Journal of Integer Sequences, Vol. 26 (2023),
Article 23.7.7

Divisibility Properties of Dedekind Numbers

Bartłomiej Pawelski and Andrzej Szepietowski
Institute of Informatics
University of Gdańsk
Poland
bartlomiej.pawelski@ug.edu.pl
andrzej.szepietowski@ug.edu.pl

Abstract

We study some divisibility properties of Dedekind numbers. We show that the ninth Dedekind number is congruent to 6 modulo 210.

1 Introduction

We define D_n to be the set of all monotone Boolean functions of n variables. The cardinality of this set, d_n, is known as the n-th Dedekind number. Values of d_n are described by the OEIS *(On-Line Encyclopedia of Integer Sequences)* sequence A000372 (see Table 1).

n	d_n	r_n
0	2	2
1	3	3
2	6	5
3	20	10
4	168	30
5	7,581	210
6	7,828,354	16,353
7	2,414,682,040,998	490,013,148
8	56,130,437,228,687,557,907,788	1,392,195,548,889,993,358

Table 1: Known values of d_n (A000372) and r_n (A003182).

In 1990, Wiedemann calculated d_8 [11]. His result was confirmed in 2001 by Fidytek, Mostowski, Somla, and Szepietowski [4]. The impulse for writing our paper came from the letter from Wiedemann to Sloane [12] informing about the computation of the eighth Dedekind number, specifically this fragment: "Unfortunately, I don't see how to test it...". Wiedemann only knew that d_8 is even. Despite its obvious importance, there is a lack of studies on the divisibility of Dedekind numbers. As far as we know, the only paper concerning this question is Yamamoto's paper [13], where he shows that if n is even, then d_n is also even; he also states (without proof) that d_9 is even and d_{11} is odd.

Our research aims to fill this lack by proposing new methods to determine the divisibility of Dedekind numbers. As an application of these methods, we compute remainders of d_9 divided by one-digit prime numbers, which (we hope) will help to verify the value d_9 after its first computation.

Our main result is the following system of congruences:

$$\begin{aligned} d_9 &\equiv 0 \pmod 2, \\ d_9 &\equiv 0 \pmod 3, \\ d_9 &\equiv 1 \pmod 5, \\ d_9 &\equiv 6 \pmod 7. \end{aligned}$$

By the Chinese remainder theorem, we have

$$d_9 \equiv 6 \pmod{210}.$$

Recently, after the preprint of this paper was published on ArXiv, two independent research teams [5, 7] reported the same value:

$$d_9 = 286386577668298411128469151667598498812366,$$

which confirms our results.

2 Preliminaries

Let B denote the set $\{0, 1\}$ and B^n the set of n-element sequences of B. A Boolean function with n variables is any function from B^n into B. There are 2^n elements in B^n and 2^{2^n} Boolean functions with n variables. There is the order relation in B (namely: $0 \leq 0$, $0 \leq 1$, $1 \leq 1$) and the following partial order in B^n. For any two elements, $x = (x_1, \ldots, x_n)$, $y = (y_1, \ldots, y_n)$ in B^n,

$$x \leq y \quad \text{if and only if} \quad x_i \leq y_i \quad \text{for all } 1 \leq i \leq n.$$

A function $h : B^n \to B$ is monotone if

$$x \leq y \Longrightarrow h(x) \leq h(y).$$

Let D_n denote the set of monotone functions with n variables and let d_n denote $|D_n|$. We have the partial order in D_n defined by:

$$g \leq h \quad \text{if and only if} \quad g(x) \leq h(x) \quad \text{for all } x \in B^n.$$

We shall represent the elements of D_n as strings of bits of length 2^n. Two elements of D_0 will be represented as 0 and 1. Any element $g \in D_1$ can be represented as the concatenation $g(0) * g(1)$, where $g(0), g(1) \in D_0$ and $g(0) \leq g(1)$. Hence $D_1 = \{00, 01, 11\}$. Each element of $g \in D_2$ is the concatenation (string) of four bits: $g(00) * g(10) * g(01) * g(11)$ which can be represented as a concatenation $g_0 * g_1$, where $g_0, g_1 \in D_1$ and $g_0 \leq g_1$. Hence $D_2 = \{0000, 0001, 0011, 0101, 0111, 1111\}$. Similarly, any element of $g \in D_n$ can be represented as a concatenation $g_0 * g_1$, where $g_0, g_1 \in D_{n-1}$ and $g_0 \leq g_1$. Therefore, we can treat functions in D_n as sequences of bits and as integers. We let $\preceq$ denote the total order in D_n induced by the total order in integers.

