 1
without having to count the \( \zeta \)'s.

Start by observing that
\[
\prod_{1 \leq i < j \leq n} \alpha_{i,j} = \prod_{i=1}^{n-1} \prod_{j=i+1}^{n} (\zeta^{i+j} + 1)(\zeta^{i-j} + 1)\zeta^{-i} = \zeta^* \prod_{i=1}^{n-1} \prod_{j=i+1}^{n} (\zeta^{i+j} + 1)(\zeta^{2n+1+i-j} + 1) = \zeta^* \prod_{i=1}^{n-1} \prod_{s=2i+1}^{2n} (\zeta^s + 1). 
\]

(To prove the last line, check that \( i + j \) and \( 2n + 1 + i - j \) together run over the same range as \( s \).)

In the factors where \( i > n/2 \), replace \( \zeta^s + 1 \) with \( \zeta^s(\zeta^{2n+1-s} + 1) \). Now for every \( i \), it is easy to check that
\[
\prod_{s=2i+1}^{2n} (\zeta^s + 1) = \prod_{s=2(n-i)+1}^{2n} (\zeta^{2n+1-s} + 1) = \prod_{s=1}^{2n} (\zeta^s + 1) = 1. 
\]

When \( n \) is odd, pairing \( i \) with \( n - i \) in this way takes care of every factor except for a power of \( \zeta \), which
must be real and hence 1. Thus, the whole product is 1 when \( n \) is odd, as desired.

In the case when \( n \) is even, the pairing between \( i \) and \( n - i \) leaves the \( i = n/2 \) factor unpaired. The
product is thus
\[ \zeta^* \prod_{s=n+1}^{2n} (\zeta^s + 1). \]
Notice that
\[
\left( \prod_{s=n+1}^{2n} (1 + \zeta^s) \right)^2 = \prod_{s=n+1}^{2n} \zeta^s(1 + \zeta^{2n+1-s}) \prod_{s=n+1}^{2n} (1 + \zeta^s) \\
= \prod_{s=n+1}^{2n} \zeta^s \\
= \zeta^*.
\]

Hence, since every power of \( \zeta \) has a square root among the powers of \( \zeta \) (because \( 2n + 1 \) is odd),
\[
\prod_{s=n+1}^{2n} (\zeta^s + 1) = \pm \zeta^*.
\]

Substituting this result into (3) shows that the product we are trying to evaluate must equal \( \pm 1 \), since the \( \zeta^* \) factor must be real and therefore 1. All that remains is to determine the sign.

Since
\[
\prod_{s=n+1}^{2n} (1 + \zeta^s)
\]
and
\[
\prod_{t=1}^{n} (1 + \zeta^t)
\]
are reciprocals, it is enough to answer the question for the second one (which is notationally slightly simpler).

We know that it is plus or minus a power of \( \zeta \), and need to determine which. Since \( \zeta = \zeta^{-2n} \), we have
\[
\prod_{t=1}^{n} (1 + \zeta^t) = \prod_{t=1}^{n} (1 + \zeta^{-2nt}) = \zeta^* \prod_{t=1}^{n} (\zeta^{nt} + \zeta^{-nt}).
\]

The product
\[
\prod_{t=1}^{n} (\zeta^{nt} + \zeta^{-nt})
\]
is real, so it must be \( \pm 1 \); to determine which, we just need to determine its sign. For that, we write
\[
\zeta^{nt} + \zeta^{-nt} = 2 \cos \left( t\pi - \frac{t\pi}{2n + 1} \right),
\]
which is negative iff \( t \) is odd (assuming \( 1 \leq t \leq n \)). Thus, the sign of the product is negative iff there are an odd number of odd numbers from 1 to \( n \), i.e., \( n \equiv 2 \pmod{4} \) (since \( n \) is even).

Therefore, the whole product is \(-1\) iff \( n \equiv 2 \pmod{4} \), and is 1 otherwise.

