

Carryless Arithmetic Mod 10

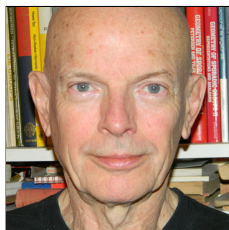
David Applegate, Marc LeBrun, and N. J. A. Sloane



David Applegate (david@research.att.com) received his Ph.D. in Computer Science from Carnegie Mellon and has been at AT&T Shannon Labs since 2000. His research interests include combinatorial optimization, the Traveling Salesman Problem, and other mathematical diversions.



Marc LeBrun (mlb@well.com) was confirmed as an ardent amateur mathematician at age ten, when Martin Gardner graciously answered a fan letter. He is delighted to find professional colleagues who share his interests in recreational arithmetic, and is an enthusiastic contributor to the On-Line Encyclopedia of Integer Sequences.



N. J. A. Sloane (njas@research.att.com) has been at AT&T Bell Labs and later AT&T Shannon Labs since 1969. He has written many books and articles on mathematics, engineering and statistics. He also runs the On-Line Encyclopedia of Integer Sequences.

Nim

Forms of Nim have been played since antiquity and a complete theory was published as early as 1902 (see [3]). Martin Gardner described the game in one of his earliest columns [7] and returned to it many times over the years ([8–16]).

Central to the analysis of Nim is Nim-addition. The Nim-sum is calculated by writing the terms in base 2 and adding the columns mod 2, with *no carries*. A Nim position is a winning position if and only if the Nim-sum of the sizes of the heaps is zero [2], [7].

Is there a generalization of Nim in which the analysis uses the base- b representations of the sizes of the heaps, for $b > 2$, in which a position is a win if and only if the mod- b sums of the columns is identically zero? One such game, Rim_b (an abbreviation of Restricted-Nim) exists, although it is complicated and not well known. It was introduced in an unpublished paper [6] in 1980 and is hinted at in [5]. Despite his interest in Nim, Martin Gardner never mentions Rim_b , nor does it appear in *Winning Ways* [2], which extensively analyzes Nim variants.

In the present paper we focus on $b = 10$, and consider, not Rim_{10} itself, but the arithmetic that arises if calculations, addition and multiplication, are performed mod 10, with *no carries*. Along the way we encounter several new and interesting number sequences, which would have appealed to Martin Gardner, always a fan of integer sequences.

<http://dx.doi.org/10.4169/college.math.j.43.1.043>
MSC: 06D05, 11A63

The fabled residents of the Carryless Islands



© The New Yorker collection/www.cartoonbank.com

"I'm just here for the dental."

—Emily Flake, *The New Yorker*, August 29, 2011.

The carryless primes

If we require that a prime π is a number whose only factorization is 1 times itself, we are out of luck, since every carryless number is divisible by 9, and there would be no primes at all. (For $9 \times 1 = 9$, $9 \times 2 = 8$, $9 \times 3 = 7$, \dots , $9 \times 9 = 1$. So if we construct a number ρ by replacing all the 1's in π by 9's, all the 2's by 8's, \dots then $\pi = 9 \times \rho$, and π would not be a prime.)

There *are* primes, when defined in the right way. Since $1 \times 1 = 1$, $3 \times 7 = 1$ and $9 \times 9 = 1$, all of 1, 3, 7 and 9 divide 1 and so divide any number. We call 1, 3, 7 and 9 *units*, the usual name for integers that divide 1. Units should not be counted as factors when considering if a number is prime (just as factors of -1 are ignored in ordinary arithmetic: $7 = (-1) \times (-7)$ doesn't count as a factorization when considering if 7 is a prime).