For a set $Y \subseteq D_n$, by Y^2 we denote the Cartesian power $Y^2 = Y \times Y$, that is the set of all ordered pairs (x, y) with $x, y \in Y$. Similarly for more than two factors, we write Y^k for the set of ordered k-tuples of elements of Y. We let $\top$ denote the maximal element in D_n, that is, $\top = (1 \dots 1)$; and $\bot$ denote the minimal element in D_n, that is, $\bot = (0 \dots 0)$. For two elements $x, y \in D_n$, we let $x|y$ denote the bitwise or; and $x\&y$ denote the bitwise and. Furthermore, we let $\mathrm{re}(x, y)$ denote $|\{z \in D_n : x \leq z \leq y\}|$. Note that $\mathrm{re}(x, \top) = |\{z \in D_n : x \leq z\}|$ and $\mathrm{re}(\bot, y) = |\{z \in D_n : z \leq y\}|$.

2.1 Posets

A *poset (partially ordered set)* $(S, \leq)$ consists of a set S together with a binary relation (partial order) $\leq$ which is reflexive, transitive, and antisymmetric. Given two posets $(S, \leq)$ and $(T, \leq)$ a function $f : S \to T$ is *monotone*, if $x \leq y$ implies $f(x) \leq f(y)$. By T^S we denote the poset of all monotone functions from S to T with the partial order defined by

$$f \leq g \quad \text{if and only if} \quad f(x) \leq g(x) \text{ for all } x \in S.$$

In this paper we use the following well-known lemma; see [3, 10]:

Lemma 1. *The poset D_{n+k} is isomorphic to the poset $D_n^{B^k}$—the poset of monotone functions from B^k to D_n.*

3 Divisibility of Dedekind numbers by 2

In 1952, Yamamoto [13] proved that if n is even, then d_n is also even; he also stated (without proof) that d_9 is even and d_{11} is odd. In order to prove that d_9 is even, we will leverage the duality property of Boolean functions. For each $x \in D_n$, we have *dual* x^d which is obtained by reversing and negating all bits. For example, $1111^d = 0000$ and $0001^d = 0111$. An element $x \in D_n$ is *self-dual* if $x = x^d$. For example, 0101 and 0011 are self-duals in D_2. If x is not self-dual, and $y = x^d \neq x$, then $y^d = x$. Thus, non-self-duals form pairs of the form (x, x^d), where $x \neq x^d$. Let k_n denote the number of these pairs and let λ_n denote the number of self-dual functions in D_n. We have that $d_n = 2k_n + \lambda_n$. Hence $\lambda_n \equiv d_n \pmod 2$. Values of λ_n are described by the OEIS sequence A001206; see Table 2. The last known term of this sequence, λ_9, was calculated in 2013 by Brouwer et al. [2].

n	λ_n
0	0
1	1
2	2
3	4
4	12
5	81
6	2,646
7	1,422,564
8	229,809,982,112
9	423,295,099,074,735,261,880

Table 2: Known values of λ_n (A001206).

Corollary 2. *We have* $d_9 \equiv \lambda_9 \equiv 0 \pmod 2$.

One can directly check that $d_n \equiv \lambda_n \pmod 2$ for $n \leq 8$.

4 Divisibility of Dedekind numbers by 3

By Lemma 1, the poset D_{n+3} is isomorphic to the poset $D_n^{B^3}$—the set of monotone functions from $B^3 = \{000, 001, 010, 100, 110, 101, 011, 111\}$ to D_n. Now consider the group S_3—the permutations on $\{1, 2, 3\}$. The group S_3 is isomorphic to the automorphism group $\mathrm{Aut}(B^3)$ of the Boolean lattice B^3. The automorphism group $\mathrm{Aut}(B^3)$ acts in a natural way on $D_n^{B^3}$ by

$$\alpha(f) = f \circ \alpha^{-1}$$

for all $\alpha \in \mathrm{Aut}(B^3)$ and all $f \in D_n^{B^3}$. Let $\mathcal{O}(f) = \{\alpha(f) \in D_n^{B^3} : \alpha \in \mathrm{Aut}(B^3)\}$ denote the orbit of f under this action and by $\gamma(f) = |\mathcal{O}(f)|$ its cardinality. The orbits form a partition of $D_{n+3} = D_n^{B^3}$. Each of these orbits has one, three, or six elements. Moreover, an orbit $\mathcal{O}(f)$ has one element if and only if $f(001) = f(010) = f(100)$ and $f(011) = f(101) = f(110)$. Such a function f can be identified with a monotone function from the path P_4 to D_n. Hence,

