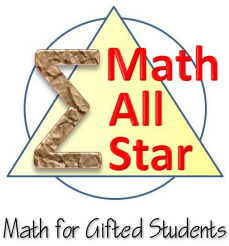
Number Theory - MOD

Math All Star Practice by Subject Series



use your mobile device to scan this QR code for more resources including books, practice problems, online courses, and blog.

This book was produced using the LaTeX system.

How to get the most out of practice

The most important tip is to learn before practice. This approach is what students do in schools. It also applies to competition math. Systematic learning will help students develop the following skills, and get the most out of practice afterwards.

1. Being able to recognize which subject a given problem belongs to.
2. Knowing relevant solving techniques for such type of problems.
3. Being able to choose the most appropriate solution for this particular problem.

There are many tutorial materials available on the website, including books, videos, articles, and so on. The address is `https://www.mathallstar.org`.

Meanwhile, it is important to read and understand reference solution instead of just checking the answer. One objective of practice is for students to check whether they understand and master all the necessary solving techniques or not. However, merely obtaining the correct answer does not necessarily mean the most suitable technique is used. Therefore, it is beneficial to understand the solution in addition to obtaining the correct answer.

Contents

CONTENTS

Part I

Review

Copyrighted material, issued at 5/11/2026 11:00:20 PM

Chapter 1

MOD Basic

1.1 MOD Basic

1.1.1 Definition

Let a, b, and m be three integers where $m > 0$. If the difference of a and b is a multiple of m, we say a *is congruent to* b *modulo* m and write this relationship as

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

For example,

$$30 \equiv 16 \equiv 2 \equiv -5 \pmod{7}$$

It is important to note that a and b can be negative. In fact, using negative number is a frequently used technique to simplify computation.

1.1.2 Residue Class and Residue System

A *residue class* is a set of integers which are equivalent congruent to modulo m. There are exactly m different residue classes for modulo m.

A *complete residue system* is a set of integers which contains one and exactly one element from each of all the residue classes. Obviously, for modulo m, a complete residue system contains exactly m element. There are an infinite number of complete residue systems modulo m. The following one is called the least non-negative residue system:

$$\{0, 1, \cdots, m-1\}$$

1.2 MOD Operations

1.2.1 Basic Properties

MOD operations follow the same basic rules as regular algorithmic except the division operation.

Theorem 1.2.1 MOD Addition and Subtraction

Let $a \equiv b \pmod{m}$ and $c \equiv d \pmod{m}$, then

$$a \pm c \equiv b \pm d \pmod{m}$$

Theorem 1.2.2 MOD Multiplication

Let $a \equiv b \pmod{m}$ and $c \equiv d \pmod{m}$, then

$$a \times c \equiv b \times d \pmod{m}$$

Theorem 1.2.3 MOD Multiplication with Constant

Let $a \equiv b \pmod{m}$ and k be an integer, then

$$k \times a \equiv k \times b \pmod{m}$$

Theorem 1.2.4 MOD Exponentiation

Let $a \equiv b \pmod{m}$ and k be a positive integer, then

$$a^k \equiv b^k \pmod{m}$$

However, it is important to note the division is an exception here. In order to make the division hold, the relationship between the divisor k and the modulo m must be taken into consideration.

Theorem 1.2.5 MOD Division

Let $a \equiv b \pmod{m}$ and k be an integer, then

$$\frac{a}{k} \equiv \frac{b}{k} \pmod{\frac{m}{\gcd(m,k)}}$$

where $\gcd(m,k)$ is the greatest common divisor of m and k.

For example, given $30 \equiv 6 \pmod 8$, simply dividing both sides by 2 will invalidate the relationship: $15 \not\equiv 3 \pmod 8$. Instead, it is necessary to divide the modulo by 2 which is the greatest common divisor of 8 and 2: $15 \equiv 3 \pmod 4$.

1.2.2 Modular Multiplicative Inverse

Given an integer a, its modular multiplicative inverse modulo m, is also an integer which is written as a^{-1} or $\frac{1}{a}$ and satisfies $aa^{-1} \equiv 1 \pmod m$.

Theorem 1.2.6 Existence of Modular Multiplicative Inverse

The modulo multiplicative inverse of a modulo m exists if and only if a and m are co-prime.

