Modular Arithmetic and Doomsday

Blake Thornton

Much of this is due directly to Joshua Zucker and Paul Zeitz.

1. **Subtraction Magic Trick.** While blindfolded, a magician asks a member from the audience to write a 10 digit number on the board. The magician then asks the volunteer to reverse the digits and subtract the smaller number from the larger number. Then, the volunteer circles any one of the digits of the result (except, the volunteer is not allowed to circle 0) and read all the digits to the magician. The magician then tells the audience what the circled digit is. How is this trick done? Why does the trick work? By the way, there is nothing special about the number of digits, the number could have been any length.

2. **Modular Arithmetic.** There are several ways to think about modular arithmetic. Here are a couple.

   We say that $x \equiv y \pmod{n}$ if x and y have the same remainder when they are divided by n. Another way to say this is that $x \equiv y \pmod{n}$ if n divides $x - y$.

   In any case, we would say, "x is congruent to y mod (or modulo) n."

   (a) What are the possible remainders when dividing by 2? Every integer will be congruent to one of these numbers mod 2.

   (b) What do we call integers that are congruent to 0 mod 2?

   (c) What do we call integers that are congruent to 1 mod 2?

   (d) What are the possible remainders when dividing by 3?

   (e) What are the possible remainders when dividing by n?

   (f) Show that if $a \equiv x \pmod{n}$ and $b \equiv y \pmod{n}$ then $a + b \equiv x + y \pmod{n}$ and $ab \equiv xy \pmod{n}$.

   (g) What is the remainder of 324^{3847} when divided by 5?

   (h) Let $N = 2^{2008}$. Find the remainders when N is divided by each of the primes $2, 3, 5, 7, 11$ and 13.

3. **Divisibility tests.** Can you see why these work? Can you explain these in terms of modular arithmetic?

   (a) A number is divisible by two if and only if the last digit is even.

   (b) A number is divisible by three if and only if the sum of the digits is divisible by 3.

(c) A number is divisible by five if and only if the last digit is a 0 or 5.

(d) A number is divisible by nine if and only if the sum of the digits is divisible by 9.

(e) A number is divisible by four if and only if the last two digits (taken as a two digit number) are divisible by 4.

(f) Divisibility by 11?[1]

(g) Divisibility by 7?

(h) Divisibility by 13?[2]

(i) Divisibility by 19? Can you find a similar rule to the divisibility by 7 and 13 tests?

(j) Use your divisibility test to check divisibility of :

i. 1234567

ii. 12345678

iii. 70642

iv. 418418

(k) Is 349602 divisible by 3? If not, what is the nearest number that is divisible by 3?

(l) How can you check divisibility by 6? Is 73645362 divisible by 6?

(m) How can you check divisibility by 8?[3]

(n) How can you check divisibility by 27?[4]

(o) What are the factors of 99, 999, 9999 and 99999. Do these lead to any useful divisibility tests?

4. **Final Digits Sum.** For an integer n, let $f(n)$ denote the sum of the digits of n.

(a) For any integer n, explain why the sequence

$$f(n), f(f(n)), f(f(f(n))), \ldots$$

will eventually become constant. This constant value is called the *final digits sum* of n.

(b) Experiment with the final digits sum for products of twin primes. Twin primes are primes that are 2 apart. So, for example 3 and 5 are twin primes. 11 and 13 are also twin primes.

(c) Let $N = 4444^{4444}$. Find $f(f(f(N)))$.

5. **Squares.**

(a) What are all the square numbers mod 2? **Solution:** If you square an even number you get an even number. If you square an odd number you get an odd number.

Another way to say this is that $0^2 = 0$ and $1^2 = 1$ and those are all the squares mod 2—you only have to check 2 numbers!

[1] You can use the fact that $10 \equiv -1 \pmod{11}$

[2] You can use the fact that $1001 = 7 \cdot 11 \cdot 13$

[3] Hint: 1000 is divisible by 8

[4] Hint: 999 is divisible by 27

(b) What are all the squares mod 3? In other words, what are the possible remainders when you divide a square number by 3?

(c) What are all the squares mod 4? Explain why any prime equal to 3 (mod 4) cannot be made by adding two squares.

(d) What about squares mod 5? 7? 8? 10?

6. **Modular "Division"**. By "division" we really mean multiplying the an inverse. But, we want to stick with integers. So, for example in mod 12, we have $5 \cdot 5 = 25 \equiv 1 \pmod{12}$ and so the inverse of 5 is 5.

   (a) Here's another way to think of it. If we want to divide 6 by 2 we want to fill in the question mark: $2 \times ? = 6$. But, if we are working mod 12 then there are actually two ways to fill in this question mark. Find them.