$$d_{n+3} \equiv |D_n^{P_4}| \pmod 3.$$

It is well known, see [1, 10], that the number of monotone functions from the path $P_4 = (a < b < c < d)$ to a poset S is equal to the sum of the elements of the third power of $M(S)$—the incidence matrix of S. For example, for the poset $D_1 = \{00 < 01 < 11\}$, we have

$$M(D_1) = \begin{pmatrix} 1 & 1 & 1 \\ 0 & 1 & 1 \\ 0 & 0 & 1 \end{pmatrix}$$

and

$$M(D_1)^3 = \begin{pmatrix} 1 & 3 & 6 \\ 0 & 1 & 3 \\ 0 & 0 & 1 \end{pmatrix}.$$

The sum of the elements of $(M(D_1)^3)$ is equal to 15, which is equal to $|D_1^{P_4}|$—the number of monotone functions from P_4 to D_1.

Furthermore, consider $D_2 = \{0000, 0001, 0011, 0101, 0111, 1111\}$ and its incidence matrix:

$$M(D_2) = \left(\begin{array}{cc|cc|cc} 1 & 1 & 1 & 1 & 1 & 1 \\ 0 & 1 & 1 & 1 & 1 & 1 \\ \hline 0 & 0 & 1 & 0 & 1 & 1 \\ 0 & 0 & 0 & 1 & 1 & 1 \\ \hline 0 & 0 & 0 & 0 & 1 & 1 \\ 0 & 0 & 0 & 0 & 0 & 1 \end{array}\right).$$

Now consider the third power of the incidence matrix of D_2:

$$M(D_2)^3 = \left(\begin{array}{cc|cc|cc} 1 & 3 & 6 & 6 & 14 & 20 \\ 0 & 1 & 3 & 3 & 9 & 14 \\ \hline 0 & 0 & 1 & 0 & 3 & 6 \\ 0 & 0 & 0 & 1 & 3 & 6 \\ \hline 0 & 0 & 0 & 0 & 1 & 3 \\ 0 & 0 & 0 & 0 & 0 & 1 \end{array}\right).$$

The sum of the elements of $(M(D_2)^3)$ is equal to 105, which is equal to $|D_2^{P_4}|$—the number of monotone functions from P_4 to D_2. In a similar we can compute $|D_n^{P_4}|$ for $n = 3, 4, 5$. Unfortunately, this method cannot be easily applied for $n = 6$, because $M(D_6)$ is too large. However, Pawelski [8] proposed another method: $|D_{(n+m)}^{P_4}| = |D_n^{P_4 \times B^m}| = |(D_n^{P_4})^{B^m}|$ (also see [10]). Using the same program as used in [8] to compute $|D_5^{P_4}|$ we can calculate $|D_6^{P_4}|$ and the result (see Table 3) is divisible by 3.

Corollary 3. *As* $|D_6^{P_4}| = 868329572680304346696$ *is divisible by 3, the quantity* d_9 *is also divisible by 3.*

One can directly check that $d_{n+3} \equiv |D_n^{P_4}| \pmod 3$ for $n \leq 5$.

n	$\lvert D_n^{P_4}\rvert$	$\lvert D_n^{P_4}\rvert$ mod 3
0	5	2
1	15	0
2	105	0
3	3,490	1
4	2,068,224	0
5	262,808,891,710	1
6	868,329,572,680,304,346,696	0

Table 3: Known values of $|D_n^{P_4}|$. Note that $d_{n+3} \equiv |D_n^{P_4}| \pmod 3$.

5 Main lemma

In the sequel we shall use another definition of a group acting on $D_n^{B^k}$. In order to do this it is convenient to identify the lattice $D_n = B^{B^n}$ with the isomorphic up-set lattice $\mathcal{U}_n$ of B^n. An isomorphism is given by $h : D_n \to \mathcal{U}_n$, where $h(x) = x^{-1}(1)$ for all $x \in D_n$. For $\beta \in \mathrm{Aut}(B^n)$ and $x \in D_n$, we have

$$h(\beta(x)) = \beta(h(x)).$$

Let P and Q be two posets and let P^Q be the poset of monotone functions from Q to P. Now, we can define an action of $\mathrm{Aut}(P)$ on P^Q by setting

$$\beta(f) = \beta \circ f$$

for all $\beta \in \mathrm{Aut}(P)$ and $f \in P^Q$. We let

$$\mathcal{O}(f) = \{\beta(f) : \beta \in \mathrm{Aut}(P)\}$$

denote the orbit of f under this action. Additionally, for $p \in P$, we write

$$[p] = \{\beta(p) : \beta \in \mathrm{Aut}(P)\}$$

for the orbit of p under the natural action of $\mathrm{Aut}(P)$ on P.

