Some Remainder Problems

What is the remainder when ...

1. ... 12345 is divided by 11?
2. ... $10 + 11 + 12$ is divided by 6?
3. ... $1 + 2 + 3 + 4 + 5 + 6 + 7 + 8 + 9$ is divided by 5?
4. ... $2009^2 + 2010 + 2011$ is divided by 11?
5. ... $100^2 + 101^2$ is divided by 8?
6. ... the sum of the numbers from 1 to 100 is divided by 5?
7. ... the sum of all odd numbers between 1000 and 2000 is divided by 10?
8. ... 8^{1000} is divided by 7?
9. ... 5^{1001} is divided by 6?
10. ... $2^{120359812348080931463727896861293867 49}$ is divided by 3?
11. ... $3^{8675309}$ is divided by 5?
12. ... $2009^{2009^{2009}}$ is divided by 3?
13. ... $n^3 + 2n + 1$ is divided by 3 (for any number n)?

Modular Arithmetic

We say that

$$a \equiv b \mod n$$
("a is *congruent* to b mod n")

if a and b differ by a multiple of n, or in other words $n \mid (b-a)$. For example,

$$15 \equiv 4 \mod 11, \quad 22 \equiv 7 \mod 5, \quad 34 \equiv -8 \mod 7.$$

because $15 - 4 = 11 = 1 \cdot 11$, $22 - 7 = 15 = 3 \cdot 5$, $34 - (-8) = 42 = 6 \cdot 7$.

Here are some different statements that all mean the same thing:

- $a \equiv b \mod n$
- $n \mid (b-a)$
- $b - a$ is a multiple of n
- a and b differ by a multiple of n
- a and b have the same remainder when divided by n
- If $a = q_a n + r_a$ and $b = q_b n + r_b$, where $0 \leq r_a < n$ and $0 \leq r_b < n$, then $r_a = r_b$.

What is amazing is that arithmetic still "works", in much the usual way. That is:

$$\left\{ \begin{array}{l} a \equiv b \mod n \\ c \equiv d \mod n \end{array} \right\} \Longrightarrow \left\{ \begin{array}{l} a + c \equiv b + d \mod n \\ ac \equiv bd \mod n. \end{array} \right\}$$

How to think of this? A few ways:

- We're computing sums and products but instead of the answer all we care about is the remainder when the answer is divided by n.
- We're defining a new sort of number system, which only has the numbers 0, 1, 2, ..., $n-1$, with special rules addition and multiplication defined.
- We're identifying all numbers which differ by a multiple of n. Thus we have

  $$0 \equiv n \equiv 2n \equiv \cdots$$
  $$1 \equiv (n+1) \equiv (2n+1) \equiv \cdots,$$

  and so forth (along with negative integers too), and we're talking about what happens when you add/multiply representatives of any two equivalence classes.

Powers Mod n

1. For each a and n, write the powers of a modulo n, i.e. what is $a, a^2, a^3, \cdots$?

   (a) $a = 2$, $n = 5$

   (b) $a = 3$, $n = 5$

   (c) $a = 2$, $n = 12$

   (d) $a = 12$, $n = 15$

   (e) $a = 10$, $n = 3$

   (f) $a = 10$, $n = 7$

   (g) $a = 10$, $n = 9$

   (h) $a = 10$, $n = 11$

2. Make a table that keeps track of the following question: How many powers of a are there modulo n? Each row should be a value of n and each column a value of a from 0 to n.

Some Challenge Problems

1. Find the last digit of $1^2 + 2^2 + 3^2 + \cdots + 99^2$.

2. What are the possible values of p if:

   $\cdots$ p and $p^2 + 2$ are prime numbers.

   $\cdots$ p, $p + 10$, $p + 14$ are prime numbers.

3. There are seven natural numbers such that the sum of any six of them is divisible by 5. Prove that each of the numbers is divisible by 5.

4. Prove that $a^3 + b^3 + 4$ is never a perfect cube for any natural numbers a and b.