   (b) Make a multiplication table for mod 5, remembering only to write the remainder when you divide by 5. Which numbers can be multiplied to get 1?

   (c) Make a multiplication table for mod 6, remembering only to write the remainder when you divide by 6. Which numbers can be multiplied to get 1?

   (d) Figure out the patterns. Which numbers can be multiplied to make 1 in which mod systems? For example, will 87 have an inverse mod 99? Will 91 have an inverse mod 137?

7. **Powers.**

   (a) What are the powers of 2 mod 5?

   (b) What are the powers of 2 mod 10?

   (c) What are the powers of 2 mod 6?

   (d) What are the powers of 2 mod 17?

   Look for patterns.

8. **Fermat's Little Theorem.** Examine the powers of a given $x^n \pmod{n}$ for different values of x and n. In particular, look at $n = 5, 6, 7$ and all possible values of x.

   See if you can see and prove a pattern.

9. **Factorials.** For a fixed value of n, $n! \equiv 0 \pmod{n}$ (why?). But, what about $(n-1)! \pmod{n}$? Compute $(n-1)! \pmod{n}$ for various values of n. See if you can find and prove a pattern.

10. **John Conway's Doomsday Algorithm.** This is a method to determine the day of the week quickly without a calendar or calculator. I will tell you how the algorithm works for dates in the 1900s. Your job is to learn the algorithm and figure out why it works.

    - For each year, Doomsday is defined to be the day of the week that the last day of February falls on (2/28 for ordinary years, 2/29 for leap years).
    - For any year, the dates 4/4, 6/6, 8/8, 10/10 and 12/12 are Doomsdays.
    - For any year, the dates 5/9, 9/5, 7/11, 11/7 are Doomsdays ("A 9 to 5 job at the 7-11")

- The "last" day of January is a Doomsday, if we define this to be 2/1 in a leap year.
- Facts to remember: Doomsday for 1900 is Wednesday, Doomsday for 2000 is Tuesday.
- All days are regarded as modulo 7, with Sunday equal to 0 (you can remember this as noneday, with nuns in a church). Therefore Monday is 1, Tuesday is 2, etc.

Here is how you compute the day of the week for a given date (with the example being February 21, 2008).

I. Determine the number of days (in mod 7) that the date is from a Doomsday.
   - For 2/21/08 we are -8 from the Doomsday of 2/29, which is equal to 6 (mod 7). We are also 20 days from the Doomsday of 2/1 (remember 2008 is a leapyear) which is also equal to 6 (mod 7).

II. Add in for the century: +3 (Wednesday) for 1900, +2 (Tuesday) for 2000.
   - +2 since we are in the year 2008.

III. Dozen: divide the year of concern by 12, write down the quotient.
   - Our year is 08, 8/12 is 0 with remainder 8.

IV. Remainder of division by 12
   - For the year 07, the remainder was 8.

V. Divide the reminder in Part IV by 4, write down the quotient. (Number of leap years in the remainder.)
   - 8/4 is 2 with a reminder of 0.

VI. Add everything up (mod 7)
   - $6 + 2 + 0 + 8 + 2 = 18 \equiv 4 \pmod 7$, so February 21, 2008 is a Thursday!

(a) Practice this with the following dates:
   - July 17, 1970 (Friday)
   - May 15, 1999 (Saturday)
   - Christmas day in 2047 (Wednesday)
   - Your birthday this year
   - Your birthday

(b) Why does it work???

(c) What about for other centuries?