We use $\sim$ to denote an equivalence relation on D_n. Namely, two functions $p, r \in D_n$ are *equivalent*, $p \sim r$, if there is an automorphism $\alpha \in \mathrm{Aut}(D_n)$ such that $p = \alpha(r)$. For a function $p \in D_n$ its *equivalence class* is the set $[p] = \{r \in D_n : r \sim p\}$. We let $\gamma(f)$ denote $|[f]|$. For $m > 1$, let $E_{n,m} = \{p \in D_n : \gamma(f) \equiv 0 \pmod m\}$ and $E^c_{n,m} = D_n - E_{n,m}$. For the class $[p]$, we define its *canonical representative* as the one element in $[p]$ chosen to represent the class. One of the possible approaches is to choose its minimal (according to the total order $\preceq$) element [11]. Sometimes we shall identify the class $[p]$ with its canonical representative and treat $[p]$ as an element in D_n. We let R_n denote the set of equivalence classes and r_n the number of equivalence classes; that is, $r_n = |R_n|$. Values of r_n are described by A003182 OEIS sequence; see Table 1.

Lemma 4. *For every $q \in Q$ and every $f \in P^Q$, the integer $|[f(q)]|$ divides $|\mathcal{O}(f)|$.*

Proof. For every $p \in [f(q)]$ we define

$$\mathcal{G}(p) := \{g \in \mathcal{O}(f) : g(q) = p\}.$$

The sets $\mathcal{G}(p)$, $p \in [f(q)]$ form a partition of $\mathcal{O}(f)$ and the sets $\mathcal{G}(p)$ have the same cardinality. Indeed, for every $\beta \in \operatorname{Aut}(P)$,

$$g \in \mathcal{G}(f(q)) \quad \iff \quad \beta(g) \in \mathcal{G}(\beta(f(q))).$$

□

Lemma 5. *For arbitrary subset $W \subseteq Q$, the cardinality of P^Q is congruent modulo m to the cardinality of*

$$\{f \in P^Q : f(W) \subseteq E^c_{n,m}\}.$$

Proof. For each automorphism $\alpha \in \operatorname{Aut}(P)$ and for each $p \in P$, we have $[p] = [\alpha(p)]$. Hence,

$$p \in E^c_{n,m} \quad \iff \quad \alpha(p) \in E^c_{n,m}$$

and for every function $f \in P^Q$, we have

$$f(W) \subseteq E^c_{n,m} \quad \iff \alpha \circ f(W) \subset E^c_{n,m}$$

Orbits $\mathcal{O}(f)$ form a partition of P^Q. If $f \sim g$ (or in other words if $f \in \mathcal{O}(g)$), then there exists automorphism $\alpha \in \operatorname{Aut}(P)$, such that $g = \alpha \circ f$ and

$$f(W) \subseteq E^c_{n,m} \quad \iff \quad g(W) \subseteq E^c_{n,m}.$$

So we have two kinds of orbits:

- orbits $\mathcal{O}(f)$, where $g(W) \subseteq E^c_{n,m}$ for all $g \in \mathcal{O}(f)$,
- orbits $\mathcal{O}(f)$, where $g(W) \not\subseteq E^c_{n,m}$ for all $g \in \mathcal{O}(f)$.

Moreover, if $f(W) \not\subseteq E^c_{n,m}$, then there exists $w \in W$ such that $f(w) \in E_{n,m}$, hence, m divides $|[f(w)]|$ and by Lemma 4, m divides $|\mathcal{O}(f)|$.

□

6 Counting functions from B^2 to D_n

By Lemma 1, the poset D_{n+2} is isomorphic to the poset $D_n^{B^2}$—the poset of monotone functions from $B^2 = \{00, 01, 10, 11\}$ to D_n. Consider the function G that, for every pair $(x, y) \in D_n^2$, takes the value

$$G(x, y) = \operatorname{re}(x|y, \top) \cdot \operatorname{re}(\bot, x\&y).$$

Observe that $G(x, y)$ is equal to the number of functions $f \in D_n^{B^2}$ with $f(01) = x$ and $f(10) = y$. Function G is well-known, as it is discussed in [3, 4, 11].