If a^{-1} exists, it must be one of $1, 2, \cdots, (m-1)$. It can also be shown that the modular multiplicative inverse is unique within this range. Therefore, for a small integer m, the easiest way to find a^{-1} is just to enumerate through all the values within this range. For example, $\frac{1}{3} \equiv 5 \pmod 7$ because $3 \times 5 \equiv 1 \pmod 7$. No other integers within $[1, 6]$ satisfies this condition. For a big number, Euler theorem may be useful to help find its modular multiplicative inverse.

1.3 Evaluating MOD Expression

Most MOD expressions to be evaluated are in exponential forms. Therefore, most techniques involve exponentiation manipulation.

1.3.1 The Negative One Method

Converting the base to (-1) is a useful technique. Let's review an example.

Example 1.3.1

Find all positive integer n such that $2^n + 1$ is divisible by 3.

Solution

The answer is the set of all odd integers because

$$2^n + 1 \equiv (-1)^n + 1 \equiv 0 \pmod 3$$

holds if and only if n is odd.

Done.

Sometimes, it may require a few intermediate steps to obtain (-1). For example,

$$3^{2018} \equiv (3^2)^{1009} \equiv 9^{1009} \equiv (-1)^{1009} \equiv -1 \equiv 9 \pmod{10}$$

1.3.2 Advanced Methods

Other computation techniques will involve Euler's theorem, Fermat little theorem, and so on. These will be discussed later.

1.4 Sum of Digits (The MOD 9 Technique)

When a problem involves the sum of digits, the following theorem should be considered.

Theorem 1.4.1 Sum of Digits

Let n be a positive integer and $S(n)$ be the sum of its digits, then

$$n \equiv S(n) \pmod{9}$$

The 18^{th} problem in 2017 AMC12A offers a typical example.

Example 1.4.1

Let $S(n)$ equal the sum of the digits of positive integer n. For example, $S(1507) = 13$. For a particular positive integer n, $S(n) = 1274$. Which of the following could be the value of $S(n+1)$?

(A) 1 (B) 3 (C) 12 (D) 1329 (E)1265

Solution

By the MOD 9 technique, we have $n \equiv S(n) \equiv 1274 \equiv 5 \pmod{9}$. Therefore $n+1 \equiv 6 \pmod{9}$. Among the given choices, only 1329 satisfies this constraint.

Done.

Another type of problems which can be solved with this technique is to find a missing digit while all the others present. An example is shown below:

Example 1.4.2

The number 2^{29} is a nine-digit number whose digits are all distinct. Which digit of 0 to 9 does not appear?

Solutions to this example is provided in the solution chapter.

1.5 Finding End Digit(s)

1.5.1 Finding the Units Digit

Finding the units digit of m^n is usually easy. The result obviously only depends on the units digit of m. An elementary method to find the last digit is just to observe the repeating pattern. For example, the last digits of 7^n where $n = 1, 2, \cdots$ are

$$7, 9, 3, 1, 7, 9, 3, 1, \cdots$$

1.5.2 Finding the Last k Digits

Finding the last k digits of m^n is equivalent to evaluating $m^n \pmod{10^k}$. In addition to the usual evaluation techniques, binomial expansion is a powerful method to find the last k digits when m ends with one[1].

Let's consider an example which is based on a 2011 AMC10 problem.

Example 1.5.1

What are the last 3 digits of 2011^{2011}?

Solution

Firstly, $2011^{2011} \equiv 11^{2011} \pmod{1000}$. Next, let's rewrite 11 as $(10+1)$ and expand the expression:

$$(10+1)^{2011} = \cdots + C_{2011}^{3} \times 10^3 + C_{2011}^{2} \times 10^2 + C_{2011}^{1} \times 10 + 1$$

It is clear that all the terms except that last three will be multiples of 1000 whose last 3 digits are always 000. Therefore, it is sufficient to calulate the last three digits of the sum of the last three terms in order to find the answer.

$$\begin{aligned} & C_{2011}^{2} \times 10^2 + C_{2011}^{1} \times 10 + 1 \\ =& \frac{2011 \times 2010}{2} \times 100 + 2011 \times 10 + 1 \end{aligned}$$

[1]For those readers who are not familiar with binomial expansion, this section can be safely ignored

$$\begin{aligned}
&\equiv 2011 \times 2010 \times 50 + 11 \times 10 + 1 \\
&\equiv 11 \times 10 \times 50 + 110 + 1 \\
&\equiv 611 \pmod{1000}
\end{aligned}$$

Hence, the last three digits are $\boxed{611}$.