For more information see `http://en.wikipedia.org/wiki/Doomsday_algorithm`

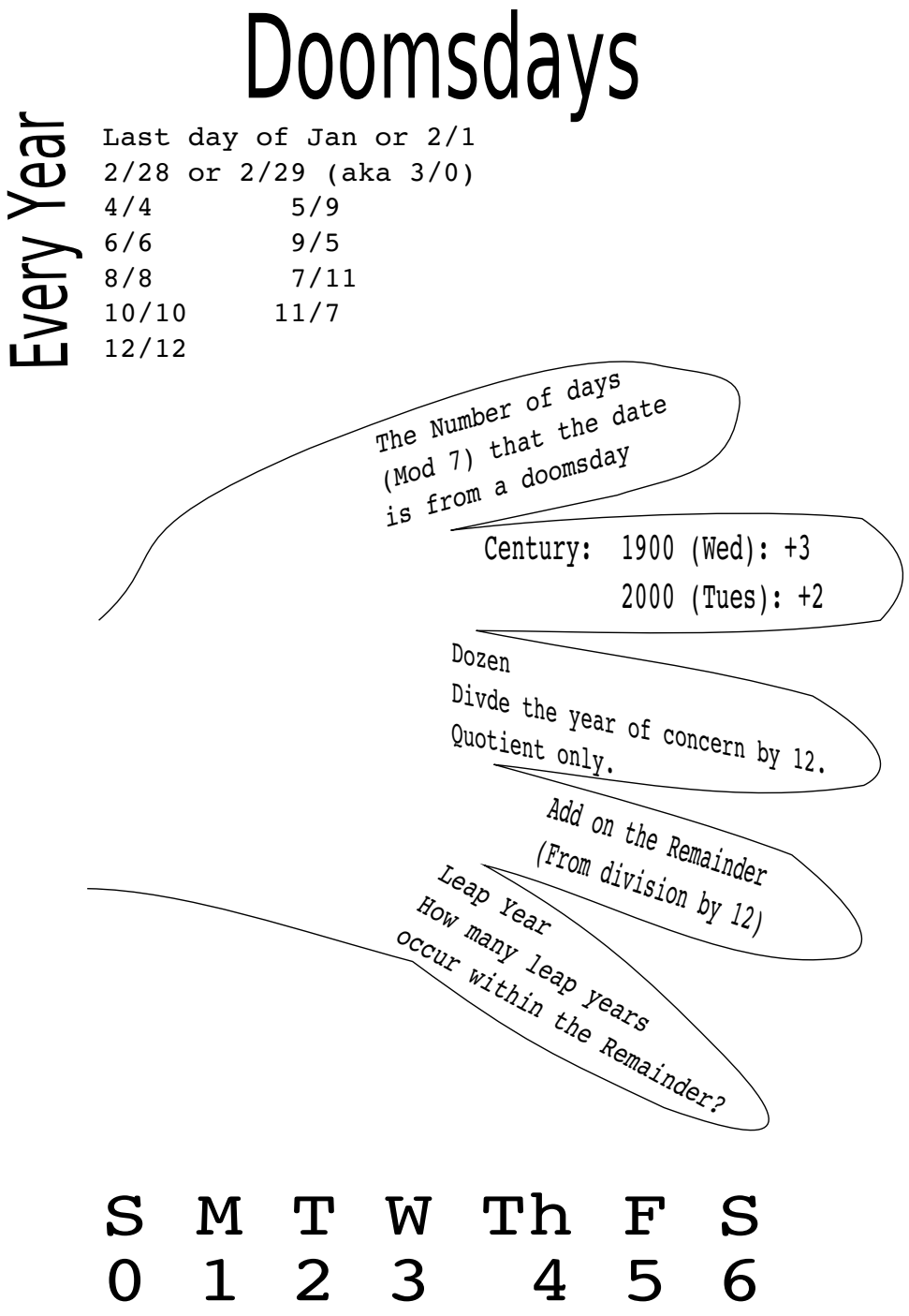

Figure 1: Conway's Doomsday Method

1 Exercises

11. Give at least two different examples, using two different modulus, of two nonzero numbers multiplying to give 0.

12. Can you find a modulus where it is never the case that two nonzero numbers multiply to 0? Write down the multiplication table for your modulus to be sure. Is it the only one possible modulus, or are there others?

13. Solve for x, where possible. If there is no inverse write "No inverse exists!"

    (a) $3x \equiv 1 \pmod 8$

    (b) $5x \equiv 1 \pmod 7$

    (c) $6x \equiv 1 \pmod{11}$

    (d) $2x \equiv 1 \pmod{12}$

    (e) $8x \equiv 1 \pmod{15}$

    (f) $9x \equiv 1 \pmod{15}$

    (g) $2x \equiv 1 \pmod{1000}$

14. Fix a prime number p. The *order* of a number $x \pmod p$ is the smallest positive integer n such that $x^n \equiv 1 \pmod p$. So, for example, if $p = 5$ then the order of $2 \pmod 5$ is 4 because $2^4 \equiv 1 \pmod 5$.

    (a) Find the order of all nonzero numbers in $\mathbb{Z}_3$.

    (b) Find the order of all nonzero numbers in $\mathbb{Z}_5$.

    (c) Find the order of all nonzero numbers in $\mathbb{Z}_7$.

    (d) Find the order of all nonzero numbers in $\mathbb{Z}_{11}$.

    (e) Find the order of all nonzero numbers in $\mathbb{Z}_{13}$.

    (f) Find the order of all nonzero numbers in $\mathbb{Z}_{17}$.

    (g) Find the order of all nonzero numbers in $\mathbb{Z}_{19}$.