For $A \subseteq D_n \times D_n$ let $G(A)$ denote $\sum_{(x,y)\in A} G(x, y)$. By Lemma 1, we have

$$d_{n+2} = G(D_n \times D_n) = \sum_{x\in D_n} \sum_{y\in D_n} G(x, y).$$

Consider the set $W_2 = \{01, 10\}$. By Lemma 5, we have

$$d_{n+2} \equiv G(D_n \times D_n) \equiv G(E_{n,m}^c \times E_{n,m}^c) \pmod m.$$

Observe that, for every automorphism $\pi \in \mathrm{Aut}(B^n)$ and every $x, y \in D_n$, we have $G(x, y) = G(\pi(x), \pi(y))$.

Lemma 6. *Let Y be a subset $Y \subseteq D_n$ and suppose that $\pi(Y) = Y$ for every automorphism $\pi \in \mathrm{Aut}(B^n$; and let x and y be two equivalent, $x \sim y$, elements in D_n. Then*

1. $G(\{x\} \times Y) = G(\{y\} \times Y)$.
2. $G([x] \times Y) = \gamma(x) \cdot G(\{x\} \times Y)$.

Proof. Notice that condition $\pi(Y) = Y$ implies that π is a bijection on Y, or in other words, π permutes the elements of Y.

For (1), observe that

$$\begin{aligned} G(\{x\} \times Y) &= \sum_{s\in Y} G(x, s) = \sum_{s\in Y} G(\pi(x), \pi(s)) \\ &= \sum_{t\in\pi(Y)} G(\pi(x), t) = \sum_{t\in Y} G(\pi(x), t) = G(\{\pi(x)\} \times Y). \end{aligned}$$

We use the fact that $\pi(Y) = Y$. □

Observe that for every automorphism $\pi \in \mathrm{Aut}(b^n)$, we have and $\pi(E_{n,m}^c) = E_{n,m}^c$. Hence, by Lemma 6, we get

Theorem 7.

$$d_{n+2} \equiv \sum_{x\in R_n\cap E_{n,m}^c} \sum_{y\in E_{n,m}^c} \gamma(x) \cdot G(x, y) \pmod m.$$

Here we identify each class $[x] \in R_n$ with its canonical representative.

Example 8. Consider the poset $D_2 = \{0000, 0001, 0011, 0101, 0111, 1111\}$. There are five equivalence classes: namely, $R_2 = \{\{0000\}, \{0001\}, \{0011, 0101\}, \{0111\}, \{1111\}\}$. Two elements: 0101 and 0011 are equivalent. For $m = 2$, we have $E_{2,2} = \{0011, 0101\}$ and $E_{2,2}^c = \{0000, 0001, 0111, 1111\}$. Table 4 presents values of $G(x, y)$ for $x, y \in D_2$. Let

$Y = [0011] = \{0011, 0101\}$. For every permutation $\pi \in S_2$, we have $\pi(Y) = Y$. Furthermore, $G(\{0011\} \times Y) = G(\{0101\} \times Y) = 9 + 4 = 13$; and $G([0011] \times Y) = 2 \cdot 13 = 26$, which is divisible by 2.

Similarly, for $Z = [0001] = \{0001\}$, we have that $\pi(Z) = Z$ for every permutation $\pi \in S_2$. Furthermore, $G(\{0011\} \times Z) = G(\{0101\} \times Z) = 6$; and $G([0011] \times Z) = 2 \cdot 6 = 12$, which is divisible by 2. By summing up all values in Table 4 we obtain $G(D_2 \times D_2) = 168 = d_4$.

x \ y	0000	0001	0011	0101	0111	1111
0000	6	5	3	3	2	1
0001	5	10	6	6	4	2
0011	3	6	9	4	6	3
0101	3	6	4	9	6	3
0111	2	4	6	6	10	5
1111	1	2	3	3	5	6

Table 4: Values of $G(x, y)$ for $x, y \in D_2$.

Example 9 (Continuation of Example 8)**.** By summing the relevant values listed in Table 4, we obtain $G(E^c_{2,2} \times E^c_{2,2}) = 6+5+2+1+5+10+4+2+2+4+10+5+1+2+5+6 = 70$. By Theorem 7, we have $d_4 \equiv 70 \pmod 2$. Indeed, $d_4 = 168$, which is even.

