Modular Arithmetic

JV Practice 7/19/20

Anish Sevekari

Warmup

1. Find the units place of
   (a) 11^{2020}
   (b) 7^{2020}
   (c) 147^{2020}
2. Is $31^{57} - 43^{61}$ a multiple of 11?
3. Explain why divisibility rule of 4, that is, a number is divisible by 4 if and only if the number formed by its last 2 digits is divisible by 4.

Basic Properties and Definitions

We say that a is *congruent* to b *modulo* n, written as

$$a \equiv b \pmod{n}$$

if a and b leave the same remainder after dividing by n. This is equivalent to saying that $n \mid a - b$ (n divides $a - b$).

If $a \equiv b \pmod{n}$ and $c \equiv d \pmod{n}$, then

$$\begin{aligned} a + c &\equiv b + d \pmod{n} \\ a - c &\equiv b - d \pmod{n} \\ a \times c &\equiv b \times d \pmod{n} \end{aligned}$$

Modular Inverses

As we saw in problem 8, the equation $ax = b \pmod{n}$ might not always have a solution. One obstruction for this is the gcd, namely, if $\gcd(a, n)$ does not divide b, we cannot find a x satisfying the above equation. It turns out that this is, in fact the only obstruction. One way to solve for $ax \equiv b \pmod{n}$ is to first solve for $ax \equiv 1 \pmod{n}$, and then multiply both sides by b. Any x satisfying $ax \equiv 1 \pmod{n}$ is called the *modular inverse* of a. Here are some facts about modular inverses:

1. Modular inverse of a modulo p exists if and only if $\gcd(p, a) = 1$.
2. Modular inverses can be computed in general using Euclid's Algorithm.

3. Modular inverses can also be computed using Fermat's Little Theorem.
4. Modular inverses come in pairs except for $1, -1$.

Problems

1. Find the remainder when 555 is divided by 13 (Using Modular Arithmetic!)
2. Find the remainder when 555^2 is divided by 13.
3. Find the remainder when $7^{(7^7)}$ is divided by 10.
4. Divisibility test for 3: A natural number written as $\overline{a_n a_{n-1} \ldots a_1 a_0}$ in base 10 is divisible by 3 if and only if sum of its digits, that is $a_0 + a_1 + \cdots + a_n$ is divisible by 3.
5. Divisibility test for 11: A natural number written as $\overline{a_n a_{n-1} \ldots a_1 a_0}$ in base 10 is divisible by 11 if and only if $a_0 - a_1 + a_2 - \cdots + (-1)^n a_n$ is divisible by 11.
6. Find x such that $2x \equiv 23 \pmod{39}$.
7. Find x such that $3x \equiv 22 \pmod{37}$.
8. Is there a x such that $6x \equiv 22 \pmod{39}$.
9. Find the remainder when $1 \cdot 3 \cdot \ldots \cdot 2019 - 2 \cdot 4 \cdot \ldots \cdot 2020$ is divided by 2021.
10. A palindrome between 1000 and 10000 is chosen at random. What is the probability that it is divisible by 7?
11. In year N, the 300th day of the year is a Tuesday. In year $N+1$, the 200th day is is also a Tuesday. On what day of the week did the 100th day of year $N-1$ occur?
12. Find the number of integers n, $1 \leq n \leq 25$ such that $n^2 + 3n + 2$ is divisible by 6.
13. The positive integers N and N^2 both end in the same sequence of four digit $abcd$ when written in base 10, where digit a is non-zero. Find the three-digit number abc.
14. Given that $5x \equiv 6 \pmod{8}$, find x.
15. Find the inverse of 31 modulo 100.
16. Prove Wilson's theorem, that is for any prime p,
$$1 \cdot 2 \cdot \ldots \cdot (p-1) \equiv -1 \pmod{p}$$
17. Prove Fermat's little theorem, that is, for any a such that $\gcd(p, a) = 0$, then
$$a^{p-1} \equiv 1 \pmod{p}$$