So we define a carryless prime to be a non-unit π whose only factorizations are of the form $\pi = u \times \rho$ where u is a unit. Computer experiments suggest that the first few primes are

$$21, 23, 25, 27, 29, 41, 43, 45, 47, 49, 51, 52, 53, 54, 56, 57, 58, 59, 61, 63, \dots, \quad (1)$$

but there are surprising omissions in this list, resulting from some strange factorizations: $2 = 2 \times 51$, $10 = 56 \times 65$, $11 = 51 \times 61$. It is hard to be sure at this stage that the above list is correct, since there exist factorizations where one of the numbers is much larger than the number being factored, such as $2 = 4 \times 5005505553$. One property that makes carryless arithmetic interesting is the presence of *zero-divisors*: the product of two numbers can be zero without either of them being zero: $2 \times 5 = 0$, $628 \times 55 = 0$. Perhaps 21 is the product of two really huge numbers? Nonetheless, the list *is* correct, as we will see (it is now sequence A169887 in [17]).

Algebra to the rescue

The secret to understanding carryless arithmetic is to introduce a little algebra. Let R_{10} denote the ring of integers mod 10, and $R_{10}[X]$ the ring of polynomials in X with coefficients in R_{10} . Then we can represent carryless numbers by elements of $R_{10}[X]$: 21 corresponds to $2X + 1$, 109 to $X^2 + 9$, and so on. Carryless addition and multiplication are simply addition and multiplication in $R_{10}[X]$: our first example,

$$785 + 376 = 51$$

corresponds to

$$(7X^2 + 8X + 5) + (3X^2 + 7X + 6) = 5X + 1,$$

where the polynomials are added or multiplied in the usual way, and the coefficients then reduced mod 10. Conversely, any element of $R_{10}[X]$ represents a unique carryless number (just set $X = 10$ in the polynomial). In fact arithmetic in $R_{10}[X]$ is clearly exactly the same as the arithmetic of carryless numbers. This could be used as a formal definition of carryless arithmetic mod 10. It also shows that this arithmetic is commutative, associative and distributive.

Since $R_{10}[X]$ is a ring, we can not only add and multiply, we can also subtract, something the Carryless Islanders never considered. The negatives of the elements of R_{10} are $-1 = 9$, $-2 = 8$, \dots , $-9 = 1$, and similarly for the elements of $R_{10}[X]$. So the negative of a carryless number is its “10’s complement,” obtained by replacing each nonzero digit d by $10 - d$, for example $-702 = 308$. To subtract A from B , we add $-A$ to B : $650 - 702 = 650 + 308 = 958$. This is equivalent to doing elementary school subtraction where we can “borrow” but don’t have to pay back!

The units in $R_{10}[X]$, that is, the elements that divide 1, are the constants 1, 3, 7, 9, and the carryless primes that we defined are the *irreducible* elements in $R_{10}[X]$, that is, non-units $f_{10}(X) \in R_{10}[X]$ whose only factorizations are of the form $f_{10}(X) = ug_{10}(X)$, where u is a unit and $g_{10}(X) \in R_{10}[X]$. The units can also be written as 1, -1 , 3 and -3 , which more closely relates them to the units 1 and -1 in ordinary arithmetic (3 and -3 act in some ways like the imaginary units i and $-i$, squaring to -1 , for example).

The key to further progress is to notice that R_{10} is the direct sum of the ring R_2 of integers mod 2 and the ring R_5 of integers mod 5. Given $r_{10} \in R_{10}$, we read it mod 2 and mod 5 to obtain a pair $[r_2, r_5]$ with $r_2 \in R_2$, $r_5 \in R_5$. The elements $0, 1, \dots, 9 \in R_{10}$ (or equivalently the carryless digits $0, 1, \dots, 9$) and their corresponding pairs $[r_2, r_5]$ are given by the following table. The Chinese Remainder Theorem guarantees that this is a one-to-one correspondence.

0	1	2	3	4	5	6	7	8	9	(2)
[0,0]	[1,1]	[0,2]	[1,3]	[0,4]	[1,0]	[0,1]	[1,2]	[0,3]	[1,4]	

As a check, we note that $\{1\}$ is the (singleton) set of units in R_2 , while $\{1, 2, 3, 4\}$ is the set of units in R_5 , so the pairs $[1, 1]$, $[1, 2]$, $[1, 3]$ and $[1, 4]$ correspondingly produce the units 1, 7, 3 and 9 of R_{10} .