7 Counting functions from B^3 to D_n

In the next two sections, we show that similar techniques can be also applied to functions in $D_n^{B^3}$ and $D_n^{B^4}$. Consider the function H which for every triple $(x, y, z) \in D_n^3$ returns the value

$$H(x, y, z) = \mathrm{re}(\bot, x\&y\&z) \cdot \sum_{s \geq x|y|z} \mathrm{re}(x|y, s) \cdot \mathrm{re}(x|z, s) \cdot \mathrm{re}(y|z, s).$$

Observe that $H(x, y, z)$ is equal to the number of monotone functions $f \in D_n^{B^3}$ with $f(001) = x$, $f(010) = y$ and $f(100) = z$. Thus, we have

$$d_{n+3} = H(D_n^3) = \sum_{x \in D_n} \sum_{y \in D_n} \sum_{z \in D_n} H(x, y, z).$$

Function H is discussed in [3]. Consider the set $W_3 = \{001, 010, 100\}$. By Lemma 5, we have

$$d_{n+3} \equiv G(D_n \times D_n \times D_n) \equiv G(E^c_{n,m} \times E^c_{n,m} \times E^c_{n,m}) \pmod m.$$

Observe that for every automorphism $\pi \in \mathrm{Aut}(B^n)$ and every $x, y, z \in D_n$, we have $H(x, y, z) = H(\pi(x), \pi(y), \pi(z))$.

Lemma 10. *Let Y and Z be subsets $Y, Z \subseteq D_n$ and suppose that $\pi(Y) = Y$ and $\pi(Z) = Z$ for every automorphism $\pi \in \mathrm{Aut}(B^n)$; and let x and y be two equivalent, $x \sim y$, elements in D_n. Then*

1. $H(\{x\} \times Y \times Z) = H(\{y\} \times Y \times Z)$.

2. $H([x] \times Y \times Z) = \gamma(x) \cdot H(\{x\} \times Y \times Z)$.

Proof. (1) $H(\{x\} \times Y \times Z) = \sum_{s\in Y} \sum_{t\in Z} H(x, s, t) = \sum_{s\in Y} \sum_{t\in Z} H(\pi(x), \pi(s), \pi(t)) = \sum_{u\in\pi(Y)} \sum_{v\in\pi(Z)} H(\pi(x), u, v) = \sum_{u\in Y} \sum_{v\in Z} H(\pi(x), u, v) = H(\{\pi(x)\} \times Y \times Z)$. We use the fact that π is a bijection on $Y \times Z$ and permutes the elements of $Y \times Z$. □

As an immediate corollary, we have the following:

Theorem 11.

$$d_{n+3} \equiv \sum_{x\in R_n\cap E^c_{n,m}} \sum_{y\in E^c_{n,m}} \sum_{z\in E^c_{n,m}} \gamma(x) \cdot H(x, y, z) \pmod{m}.$$

Here, again, we identify each class $[x] \in R_n$ with its canonical representative.

Example 12. Consider D_4. There are 168 elements in D_4 and 30 equivalence classes in R_4. The distribution of these equivalence classes based on their γ value is presented in Table 5. For instance, there are six equivalence classes $[x]$ with $\gamma(x) = 1$, two equivalence classes with $\gamma(x) = 3$, and so forth. For $m = 2$, the set $E^c_{4,2}$ contains only twelve elements and $R_4 \cap E^c_{4,2}$ contains eight elements. Similarly, for $m = 3$, the set $E^c_{4,3}$ contains 42 elements and $R_4 \cap E^c_{4,3}$ consists of 15 elements.

Example 13. We employed a Java implementation of the Theorem 11. For $n = 4$ and $m = 2, 3, 4, 6, 12$ we have
$d_7 \equiv 2320978352 \pmod{2}$, and therefore $d_7 \bmod 2 = 0$,
$d_7 \equiv 74128573428 \pmod{3}$, and therefore $d_7 \bmod 3 = 0$,
$d_7 \equiv 128268820802 \pmod{4}$, and therefore $d_7 \bmod 4 = 2$,
$d_7 \equiv 89637133284 \pmod{6}$, and therefore $d_7 \bmod 6 = 0$,
$d_7 \equiv 566167187562 \pmod{12}$, and therefore $d_7 \bmod 12 = 6$.
One can check these values directly by dividing d_7 by 2, 3, 4, 6, and 12.

8 Counting functions from B^4 to D_n

By Lemma 1, the poset D_{n+4} is isomorphic to the poset $D_n^{B^4}$—the set of monotone functions from B^4 to D_n. Consider the function F (also discussed in [3, 4]), which for every six elements $a, b, c, d, e, f \in D_n$, counts how many functions $g \in D_n^{B^4}$ satisfy the following equations: $g(0011) = a$, $g(0101) = b$, $g(1001) = c$, $g(0110) = d$, $g(1010) = e$, $g(1100) = f$.

k	$\lvert\{f \in R_4 : \gamma(f) = k\}\rvert$
1	6
3	2
4	9
6	6
12	7

Table 5: Number of $f \in R_4$ with $\gamma(f) = k$.