Done.

1.5.3 A Quick Way to Find the Tens Digit of m^n

In addition to the general method of finding the last k digits of m^n, there exists a quick way to find its last two digits. Because the units digit is alway easy to determine, the key is to find out the tens digit.

m ends with 0 or 5

When m ends with 0, then the tens digit of m^n is always 0 when $n \geq 2$. When m ends with 5, it can be shown that m^n can only end with 25 or 75. These two cases are trivial. No special trick is required.

m ends with 1

This can be solved using the following technique.

Theorem 1.5.1 Finding tens digit of m^n when m ends with 1

Taking the tens digit of m and multiplying it with the units digit of n, their product's units digit is the tens digit of m^n.

Let's consider the following example.

Example 1.5.2

What is the tens digit of 321^{123}?

Solution

The tens digit of 321 is 2. The units digit of 123 is 3. Thus, the tens digit of 321^{123} is $2 \times 3 = \boxed{6}$.

Done.

In another word, the last two digits of 321^{123} is 61, or $321^{123} \equiv 61 \pmod{100}$.

Theorem 1.5.1 is the steppingstone of finding the tens digit when m ends with

other digits. This theorem can be proved using binomial expansion which is described in the previous section.

m ends with $3, 7$, or 9

These three cases can be transformed to the previous case where m ends with 1 by noting that 3^4, 7^4, and 9^2 all end with 1. Here is an example.

Example 1.5.3

Find the last two digits of 123^{321}.

Solution

Firstly, we note that

$$123^{321} \equiv 23^{321} = (23^4)^{80} \times 23^1 \pmod{100}$$

Because 23^4 ends with 1, the units digit of $(23^4)^{80}$ must be 1. By *Theorem 1.5.1*, the tens digit of $(23^4)^{80}$ must be 0 because the units digit of the exponent is 0. In another word, $(23^4)^{80} \equiv 01 \pmod{100}$. Setting this to the above relation leads to

$$123^{321} \equiv 1 \times 23 = \boxed{23} \pmod{100}$$

Done.

It is important to note that 3, 7, and 9 all relate to certain powers of 3:

$$3^1 = 3, 3^2 = 9, 3^3 = 27$$

Therefore, the technique discussed in this section can help to determine the tens digit of a number in the form of 3^k.

A useful fun fact to remember is that $7^4 = 2401$ which ends with 01. Hence,

Let n be a multiple of 4, then the last two digits of 7^n must be 01.

Other Cases

Tackling the remaining cases requires a bit maneuver. The essential technique is to first factorize m and then process each part separately. A prime factor can only be 2 or ends with 1, 3, 5, 7, or 9. We have already discussed those cases when m ends with an odd digit. Therefore, the only scenario left to tackle is 2^k where k is a positive integer.

The technique to find the tens digit of 2^k depends on the following facts:

- $2^{10} = 1024$, ends with 24

- $24^2 = 576$, ends with 76
- Any power of 76 always ends with 76 itself

This means that if k is sufficiently large, 2^k can be rewritten as a product of a smaller power of 2 and 76^p, modulo 100.

Let's review an example.

Example 1.5.4

Determine the last two digits of 312^{123}.

Solution

First, let's factorize the expression to:

$$312^{123} \equiv 12^{123} = (2^2 \times 3)^{123} = 2^{246} \times 3^{123} \pmod{100}$$

and then tackle the two terms separately:

$$2^{246} = (2^{10})^{24} \times 2^6 = (1024)^{24} \times 64 \equiv 24^{24} \times 64 \equiv (24^2)^{12} \times 64 \equiv 76 \times 64 \pmod{100}$$
$$3^{123} = (3^4)^{30} \times 3^3 = 81^{30} \times 27 \equiv 01 \times 27 = 27 \pmod{100}$$

Therefore, the answer we are looking is

$$64 \times 76 \times 27 \equiv \boxed{28} \pmod{100}$$

Done.