Now that we have dealt with the behavior of \( f \) modulo 4, we can simplify the problem considerably by working with \( f^2 \) rather than \( f \). Recall that proving uniform continuity is equivalent to showing that for every \( k \), there exists an \( \ell \) such that if \( n \equiv m \pmod{2^\ell} \), then \( f(n) \equiv f(m) \pmod{2^k} \). If we can find an \( \ell \) such that \( n \equiv m \pmod{2^\ell} \) implies that \( f(n)^2 \equiv f(m)^2 \pmod{2^{2k}} \), then it follows that \( f(n) \equiv \pm f(m) \pmod{2^k} \), and our knowledge of \( f \) modulo 4 pins down the sign as +1. The same reasoning applies to the functional equation, so if we can show that \( f^2 \) is uniformly continuous 2-adically and satisfies \( f(-1 - n)^2 = f(n)^2 \), then we will have proved Theorem 1. \( \square \)
We begin by using (1) to write
\[ 2^n f(n)^2 = \left( \prod_{i,j=1}^{n} \alpha_{i,j} \right) \prod_{i,j=1}^{n} \left( 1 + \frac{4}{\alpha_{i,j}} \right) = \left( \prod_{i,j=1}^{n} \alpha_{i,j} \right) \sum_{k\geq0} 4^k E_k(n), \]
where \( E_k(n) \) is the \( k \)-th elementary symmetric polynomial in the \( 1/\alpha_{i,j} \)'s (where \( 1 \leq i, j \leq n \)). We can evaluate the product
\[ \prod_{i,j=1}^{n} \alpha_{i,j} \]
by combining Lemma 3 with the equation
\[ \prod_{t=1}^{n} (\zeta^t + \zeta^{-t}) = (-1)^{\lfloor \frac{n+1}{2} \rfloor}, \]
which can be proved using the techniques of Lemma 3: it is easily checked that the product squares to 1, and its sign is established by writing
\[ \zeta^t + \zeta^{-t} = 2 \cos \frac{2t\pi}{2n+1}, \]
which is positive for \( 1 \leq t < (2n+1)/4 \) and negative for \( (2n+1)/4 < t \leq n \). This shows that
\[ \prod_{i,j=1}^{n} \alpha_{i,j} = (-1)^{\lfloor \frac{n+1}{2} \rfloor} 2^n, \]
so we conclude that
\[ f(n)^2 = (-1)^{\lfloor \frac{n+1}{2} \rfloor} \sum_{k\geq0} 4^k E_k(n). \] (4)

The function \( n \mapsto (-1)^{\lfloor \frac{n+1}{2} \rfloor} \) is uniformly continuous 2-adically and invariant under interchanging \( n \) with \( -1 - n \), so to prove these properties for \( f^2 \) we need only prove them for the sum on the right of (4).

Because \( \alpha_{i,j} \) has 2-adic valuation at most 1, that of \( E_k(n) \) is at least \( -k \), and hence \( 2^k E_k(n) \) is a 2-adic integer (in the field \( \mathbb{Q}_2(\zeta) \)). Thus, to determine \( f(n)^2 \mod 2^k \) we need only look at the first \( k+1 \) terms of the sum (4).

Define
\[ S_k(n) = \sum_{i,j=1}^{n} \frac{1}{\alpha_{i,j}^k}. \]
We will prove the following proposition about \( S_k \).

**Proposition 4.** For each \( k \), \( S_k(n) \) is a polynomial over \( \mathbb{Q} \) in \( n \) and \( (-1)^n \). Furthermore,
\[ S_k(n) = S_k(-1 - n). \]

We will call a polynomial in \( n \) and \( (-1)^n \) a quasi-polynomial. Notice that every quasi-polynomial over \( \mathbb{Q} \) is uniformly continuous 2-adically.

In fact, \( S_k \) is actually a polynomial of degree \( 2k \). However, we will not need to know that. The only use we will make of the fact that \( S_k \) is quasi-polynomial is in proving uniform continuity, so we will prove only this weaker claim.
Given Proposition 4, the same must hold for $E_k$, because the $E_k$'s and $S_k$'s are related by the Newton identities

$$kE_k = \sum_{i=1}^{k} (-1)^{i-1} S_i E_{k-i}.$$ 

It now follows from (4) that $f^2$ is indeed uniformly continuous and satisfies the functional equation. Thus, we have reduced Theorem 1 to Proposition 4.

Define

$$T_k(n) = \sum_{i,j=0}^{2n} \frac{1}{\alpha_{i,j}^k},$$

and

$$R_k(n) = \sum_{i=0}^{2n} \frac{1}{\alpha_{i,0}^k}.$$ 

Because $\alpha_{i,j} = \alpha_{-i,j} = \alpha_{i,-j} = \alpha_{-i,-j}$, we have

$$T_k(n) = 4S_k(n) + 2R_k(n) - \frac{1}{\alpha_{0,0}^k}.$$ 

To prove Proposition 4, it suffices to prove that $T_k$ and $R_k$ are quasi-polynomials over $\mathbb{Q}$, and that $T_k(-1-n) = T_k(n)$ and $R_k(-1-n) = R_k(n)$.