For $A \subseteq (D_n)^6$ let $F(A)$ denote $\sum_{(a,b,c,d,e,f)\in A} F(a,b,c,d,e,f)$. By Lemma 1, we have

$$d_{n+4} = F(D_n^6) = \sum_{a\in D_n}\sum_{b\in D_n}\sum_{c\in D_n}\sum_{d\in D_n}\sum_{e\in D_n}\sum_{f\in D_n} F(a,b,c,d,e,f).$$

Consider the set $W_4 = \{0011, 0101, 1001, 0110, 1010, 1100\}$. By Lemma 5, we have

$$d_{n+4} \equiv F(D_n^6) \equiv F((E^c_{n,m})^6) \pmod{m}$$

Observe that for every automorphism $\pi \in \mathrm{Aut}(B^n)$ and every $a, b, c, d, e, f \in D_n$, we have $F(a, b, c, d, e, f) = F(\pi(a), \pi(b), \pi(c), \pi(d), \pi(e), \pi(f))$. Consider Cartesian product $Y = Y_1 \times Y_2 \times Y_3 \times Y_4 \times Y_5$ and let $\pi(y_1, \ldots, y_5) = (\pi(y_1), \ldots, \pi(y_5))$. Observe that, if $\pi(Y_i) = Y_i$ for every i, then $\pi(Y) = Y$ and π permutes the elements of Y.

Lemma 14. *Let Y be a subset $Y \subseteq D_n^5$ and suppose that $\pi(Y) = Y$ for every automorphism $\pi \in \mathrm{Aut}(B^n)$; and let x and y be two equivalent, $x \sim y$, elements in D_n. Then*

1. $F(\{x\} \times Y) = F(\{y\} \times Y)$.
2. $F([x] \times Y) = \gamma(x) \cdot F(\{x\} \times Y)$.

Proof. (1) $F(\{x\} \times Y) = \sum_{s\in Y} F(x, s) = \sum_{s\in Y} F(\pi(x), \pi(s)) = \sum_{u\in\pi(Y)} F(\pi(x), u) = \sum_{u\in Y} F(\pi(x), u) = F(\{\pi(x)\} \times Y)$. We use the fact that π is a bijection on Y and permutes the elements of Y. □

As a corollary we get the following result.

Theorem 15.

$$d_{n+4} \equiv \sum_{a\in R_n\cap E^c_{n,m}}\sum_{b\in E^c_{n,m}}\sum_{c\in E^c_{n,m}}\sum_{d\in E^c_{n,m}}\sum_{e\in E^c_{n,m}}\sum_{f\in E^c_{n,m}} \gamma(a)\cdot F(a,b,c,d,e,f) \pmod{m}.$$

Example 16. We utilized a Java implementation of the Theorem 15. For $n = 4$ and $m = 2, 3, 4, 6, 12$ we get

$d_8 \equiv 53336702474849828$, and therefore $d_8 \bmod 2 = 0$;
$d_8 \equiv 3019662424037271148 \pmod{3}$, and therefore $d_8 \bmod 3 = 1$;
$d_8 \equiv 25754060568741983624 \pmod{4}$, and therefore $d_8 \bmod 4 = 0$;
$d_8 \equiv 14729824485525634108 \pmod{6}$, and therefore $d_8 \bmod 6 = 4$;
$d_8 \equiv 15054599294580333880 \pmod{12}$, and therefore $d_8 \bmod 12 = 4$.

One can check these values directly by dividing d_8 by 2, 3, 4, 6, and 12.

9 Application

To compute remainders of d_9 divided by 5 and 7, we chose the algorithm described in Section 6. Our implementation lists all 490,013,148 elements of R_7 and calculates $\gamma(x)$ and $\text{re}(\perp, x)$ for each element $x \in R_7$. This feat was previously accomplished only by Van Hirtum in 2021 [6]. It is worth noting that the number of elements x in R_n with $\gamma(x) = n!$ for $n > 1$ can be found in the OEIS sequence A220879 (see Table 6). Using the available precalculated sets, we can efficiently determine the 7th term of the sequence, which was not recorded in the OEIS before.

n	A220879 (n)
1	0
2	1
3	0
4	0
5	7
6	7281
7	468822749

Table 6: Inequivalent monotone Boolean functions of n variables with no symmetries.

Our program's most critical part, the Boolean function canonization procedure, is based on Van Hirtum's fast approach [6, Section 5.2.9] and implemented in Rust. Our program is running on a 32-thread machine with Xeon cores.

After the preprocessed data has been loaded into the main memory, the test was performed and the value of d_8 was recomputed in just 16 seconds. However, using this method to check the divisibility of d_9 for any value of m is significantly more challenging.