1.5.4 Useful Facts

- 25 and 76 are the only two-digit integers whose k^{th} powers always end with themselves where k is a positive integer.
- 376 and 625 are the only three-digit integers whose k^{th} powers always end with themselves where k is a positive integer.

Chapter 2

Import Theorems

2.1 Fermat Little Theorem

This theorem is stated as follows:

Theorem 2.1.1 Fermat Little Theorem

Let p be a prime and a be an integer, then

$$a^p \equiv a \pmod{p} \tag{2.1}$$

A useful equivalent conclusion to *(2.1)* is:

Theorem 2.1.2 Fermat Little Theorem Equivalence

Let p be a prime and a be an integer not divisible by p, then

$$a^{p-1} \equiv 1 \pmod{p} \tag{2.2}$$

2.2 Euler's Theorem

Fermat Little Theorem can be generalized into Euler's Theorem.

Theorem 2.2.1 Euler's Theorem

Let a and n be two co-prime integers, then

$$a^{\varphi(n)} \equiv 1 \pmod{n} \tag{2.3}$$

Here, $\varphi(n)$ is Euler's totient function.

Definition 2.2.1 Euler's Totient Function

Let positive integer n's prime factorization is $n = p_1^{\alpha_1} p_2^{\alpha_2} \cdots p_k^{\alpha_k}$, then

$$\varphi(n) = n\left(1 - \frac{1}{p_1}\right)\left(1 - \frac{1}{p_2}\right)\cdots\left(1 - \frac{1}{p_k}\right)$$

When n is a prime, then $\varphi(n) = n - 1$ and *Equation 2.3* becomes *(2.2)*.

The converse of Euler's theorem is also true.

Theorem 2.2.2 Converse to Euler's Theorem

If $a^{\varphi(n)} \equiv 1 \pmod{n}$ holds where a and n be two positive integers, then a and n are co-prime.

Euler's theorem can be a powerful tool to compute $a^b \pmod{n}$ when a and n are co-prime. To tackle this, it is sufficient to first compute $c \equiv b \pmod{\varphi(n)}$. Then

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

2.3 Chinese Remainder Theorem (CRT)

CRT relates to solve a system of congruent relations.

Theorem 2.3.1 Chinese Remainder Theorem

Let integers $m_1, m_2, \cdots, m_k$ be pair-wise co-prime and $a_1, a_2, \cdots, a_k$ be any integers, then the system

$$\begin{cases} x & \equiv a_1 \pmod{m_1} \\ x & \equiv a_2 \pmod{m_2} \\ & \cdots \\ x & \equiv a_k \pmod{m_k} \end{cases}$$

has a unique solution

$$x \equiv \sum_{i=1}^{k} a_i b_i b_i' \pmod{M}$$

where $M = m_1 m_2 \cdots m_k$, $b_i = M/m_i$, and $b_i' = b_i^{-1} \pmod{m_i}$.

Please note that some special systems can be solved in an easier way. Two notable cases are $a_1 = a_2 = \cdots = a_k = n$ and $a_i = m_i - n$ where n is a constant.

2.4 Wilson's Theorem

When a MOD expression involves factorial, the Wilson' theorem may be applicable.

Theorem 2.4.1 Wilson's Theorem

An positive integer n is a prime if and only if

$$(n-1)! \equiv -1 \pmod{n}$$

Part II

Practice

Copyrighted material, issued at 5/11/2026 11:00:20 PM

Practice 1

What is the units digit of 13^{2012}?

(ref: 1186 - AMC8)

Practice 2

What is the tens digit of $2015^{2016} - 2017$?

(ref: 2913 - AMC10)

Practice 3

Let $a > b > c$ be three positive integers. If their remainders are 2, 7, and 9 respectively when being divided by 11. Find the remainder when $(a+b+c)(a-b)(b-c)$ is divided by 11.

(ref: 122)

Practice 4

What is the last digit of 9^{2015}?

(ref: 272)

Practice 5

What are the last two digits of 8^{88}?

(ref: 273)

Practice 6

Find the remainder when $3^{2015} + 4^{2015}$ is divided by 5?

(ref: 274)

Practice 7

Find the remainder when $9 \times 99 \times 999 \times \cdots \times \underbrace{99\cdots9}_{999}$ is divided by 1000.

