1 Modular Arithmetic

1.1 Introduction

Even though the name sounds fancy, modular arithmetic is simply a linear equation, or a set of them. For example, take

$$x \equiv y \pmod{z}$$

. This equation gives you that the remainder when x is divided by z is y. In other words, $x = za + y$ where a is an integer. For example, $34 \equiv 4 \pmod{10}$ Take a more specific example:

$$a \equiv 1 \pmod{8}$$

. Since we are given that the remainder when a is divided by 8 is 1, we have the linear equation $a = 1 + 8x$. Now, it is clear that we can extend the equation for $-a$ as well. taking x to be -1, we have that $-1 \equiv 7 \pmod{8}$. More generally, given $x \equiv y \pmod{z}$, we see that $(x - z) \equiv y \pmod{z}$ even if $x < z$, which give $x - z$ to be negative.

1.2 Properties

There are several properties that are needed when deeling with mods. Given $x \equiv y \pmod{z}$ and $a \equiv b \pmod{c}$.

1. Addition: If $z = c$, $x + a \equiv y + b \pmod{z}$. For example, $4 \equiv 1 \pmod{3}$ and $8 \equiv 2 \pmod{3}$. $3 = 3$, so $12 \equiv 3 \pmod{3}$.
2. Subtraction: If $z = c$, $x - a \equiv y - b \pmod{z}$. For example, $4 \equiv 1 \pmod{3}$ and $2 \equiv 2 \pmod{3}$. $3 = 3$, so $2 \equiv -1 \pmod{3}$.
3. Multiplication: If $z = c$, $ax \equiv by \pmod{z}$.
4. Exponentiation: $a^e \equiv b^e \pmod{m}$ where e is a positive integer.
5. Division: $\frac{a}{e} \equiv \frac{b}{e} \pmod{\frac{m}{\gcd(m,e)}}$, where e is a positive integer that divides a and b.

1.3 Chinese Remainder Theorem and Gauss's Method

The Chinese Remainder Theorem (CRT) states that if m is relatively prime to n and you have a system of congruences $\pmod{m}$ and $\pmod{n}$, there exists a unique remainder $\pmod{mn}$. This unique remainder can be calculated by Gauss's algorithm. Suppose you wish to find the least number x which leaves a remainder of:

y_1 when divided by d_1
y_2 when divided by d_2
$\vdots$ $\vdots$
y_n when divided by d_n

such that d_1 , d_2 , ... d_n are all relatively prime. Let $M = d_1 d_2 \cdots d_n$, and $b_i = \frac{M}{d_i}$. Now if the numbers a_i satisfy:

$a_i b_i - 1 \equiv 0 \pmod{d_i}$

for every $1 \le i \le n$, then a solution for x is:

$x = \sum\limits_{i=1}^{n} a_i b_i y_i \pmod{M}$

2 Exercises

In these exercises, we will attempt to use properties of number theory to get a well-known result called Euler's (Totient) Theorem.
Example 1: We will start by proving a smaller theorem that $a^p \equiv a \pmod{p}$ for all integers $a \neq p$ and all priimes p by induction. Prove the base case of this argument if we are induction on a.

Example 2: What does the binomial theorem tell us about $(a+1)^p \pmod p$? Use this result to complete the proof by induction. $a^p \equiv a \pmod p$

Solution: Base case: a = 1 $1^p \equiv 1 \pmod p$ The base case is clearly true.
Suppose $p|a^{p-a}$ (i.e., p divides $a^p - a$). Then examine $(a+1)^p - (a+1)$. From the binomial theorem,$(a+1)^p = a^p + \binom{p}{1}a^{p-1} + \binom{p}{2}a^{p-2} + ... + \binom{p}{p-1}a + 1$
This means: $(a+1)^p - a^p - 1 = \binom{p}{1}a^{p-1} + \binom{p}{2}a^{p-2} + ... + \binom{p}{p-1}a$.
But p divides the right side, so it also divides the left side. Combining with the induction hypothesis gives that p divides the sum $[(a+1)^p - a^p - 1] + (a^p - a) = (a+1)^p - (a+1)$
Example 3: Now we move on to Euler's Theorem which states that $a^\phi(n) \equiv 1(modn)$. We define the phi function as $\phi(n)$ is the number of non-negative integers less than n that are relatively prime to n.Prove that $\phi(mn) = \phi(n)\phi(m)$.