In order to determine which remainders can be computed by our methods, we can use the information in Table 7. Note that

$$|E^c_{7,m}| = \sum_{\substack{x \in R_7 \\ \gamma(x) \bmod m \neq 0}} \gamma(x).$$

The four smallest $E^c_{7,m}$ are $E^c_{7,7}$ with 9999 elements, $E^c_{7,3}$ with 108873 elements, $E^c_{7,21}$ with 118863 elements, and $E^c_{7,5}$ with 154863 elements. Since d_9 is already known to be divisible by 3, the next step is to compute the remainders of d_9 divided by 5 and 7.

9.1 Remainder of d_9 divided by 5

$$\sum_{x \in R_7 \cap E^c_{7,5}} \sum_{y \in E^c_{7,5}} \gamma(x) \cdot G(x, y) = 1404812111893131438640857806,$$

k	$\lvert\{f \in R_7 : \gamma(f) = k\}\rvert$
1	9
7	27
21	75
30	5
35	117
42	99
70	90
84	9
105	1206
120	4
140	702
210	3255
252	114
315	2742
360	18
420	26739
504	237
630	47242
720	4
840	75024
1260	1024050
1680	3128
2520	20005503
5040	468822749

Table 7: Number of $f \in R_7$ with the given $\gamma(f)$.

therefore, by Theorem 7, we have $d_9 \bmod 5 = 1$. We calculated this number in approximately 7 hours. Moreover, using Theorem 15 we have $d_9 \equiv 157853570524864492086 \pmod 5$, which confirms that $d_9 \bmod 5 = 1$.

9.2 Remainder of d_9 divided by 7

$$\sum_{x \in R_7 \cap E^c_{7,7}} \sum_{y \in E^c_{7,7}} \gamma(x) \cdot G(x, y) = 29989517764506682537562623,$$

therefore, by Theorem 7, we have $d_9 \bmod 7 = 6$. We calculated this number in approximately half an hour.

10 Acknowledgments

We would like to thank the anonymous referee for his useful suggestions and references.

References

[1] M. Aigner. *Combinatorial Theory.* Springer, 1979.

[2] A. E. Brouwer, C. F. Mills, W. H. Mills, and A. Verbeek. Counting families of mutually intersecting sets. *Electron. J. Comb.* **20** (2013).

[3] F. a Campo. Relations between powers of Dedekind numbers and exponential sums related to them. *J. Integer Sequences* **21** (2018), Article 18.4.4.

[4] R. Fidytek, A. W. Mostowski, R. Somla, and A. Szepietowski. Algorithms counting monotone Boolean functions. *Inform. Process. Lett.* **79** (2001), 203–209.

[5] C. Jäkel. A computation of the ninth Dedekind number, arxiv preprint arXiv:2304.00895 [math.CO], 2023.
Available at `https://arxiv.org/abs/2304.00895`.

[6] L. Van Hirtum. A path to compute the 9th Dedekind number using FPGA supercomputing (2021). Master's thesis, available at `https://hirtum.com/thesis.pdf`.

[7] L. Van Hirtum, P. De Causmaecker, J. Goemaere, T. Kenter, H. Riebler, M. Lass, and C. Plessl. A computation of D(9) using FPGA supercomputing, preprint, 2023.
Available at `https://arxiv.org/abs/2304.03039`.

[8] B. Pawelski. On the number of inequivalent monotone Boolean functions of 8 variables. *J. Integer Sequences* **25** (2022), Article 25.7.7.

[9] N. J. A. Sloane. The On-line Encyclopedia of Integer Sequences. Available at `https://oeis.org`.

[10] A. Szepietowski. Fixes of permutations acting on monotone Boolean functions. *J. Integer Sequences* **25** (2022), Article 25.9.6.

[11] D. Wiedemann. A computation of the eighth Dedekind number. *Order* **8** (1991), 5–6.

[12] D. Wiedemann. Letter to N. J. A. Sloane (1990). Available at `https://oeis.org/A000372/a000372.pdf`.

[13] K. Yamamoto. Note on the order of free distributive lattices. *Sci. Rep. Kanazawa Univ.* **2** (1953), 5–6.

2020 *Mathematics Subject Classification*: Primary 06E30.

Keywords: Dedekind number, monotone Boolean function, ninth Dedekind number, congruence modulo, Chinese remainder theorem.

(Concerned with sequences A000372, A001206, A003182 and A220879.)

Received March 15 2023; revised versions received March 16 2023; May 17 2023; June 13 2023; June 14 2023. Published in *Journal of Integer Sequences*, August 16 2023.

Return to Journal of Integer Sequences home page.