(ref: 280 - AIME)

Practice 8

The number 2^{29} is a nine-digit number whose digits are all distinct. Which digit of 0 to 9 does not appear?

(ref: 311)

Practice 9

A box contains gold coins. If the coins are equally divided among six people, four coins are left over. If the coins are equally divided among five people, three coins are left over. If the box holds the smallest number of coins that meets these two conditions, how many coins are left when equally divided among seven people?

(ref: 991 - AMC8)

Practice 10

Let four positive integers a, b, c, and d satisfy $a + b + c + d = 2015$. Prove $a^3 + b^3 + c^3 + d^3$ cannot be an even number.

(ref: 1120)

Practice 11

What is the tens digit of 7^{2011}?

(ref: 1171 - AMC8)

Practice 12

What are the sign and units digit of the product of all the odd negative integers strictly greater than -2015?

(ref: 1259 - AMC10)

Practice 13

Three runners start running simultaneously from the same point on a 500-meter circular track. They each run clockwise around the course maintaining constant speeds of 4.4, 4.8, and 5.0 meters per second. The runners stop once they are all together again somewhere on the circular course. How many seconds do the runners run?

(ref: 1395 - AMC10)

Practice 14

When Ringo places his marbles into bags with 6 marbles per bag, he has 4 marbles left over. When Paul does the same with his marbles, he has 3 marbles left over. Ringo and Paul pool their marbles and place them into as many bags as possible, with 6 marbles per bag. How many marbles will be left over?

(ref: 1408 - AMC10)

Practice 15

What is the tens digit in the sum $7! + 8! + 9! + ... + 2006!$

(ref: 1721 - AMC10)

Practice 16

What is the units digit of the product $7^{23} \times 8^{105} \times 3^{18}$?

(ref: 1819 - MathCounts)

Practice 17

What is the smallest positive integer greater than 5 which leaves a remainder of 5 when divided by each of 6, 7, 8, and 9?

(ref: 2645 - BCML)

Practice 18

Determine the units digit of the sum $0! + 1! + 2! + \cdots + n! + \cdots + 20!$?

(ref: 2654 - BCML)

Practice 19

What is the last digit of 7^{222}?

(ref: 2741)

Practice 20

Find the largest positive integer n such that $3^{1024} - 1$ is divisible by 2^n.

(ref: 2811)

Practice 21

If 738 consecutive integers are added together, where the 178^{th} number in the sequence is $4,256,815$, what is the remainder when this sum is divided by 6?

(ref: 3070 - MathCounts)

Practice 22

Prove that $7 \mid 8^n - 1$ for $n \geq 1$.

(ref: 3191)

Practice 23

Show that $15 \mid 4^{2n} - 1$ for $n \geq 1$.

(ref: 3192)

Practice 24

Prove that $5 \mid 4^{2n} - 1$ for $n \geq 1$.

(ref: 3194)

Practice 25

An integer N is selected at random in the range $1 \leq N \leq 2020$. What is the probability that the remainder when N^{16} is divided by 5 is 1?

(ref: 3743 - AMC10)

Practice 26

Let n be any positive integer, show that

$$(5n+1)(5n+2)(5n+3)(5n+4) \equiv -1 \pmod{25}$$

(ref: 4160)

Practice 27

Let m be the least positive integer divisible by 17 whose digits sum is 17. Find m.

(ref: 70 - AIME)

Practice 28

The positive integers N and N^2 both end in the same sequence of four digits $abcd$ when written in base 10, where digit a is not zero. Find the three-digit number abc.

(ref: 90 - AIME)

Practice 29

Let integer a, b, and c satisfy $a+b+c=0$, prove $|a^{1999}+b^{1999}+c^{1999}|$ is a composite number.

(ref: 310)

Practice 30

What are the last two digits in the sum of the factorials of the first 100 positive integers?

(ref: 1117)

Practice 31

Let $k = 2008^2 + 2^{2008}$. What is the units digit of $k^2 + 2^k$?

(ref: 1608 - AMC10)

Practice 32

Farmer Hank has fewer than 100 pigs on his farm. If he groups the pigs five to a pen, there are always three pigs left over. If he groups the pigs seven to a pen, there is always one pig left over. However, if he groups the pigs three to a pen, there are no pigs left over. What is the greatest number of pigs that Farmer Hank could have on his farm?