Example 4: From this, prove that $\phi(pa) = p\phi(a)$ if $p \mid a$ and $\phi(pa) = (p-1)\phi(a)$ if $p \nmid a$.

Example 5: Prove that $\phi(n) = \prod_{p_k|n} n(1 - \frac{1}{p_k})$. (This means that $\phi(n)$ equals the product of $n(1 - \frac{1}{p_k})$ for every single p_k.)

Example 6: Finally, prove that $a^\phi(n) \equiv 1(modn)$ if a and n are relativey prime using FLT and the definition of ϕ.

3 FLT and Euler's theorem

Both Fermat's Little Theorem (FLT) and Euler's Theorem are fundamental in the number theory branch of math. FLT is related to Euler's theorem because it is possible, in fact, to use Euler's theorem in order to prove FLT. NOTE: Do not confuse Fermat's Little Theorem with Fermat's Last theorem even though both of them can be abbreviated to FLT.

4 Problems

Problem 1: What is $9^{2020} \pmod{10}$

Problem 2: Given $x \equiv 3 \pmod 6$, $x \equiv 4 \pmod 7$, and $x \equiv 8 \pmod{11}$, find all possible x.

Solution: $x \equiv -3 \pmod 6$, $x \equiv -3 \pmod 7$, and $x \equiv -3 \pmod{11}$. Since $6, 7$, and 11 are relatively prime, the answer is $x \equiv -3 \pmod{6 \cdot 7 \cdot 11}$.

Problem 3: Find $3^{31} \pmod 7, 29^{25} \pmod{11}$, and $128^{129} \pmod{17}$

Problem 4: $x = \equiv 2 \pmod 3$, $x \equiv 3 \pmod 5$, $x \equiv 2 \pmod 7$. Find all x.

Problem 5: Find the last two digits of $3^{2001} \pmod{1000}$.

Problem 6: Find the last two digits of 2^{2001}?

Solution: Use Euler's theorem. Since we can't directly calculate mod 100 since 2 isn't relative prime to 100, do mod 25. $\phi(25) = 20$. Thus, $2^{20} \equiv 1 \pmod{25}$. We then know that $2^{2001} \equiv 2 \cdot (2^{20})^{50} \equiv 2 (\text{mod } 25)$. It is trivial that $2^{2001} \equiv 0 \pmod 4$. Thus, we can use the Chinese remainder theorem and Gauss's Algorithm to combine mod 100. We want to find $c_1N_1d_1 + c_2N_2d_2$. Firstly, note that $c_2 = 0$ so the second part of the sum is 0. Then find N_1 which is $\frac{4*25}{25} = 4$. Finally, $d_1 = 4^{-1} \pmod{24}$. By using modular inverses, we need to find x such that $4x \equiv 1 \pmod{25}$. Notice that $4 \cdot 6 = -1 \pmod{25}$. Thus, $4 \cdot (-6) \equiv 1 \pmod{25}$ and $x = -6$. Thus, the sum is $2 \cdot 4 \cdot -6 = -48$. $-48 \equiv \boxed{52} \pmod{100}$.

Problem 7: Let $k = 2008^2 + 2^{2008}$. What is the units digit of $k^2 + 2^k$? (Source: AMC 12)

Solution: $k \equiv 2008^2 + 2^{2008} \equiv 8^2 + 2^4 \equiv 4 + 6 \equiv 0 \pmod{10}$.

So, $k^2 \equiv 0 \pmod{10}$. Since $k = 2008^2 + 2^{2008}$ is a multiple of four and the units digit of powers of two repeat in cycles of four, $2^k \equiv 2^4 \equiv 6 \pmod{10}$.

