PROBLEM-SOLVING AND PROOFS: ASSIGNMENT 7
DUE FRIDAY, APRIL 28, 4PM.

Problems to be handed in. Solve three of the following four problems.

(1) (a) Reduce 2^{100} modulo 13.
(b) Reduce 11^{1000} modulo 8.

We will use the fact that if $a \equiv b \mod n$, then $a^k \equiv b^k \mod n$ for any non-negative integer k. Using Fermat's little theorem[1] or by direct calculation, one has $2^{12} \equiv 1 \mod 13$. Thus,

$$\begin{aligned} 2^{100} &\equiv (2^{12})^8 \cdot 2^4 \mod 13 \\ &\equiv 1^8 \cdot 2^4 \mod 13 \\ &\equiv 16 \mod 13 \\ &\equiv 3 \mod 13 \end{aligned}$$

So we have $2^{100} \equiv 3 \mod 13$.

(b) We compute $11^2 \equiv 121 \equiv 1 \mod 8$. It then follows that $11^{1000} = (11^2)^{500} \equiv 1 \mod 8$.

(2) Let $a, b, c \in \mathbb{Z}$, and suppose that 5 divides $a^2 + b^2 + c^2$. Prove that 5 divides at least one of a, b, or c.

We will prove the contrapositive of this question. That is, if 5 does not divide a, b or c, then 5 does not divide $a^2 + b^2 + c^2$.

Suppose that 5 does not divide a, then a must be congruent to either 1,2,3 or 4 mod 5. We notice that the squares of these numbers mod 5 are given by:

$$\begin{aligned} 1^2 &= 1 \mod 5 \\ 2^2 &= 4 \mod 5 \\ 3^2 &= 4 \mod 5 \\ 4^2 &= 1 \mod 5 \end{aligned}$$

So even though there are 4 different possibilities we need to check for each of the a, b and c, since we are checking something about a^2, b^2, and c^2, we really only need to check two possibilities for each. These are given in the table below:

[1] I have a truly marvelous proof of this, which this footnote is too small to contain

$a^2 \mod 5$	$b^2 \mod 5$	$c^2 \mod 5$
1	1	1
1	1	4
1	4	1
1	4	4
4	1	1
4	1	4
4	4	1
4	4	4

The symmetry of $a^2 + b^2 + c^2$ with respect to permutations of a, b and c means that the coloured entries in the table are equivalent, so in fact, there are exactly four cases we need to check. Remember that we are proving the contrapositive, so we wish to show that $a^2 + b^2 + c^2$ is not congruent to 0 mod 5. Let us now check the four cases.

- $1 + 1 + 1 \equiv 3 \mod 5$
- $1 + 1 + 4 \equiv 1 \mod 5$
- $1 + 4 + 4 \equiv 4 \mod 5$
- $4 + 4 + 4 \equiv 2 \mod 5$

In all cases, we find that $a^2 + b^2 + c^2$ is not congruent to 0 mod 5, and the result follows.

(3) Prove that every year (including leap years) has at least one Friday the 13th. What is the maximum number of Friday the 13ths in a year?

We will answer both parts of this question at the same time. Our first observation is that the 13th of any given month will fall on a Friday if and only if the month begins with a Sunday, so we are looking for months that begin with a Sunday. Now consider the following table:

Month	Days in the month mod 7
January	3
February	0
March	3
April	2
May	3
June	2
July	3
August	3
September	2
October	3
November	2
December	3

If we denote the days of the week by an integer mod 7, with Sunday being 0 mod 7 (and therefore Monday is 1 mod 7 and so on...), then we want to show that every year has at least one month beginning with 0 mod 7.

If a month begins with a given day, say $a \mod 7$, then the following month will begin with the day $a + k \mod 7$, where k is given by the value of the corresponding row in the table above. For example, if the 1st of January is a Thursday ($4 \mod 7$), then the 1st of February will be a Sunday ($4+3 \mod 7$). The days of each date of the year are uniquely determined once we specify the day of the 1st of January, and since there are 7 ways to do that, there are 7 possible types of years. We will now list all of these possibilities. Let's start with any year that begins on a Sunday[2]. The days of the 1st of each month are given by:

$$0, 3, 3, 6, 1, 4, 6, 2, 5, 0, 3, 5.$$

We see that in this case, there are exactly two months that begin with a Sunday (January and October), and so there will be exactly 2 Friday the 13ths. We could go through the other 6 cases, but that seems like a lot of typing, so instead let's be a little clever. We notice that if we were to change the day of January the first to, say, a Monday, then each number in the above list simply gets shifted by 1 (mod 7 of course). Since each congruence class mod 7 is represented in the list above, shifting every element of the list will still have a list containing every congruence class. In particular, there will always be the congruence class 0 somewhere in the list, and therefore there will always be a Friday the 13th. The maximum number of Friday the 13ths occurs when the most repeated congruence class in the above list is shifted to 0. In the above list the most repeated congruence class is a 3 (occurring in months February, March, and November), so when the year begins on a Thursday (which shifts all the congruence classes in the above list by 4), the months of February, March, and November will all begin on a Sunday, and will all therefore have Friday the 13ths.

The case of the leap years is left as an exercise to the reader (simply go to the table at the start of the question and replace the 0 in the February row with a 1, then go through the same argument).

(4) *Divisibility by 11*

(a) Formulate and prove a criterion for an integer n to be divisible by 11 in terms of the digits of n.

To find out if a number is divisible by 11, take the alternating sum of the digits (from right to left). The original number is divisible by 11 iff this sum is.

Proof: Let

$$n = \sum_{j=0}^{k} a_j 10^j$$

be the decimal expansion of the number n. Since $10^j \equiv (-1)^j \mod 11$, we have

$$n \equiv \sum_{j=0}^{k} a_j (-1)^j \equiv a_0 - a_1 + a_2 - a_3 \ldots \mod 11.$$

Thus, n is divisible by 11 iff the alternating sum of its digits is.

(b) A number is *palindromic* if it reads the same backwards and forwards, e.g. 183381. Prove that a palindromic number with an even number of digits is always divisible by 11.

This result follows from the previous part, since the alternating sum will now contain exactly two of each digit, each having the opposite sign.

[2]Which, coincidentally, includes this year.