Similarly, polynomials $f_{10}(X) \in R_{10}[X]$ correspond to pairs of polynomials $[f_2(X), f_5(X)]$, obtained by reading $f_{10}(X)$ respectively mod 2 and mod 5. Conversely, given any such pair of polynomials $[f_2(X), f_5(X)]$, there is a unique $f_{10}(X) \in R_{10}[X]$ that corresponds to them, which can be found using (2). We indicate this by writing $f_{10}(X) \leftrightarrow [f_2(X), f_5(X)]$. If also $g_{10}(X) \leftrightarrow [g_2(X), g_5(X)]$, then $f_{10}(X) +$

$g_{10}(X) \leftrightarrow [f_2(X) + g_2(X), f_5(X) + g_5(X)]$ and $f_{10}(X)g_{10}(X) \leftrightarrow [f_2(X)g_2(X), f_5(X)g_5(X)]$.

We are now in a position to answer many questions about carryless arithmetic.

The carryless primes, again

What are the irreducible elements $f_{10}(X) \in R_{10}[X]$? If $f_{10}(X) \leftrightarrow [f_2(X), f_5(X)]$ is irreducible then certainly f_2 and f_5 must be either units or irreducible, for if $f_2 = g_2h_2$ then we have the factorization $[f_2, f_5] = [g_2, f_5][h_2, 1]$. Also $[f_2, f_5] = [f_2, 1][1, f_5]$, so one of f_2, f_5 must be irreducible and the other must be a unit. So the irreducible elements in $R_{10}[X]$ are of the form $[f_2(X), u]$, where $f_2(X)$ is an irreducible polynomial mod 2 of degree ≥ 1 and $u \in \{1, 2, 3, 4\}$, together with elements of the form $[1, f_5(X)]$, where $f_5(X)$ is an irreducible polynomial mod 5 of degree ≥ 1 .

The irreducible polynomials mod 2 are $X, X + 1, X^2 + X + 1, \dots$, and the irreducible polynomials mod 5 are $uX, uX + v, \dots$, where $u, v \in \{1, 2, 3, 4\}$ (see entries A058943, A058945 in [17]). The first few irreducible elements in $R_{10}[X]$ are therefore $[X, 1], [X, 2], [X, 3], [X, 4], [X + 1, 1], [X + 1, 2], \dots$, and $[1, X], [1, 2X], [1, 3X], [1, 4X], [1, X + 1], [1, 2X + 1], \dots$. The corresponding carryless primes, according to (2), are 56, 52, 58, 54, 51, 57, \dots , and 65, 25, 85, 45, 61, 21, \dots . And so we can verify that the list in (1) is correct.

We will call a number with at least two digits in which all digits except the rightmost are even but the rightmost is odd an *e-type number* (A143712), and a number with at least two digits in which all digits except the rightmost are 0 or 5 and the rightmost is neither 0 nor 5 an *f-type number* (A144162). Similarly, we call the primes corresponding to the irreducible elements $[1, f_5(X)]$ *e-type primes*, and the primes corresponding to the irreducible elements $[f_2(X), u]$ *f-type primes*.

We also see that our earlier concern about the primality of 21 was groundless. It is impossible for the length (in decimal digits) of a nonzero carryless product to be less than the length of both of the factors. This follows from the fact that if $\ell(n)$ is the number of decimal digits in the number $n > 0$ corresponding to a pair $[f_2(X), f_5(X)]$, then $\ell(n) = 1 + \max\{\deg f_2, \deg f_5\}$. So if $mn > 0$, $\ell(mn) \geq \min\{\ell(m), \ell(n)\}$.