Therefore, $k^2 + 2^k \equiv 0 + 6 \equiv 6 \pmod{10}$. So the units digit is $6 \Rightarrow D$.

Problem 8: One of Euler's conjectures was disproved in the 1960s by three American mathematicians when they showed there was a positive integer such that $133^5 + 110^5 + 84^5 + 27^5 = n^5$. Find the value of n (Source: AIME).

Solution: Note that n is even, since the LHS consists of two odd and two even numbers. By Fermat's Little Theorem, we know n^5 is congruent to n modulo 5. Hence,

$3 + 0 + 4 + 7 \equiv n \pmod 5$ $4 \equiv n \pmod 5$ Continuing, we examine the equation modulo 3,

$1 - 1 + 0 + 0 \equiv n \pmod 3$ $0 \equiv n \pmod 3$ Thus, n is divisible by three and leaves a remainder of four when divided by 5. It's obvious that $n > 133$, so the only possibilities are $n = 144$ or $n \geq 174$. It quickly becomes apparent that 174 is much too large, so n must be $\boxed{144}$.

Problem 9: Show that if p is a prime number, and k is an integer $2 \leq k \leq p$, then the sum of the products of each k-element subset of $\{1, 2, \ldots, p\}$ is divisible by p.

Problem 10: The number obtained from the last two nonzero digits of 90! is equal to n. What is n? (Source: AMC 10)

Solution: We will use the fact that for any integer n,

$$\begin{aligned}(5n+1)(5n+2)(5n+3)(5n+4) &= [(5n+4)(5n+1)][(5n+2)(5n+3)]\\ &= (25n^2+25n+4)(25n^2+25n+6) \equiv 4 \cdot 6\\ &= 24 \pmod{25} \equiv -1 \pmod{25}.\end{aligned}$$

First, we find that the number of factors of 10 in 90! is equal to $\left\lfloor \frac{90}{5} \right\rfloor + \left\lfloor \frac{90}{25} \right\rfloor = 18 + 3 = 21$. Let $N = \frac{90!}{10^{21}}$. The n we want is therefore the last two digits of N, or $N \pmod{100}$. Since there is clearly an excess of factors of 2, we know that $N \equiv 0 \pmod 4$, so it remains to find $N \pmod{25}$.

We can write N as $\frac{M}{2^{21}}$ where

$$M = 1 \cdot 2 \cdot 3 \cdot 4 \cdot 1 \cdot 6 \cdot 7 \cdot 8 \cdot 9 \cdot 2 \cdots 89 \cdot 18 = \frac{90!}{5^{21}},$$

where every number in the form $(5^a) * n$ is replaced by n.

The number M can be grouped as follows:

$$\begin{aligned}M =&(1 \cdot 2 \cdot 3 \cdot 4)(6 \cdot 7 \cdot 8 \cdot 9)\cdots(86 \cdot 87 \cdot 88 \cdot 89)\\ &\cdot (1 \cdot 2 \cdot 3 \cdot 4)(6 \cdot 7 \cdot 8 \cdot 9)\cdots(16 \cdot 17 \cdot 18)\\ &\cdot (1 \cdot 2 \cdot 3).\end{aligned}$$

Hence, we can reduce M to

$$\begin{aligned}M &\equiv (-1)^{18} \cdot (-1)^3 (16 \cdot 17 \cdot 18) \cdot (1 \cdot 2 \cdot 3)\\ &= 1 \cdot -21 \cdot 6\\ &= -1 \pmod{25} = 24 \pmod{25}.\end{aligned}$$

Using the fact that $2^{10} = 1024 \equiv -1 \pmod{25}$,we can deduce that $2^{21} \equiv 2 \pmod{25}$. Therefore $N = \frac{M}{2^{21}} \equiv \frac{24}{2} \pmod{25} = 12 \pmod{25}$.

Finally, combining with the fact that $N \equiv 0 \pmod 4$ yields $n = \boxed{\textbf{(A) } 12}$.