We can simplify further by reducing $T_k$ to a single sum, as follows. It is convenient to write everything in terms of roots of unity, so that

$$T_k(n) = \sum_{\zeta,\xi} \frac{1}{(\zeta + 1/\zeta + \xi + 1/\xi)^k},$$

where $\zeta$ and $\xi$ range over all $(2n+1)$-st roots of unity. (This notation supersedes our old use of $\zeta$.) Then we claim that

$$T_k(n) = \left( \sum_{\zeta} \frac{1}{(\zeta + 1/\zeta)^k} \right)^2.$$ 

To see this, write the right hand side as

$$\left( \sum_{\zeta} \frac{1}{(\zeta + 1/\zeta)^k} \right) \left( \sum_{\xi} \frac{1}{(\xi + 1/\xi)^k} \right) = \sum_{\zeta,\xi} \frac{1}{(\zeta^2 + 1/(\zeta^2) + 1/(\zeta^2))^k},$$

and notice that as $\zeta$ and $\xi$ run over all $(2n+1)$-st roots of unity, so do $\zeta^2$ and $\zeta^2/\xi$. (This is equivalent to the fact that every $(2n+1)$-st root of unity has a unique square root among such roots of unity, because that implies that the ratio $\xi^2$ between $\zeta^2$ and $\zeta^2/\xi$ does in fact run over all $(2n+1)$-st roots of unity.)

We can deal with $R_k$ similarly: as $\xi$ runs over all $(2n+1)$-st roots of unity, so does $\xi^2$, and hence

$$R_k(n) = \sum_{\zeta} \frac{1}{(2 + \zeta + 1/\zeta)^k} = \sum_{\xi} \frac{1}{(2 + \xi^2 + 1/\xi^2)^k} = \sum_{\xi} \frac{1}{(\xi + 1/\xi)^{2k}}.$$ 

Define

$$U_k(n) = \sum_{\zeta} \frac{1}{(\zeta + 1/\zeta)^k}.$$ 

Now everything comes down to proving the following proposition:

**Proposition 5.** The function $U_k$ is a quasi-polynomial over $\mathbb{Q}$, and satisfies

$$U_k(-1-n) = U_k(n).$$
Proof. The proof is based on the observation that for any non-zero numbers, the power sums of their reciprocals are minus the Taylor coefficients of the logarithmic derivative of the polynomial with those numbers as roots, i.e.,
\[
\frac{d}{dx} \log \prod_{i=1}^{m} (x - r_i) = \sum_{i=1}^{m} \frac{1}{x - r_i} = \sum_{i=1}^{m} \frac{-1/r_i}{1 - x/r_i} = -\sum_{i=1}^{m} \left( \frac{1}{r_i} + \frac{x}{r_i^2} + \frac{x^2}{r_i^3} + \ldots \right).
\]

To apply this fact to \(U_k\), define
\[
P_n(x) = \prod_{\zeta} (x - (\zeta + 1/\zeta)) = \prod_{j=0}^{2n} (x - 2 \cos(2\pi j/(2n + 1))) = 2(\cos((2n + 1) \cos^{-1}(x/2)) - 1).
\]

Then
\[
\frac{d}{dx} \log P_n(x) = \frac{2n + 1}{2\sqrt{1 - x^2/4}} \frac{\sin((2n + 1) \cos^{-1}(x/2))}{\cos((2n + 1) \cos^{-1}(x/2)) - 1}.
\]

This function is invariant under interchanging \(n\) with \(-1 - n\) (equivalently, interchanging \(2n + 1\) with \(-(2n + 1)\)), so its Taylor coefficients are as well. By the observation above, the coefficient of \(x^k\) is \(-U_{k+1}(n)\).

Straightforward calculus shows that these coefficients are polynomials over \(\mathbb{Q}\) in \(n\), \(\sin((2n + 1)\pi/2)\), and \(\cos((2n + 1)\pi/2)\). Using the fact that \(\cos((2n + 1)\pi/2) = 0\) and \(\sin((2n + 1)\pi/2) = (-1)^n\) completes the proof.

Acknowledgements

I am grateful to James Propp for telling me of his conjecture, to the anonymous referee for pointing out a sign error in the original manuscript, and to Karen Acquista, Noam Elkies, Matthew Emerton, and Vis Taraz for helpful conversations.

References

[G] F. Gouvea, \(p\)-adic Numbers: An Introduction, 2nd ed., Springer-Verlag, New York, 1997.
[JS] P. John and H. Sachs, On a strange observation in the theory of the dimer problem, preprint, 1998.
[JSZ] P. John, H. Sachs, and H. Zernitz, Problem 5. Domino covers in square chessboards, Zastosowania Matematyki (Applications Mathematicae) XIX 3–4 (1987), 635–641.
[K] P. W. Kasteleyn, The statistics of dimers on a lattice, I. The number of dimer arrangements on a quadratic lattice, Physica 27 (1961), 1209–1225.
[L] L. Lovász, Combinatorial Problems and Exercises, North-Holland Publishing Company, Amsterdam, 1979.
[P] L. Pachter, Combinatorial approaches and conjectures for 2-divisibility problems concerning domino tilings of polyominoes, Electronic Journal of Combinatorics 4 (1997), #R29.
[TF] H. N. V. Temperley and M. E. Fisher, Dimer problem in statistical mechanics—an exact result, Phil. Mag. 6 (1961), 1061–1063.