Also, since we know how many irreducible polynomials mod 2 and mod 5 there are of given degree (see A001037, A001692 in [17]), we can write down a formula for the number of k -digit carryless primes, something that we cannot do for ordinary primes, namely

$$\frac{4}{k-1} \sum_{d \text{ divides } k-1} \mu\left(\frac{k-1}{d}\right) (2^d + 5^d),$$

for $k \geq 2$, where μ is the Möbius function (A008683). There are 28 primes with two digits (the twenty listed in (1), together with 65, 67, 69, 81, 83, 85, 87, 89), 44 with three digits, \dots (A169962). For large k the number is about $4 \cdot 5^{k-1}/(k-1)$, whereas the number of ordinary primes with exactly k digits is much larger, about $9 \cdot 10^{k-1}/(k \log 10)$, so carryless primes are much rarer than ordinary primes.

Incidentally, the *prime ideals* in $R_{10}[X]$, as distinct from the irreducible elements, all have a single generator, which is one of $[0, 1], [1, 0], [1, 1], [f_2(X), 1], [1, f_5(X)]$, where $f_2(X), f_5(X)$ are irreducible (cf. [18, Chap. III, Thm. 30]).

The carryless squares, again

Squaring a mod 2 polynomial is easy: $f_2(X)^2 = f_2(X^2)$. So if n corresponds to the pair $[f_2(X), f_5(X)]$, n^2 corresponds to $[f_2(X^2), f_5(X)^2] = [f_2(X^2), 0] + [0, f_5(X)^2]$. This gives a two-step recipe for producing all carryless squares. First find (using (2)) the carryless number m corresponding to $[0, f_5(X)^2]$, where $f_5(X)$ is any polynomial mod 5. The effect of adding a nonzero $[f_2(X^2), 0]$ changes some subset of the digits in positions 0, 2, 4, \dots of m by the addition of 5 mod 10.

For example, if $f_5(X) = X + 2$, $f_5(X)^2 = X^2 + 4X + 4$, and by (2) $[0, f_5(X)^2]$ corresponds to the carryless square $m = 644$. We now add 5 mod 10 to any subset of the digits in positions 0, 2, 4, 6, \dots of m (considering m extended by prefixing it with any number of zeros), obtaining infinitely many squares 644, 649, 144, 149, \dots , 50644, 5050649, \dots

This also leads to a formula for the number of k -digit carryless squares. For even k the number is 0, and for odd k it is

$$\frac{1}{2}9 \cdot 10^{(k-1)/2} + 2^{(k-3)/2}$$

(zero is excluded from the count). There are five squares of length 1 (namely 1, 4, 5, 6 and 9), 46 of length 3, \dots (see A059729, A169889, A169963). For large odd k there are about twice as many k -digit carryless squares as ordinary squares.

Divisors and factorizations

What about the factorization of numbers into the product of carryless primes? Unfortunately, the existence of zero-divisors complicates matters, and it turns out that there is no natural way to define, for example, an analog of the usual sum-of-divisors function $\sigma(n)$. In our analysis we define several classes of carryless numbers:

$\mathcal{U} := \{1, 3, 7, 9\}$, the units,

$\mathcal{E} := \{0, 2, 4, 6, 8, 20, 22, \dots\}$, the “evenish” numbers, in which all digits are even (A014263),

$\mathcal{F} := \{0, 5, 50, 55, \dots\}$, the “fiveish” numbers, in which all digits are 0 or 5 (A169964),

$\mathcal{Z} := \mathcal{E} \cup \mathcal{F} = \{0, 2, 4, 5, 6, 8, 20, 22, \dots\}$, the zero-divisors (A169884),

$\mathcal{N} := \{1, 3, 7, 9, 10, 11, 12, 13, \dots\}$, the positive numbers not in \mathcal{Z} (A169968).

Suppose d is a carryless divisor of n , that is, there is a number q such that $d \times q = n$. What can be said about the possible choices for q ? One can show—we omit the straightforward proofs—that

- if $d \in \mathcal{N}$ then there is a unique q ,
- if $d \in \mathcal{E}$ then $d \times q' = n$ if and only if $q' = q + v$ for some $v \in \mathcal{F}$,
- if $d \in \mathcal{F}$ then $d \times q' = n$ if and only if $q' = q + e$ for some $e \in \mathcal{E}$.

The same distinctions are needed to describe factorizations into primes.

- If $n \in \mathcal{N}$ then n has a unique factorization as a carryless product of primes, up to multiplication by units. For example, we already saw $10 = 56 \times 65$. But we also

have $10 = (3 \times 56) \times (7 \times 65) = 58 \times 25 = (9 \times 56) \times (9 \times 65) = 54 \times 45 = 9 \times 52 \times 25$, etc., illustrating the nonuniqueness. Also $11 = 51 \times 61$; $101 = 21 \times 29 \times 51$, $1234 = 23 \times 23 \times 23 \times 51 \times 51 \times 52$. It follows that any non-unit in \mathcal{N} can be written both as $e \times f$ and $e' + f'$, where e and e' are e-type numbers and f and f' are f-type numbers. For example, $12 = 81 \times 52 = 61 + 51$.

- If $n \in \mathcal{E}$ then n has a unique factorization as 2 times a product of e-type primes, up to multiplication by units (in this case, every f-type prime divides n). For example, $20 = 2 \times 65$, $22 = 2 \times 61$, $2468 = 2 \times 69 \times 69 \times 69$.
- If $n \in \mathcal{F}$ then n has a unique factorization as 5 times a product of f-type primes, up to multiplication by units (in this case, every e-type prime divides n). For example, $50 = 5 \times 52$, $505 = 5 \times 51 \times 51$.

Here are the analogous statements about divisors:

- if $n \in \mathcal{N}$, n has only finitely many divisors. If d divides n and $u \in \mathcal{U}$, then $d \times u$ divides n . The divisors may be grouped into equivalence classes $d \times \mathcal{U}$. Since the sum of the elements of \mathcal{U} is zero, so is the sum of the divisors of n .
- if $n \in \mathcal{E}$, d divides n , $u \in \mathcal{U}$ and $v \in \mathcal{F}$, then $d \times u + v$ divides n . So n has infinitely many divisors, belonging to equivalence classes $d \times \mathcal{U} + \mathcal{F}$.
- if $n \in \mathcal{F}$, d divides n , $u \in \mathcal{U}$ and $e \in \mathcal{E}$, then $d \times u + e$ divides n . So n has infinitely many divisors, belonging to equivalence classes $d \times \mathcal{U} + \mathcal{E}$.

Any attempt to define a sum-of-divisors function must specify how to choose representatives from the equivalence classes. There seems to be no natural way to do this. One possibility would be to choose the smallest decimal number in each class, but this seems unsatisfactory (since it depends on the ordering of decimal numbers, another concept the islanders seem not to be familiar with).

Further number theory

In summary, we can help the Carryless Islanders by defining subtraction, prime numbers, and factorization into primes. But further concepts such as the number of divisors, the sum of divisors and perfect numbers seem to lie beyond these Islands.

However, many other carryless analogs are well-defined, including including triangular numbers (A169890), cubes (A169885), partitions (A169973), greatest common divisors and least common multiples, and so on. Some seem exotic, while other familiar sequences simply become periodic. For example, the analog of the Fibonacci numbers coincides with the sequence of Fibonacci numbers read mod 10, A003893, which becomes periodic with period 60 (the periodicity of the Fibonacci numbers to any modulus being a well-studied subject, see sequence A001175). Similarly, the analogue of the powers of 2 (A000689) becomes periodic with period 4. We might also generalize beyond simple squares, cubes, etc. and investigate the properties of polynomials or power series based on carryless operations—How do these factor? What are their fixed points?—and so on.

Taking a different tack, carryless mod 10 partitions are enumerated in A169973, which may be derived as the coefficients of z^n in the formal expansion of the analog of the classic partition generating function $\prod_{k=1}^{\infty} (1 + z^k)$, wherein powers of z are multiplied together by combining their exponents with carryless mod 10 addition instead of the ordinary sum.

Afterword

There's a great deal yet to be explored in these Carryless Islands! Watch for our next paper on another carryless arithmetic, in which operations on single digits are defined by $a \oplus b = \max\{a, b\}$, $a \otimes b = \min\{a, b\}$. We call this "dismal arithmetic."

When the *Handbook of Integer Sequences* was published 39 years ago, Martin Gardner was kind enough to write in his *Mathematical Games* column of July 1974 that "every recreational mathematician should buy a copy forthwith." That book contained 2372 sequences: today its successor, the *On-Line Encyclopedia of Integer Sequences* (or OEIS) [17], contains nearly 200,000 sequences. We were about to write to Martin about carryless arithmetic when we heard the sad news of his death. This article, the first of a series on various kinds of carryless arithmetic, is offered in his honor.

Summary. What might arithmetic look like on an island that eschews carry digits? How would primes, squares and other number theoretical concepts play out on such an island?

References

1. Marcia Ascher, *Mathematics Elsewhere: An Exploration of Ideas Across Cultures*, Princeton University Press, Princeton, NJ, 2002.
2. E. R. Berlekamp, J. H. Conway, and R. K. Guy, *Winning Ways for Your Mathematical Plays*, A K Peters, Wellesley MA, 2nd ed., 4 vols, 2004.
3. C. L. Bouton, Nim, a game with a complete mathematical theory, *Ann. Math.* **3** (1902) 35–39; available at <http://dx.doi.org/10.2307/1967631>
4. J. H. Conway, *On Numbers and Games*, Academic Press, NY, 1976.
5. T. S. Ferguson, Some chip transfer games, *Theoret. Comput. Sci.* **191** (1998) 157–171; available at [http://dx.doi.org/10.1016/S0304-3975\(97\)00135-7](http://dx.doi.org/10.1016/S0304-3975(97)00135-7)
6. J. A. Flanigan, NIM, TRIM and RIM, unpublished document, Mathematics Department, University of California at Los Angeles, 1980; available at <http://citeseer.ist.psu.edu/viewdoc/summary?doi=10.1.1.74.955>.
7. Martin Gardner, Nim and Tac Tix, *The Scientific American Book of Mathematical Puzzles and Diversions*, Simon & Schuster NY, 1959.
8. ———, Jam, Hot and Other Games, *Mathematical Carnival*, Vintage Books NY, 1977.
9. ———, Nim and Hackenbush, *Wheels, Life and Other Mathematical Amusements*, W. H. Freeman NY, 1983.
10. ———, Sim, Chomp and Race Track, *Knotted Doughnuts and Other Mathematical Entertainments*, W. H. Freeman NY, 1986.
11. ———, Dodgem and Other Simple Games, *Time Travel and Other Mathematical Bewilderments*, W. H. Freeman NY, 1988.
12. ———, Wythoff's Nim, *Penrose Tiles to Trapdoor Ciphers . . . and the Return of Dr. Matrix*, W. H. Freeman NY, 1989.
13. ———, Matches, *Mathematical Circus*, Mathematical Association of America, Washington DC, revised ed., 1992.
14. ———, The Rotating Table and Other Problems, *Fractal Music, Hypercards and More . . .*, W. H. Freeman NY, 1992.
15. ———, Lavinia Seeks a Rule and Other Problems, *The Last Recreations: Hydras, Eggs and Other Mathematical Mystifications*, Springer NY, 1997.
16. ———, Surreal Numbers, *The Colossal Book of Mathematics*, W. W. Norton NY, 2001.
17. The OEIS Foundation Inc., *The On-Line Encyclopedia of Integer Sequences* (2011); available at <http://oeis.org>.
18. O. Zariski and P. Samuel, *Commutative Algebra*, Van Nostrand NY, vol. I, 1958.