(ref: 1869 - MathCounts)

Practice 33

Let $f(n)$ denote the sum of the digits of n. Find $f(f(f(4444^{4444})))$.

(ref: 2216 - IMO)

Practice 34

What is the last digit of $17^{17^{17^{17}}}$?

(ref: 2540 - PUMaC)

Practice 35

Compute $50^{250} \pmod{83}$.

(ref: 2740)

Practice 36

Find the smallest positive integer n so that $107n$ has the same last two digits as n.

(ref: 2805 - Harvard-MIT)

Practice 37

Find 8 prime numbers, not necessarily distinct such that the sum of the squares of these numbers is 992 less than 4 times of the product of these numbers.

(ref: 2822)

Practice 38

Let $P(x)$ be a polynomial with integer coefficients satisfying both $P(0)$ and $P(1)$ are odd. Show that $P(x)$ has no integer zeros.

(ref: 2841)

Practice 39

Show that if n is an integer greater than 1, then $(2^n - 1)$ is not divisible by n.

(ref: 3624 - Putnam)

Practice 40

Does there exist a polynomial $P(x)$ such that $P(1) = 2015$ and $P(2015) = 2016$?

(ref: 3971)

Practice 41

Find all prime number p such that both $4p^2 + 1$ and $6p^2 + 1$ are prime numbers.

(ref: 174 - Poland)

Practice 42

Ms. Math's kindergarten class has 16 registered students. The classroom has a very large number, N, of play blocks which satisfies the conditions:

- If 16, 15, or 14 students are present in the class, then in each case all the blocks can be distributed in equal numbers to each student, and
- There are three integers $0 < x < y < z < 14$ such that when x, y, or z students are present and the blocks are distributed in equal numbers to each student, there are exactly three blocks left over.

Find the sum of the distinct prime divisors of the least possible value of N satisfying the above conditions.

(ref: 190 - AIME)

Practice 43

Let $\mathcal{S}$ be the set of all perfect squares whose rightmost three digits in base 10 are 256. Let $\mathcal{T}$ be the set of all numbers of the form $\frac{x-256}{1000}$, where x is in $\mathcal{S}$. In other words, $\mathcal{T}$ is the set of numbers that result when the last three digits of each number in $\mathcal{S}$ are truncated. Find the remainder when the tenth smallest element of $\mathcal{T}$ is divided by 1000.

(ref: 219 - AIME)

Practice 44

The number 2017 is prime. Let $S = \sum_{k=0}^{62} \binom{2014}{k}$. What is the remainder when S is divided by 2017?

(ref: 474 - AMC12)

Practice 45

Seven students count from 1 to 1000 as follows:

- Alice says all the numbers, except she skips the middle number in each consecutive group of three numbers. That is, Alice says 1, 3, 4, 6, 7, 9, . . ., 997, 999, 1000.
- Barbara says all of the numbers that Alice doesn't say, except she also skips the middle number in each consecutive group of three numbers.
- Candice says all of the numbers that neither Alice nor Barbara says, except she also skips the middle number in each consecutive group of three numbers.
- Debbie, Eliza, and Fatima say all of the numbers that none of the students with the first names beginning before theirs in the alphabet say, except each also skips the middle number in each of her consecutive groups of three numbers.
- Finally, George says the only number that no one else says.

What number does George say?

(ref: 1457 - AMC10)

Practice 46

The number obtained from the last two non-zero digits of 90! is equal to n. What is n?

(ref: 1508 - AMC10)

Practice 47

Prove that if p and p^2+8 are prime, then p^3+8p+2 is prime.

(ref: 2217)

Practice 48

What is the smallest positive integer n such that $20 \equiv n^{15} \pmod{29}$?

(ref: 2614 - PUMaC)

Practice 49

Given that there are 24 primes between 3 and 100, inclusive, what is the number of ordered pairs (p, a) with p prime, $3 \leq p < 100$, and $1 \leq a < p$ such that the sum $a + a^2 + a^3 + \cdots + a^{(p-2)!}$ is not divisible by p?

(ref: 2615 - PUMaC)

Practice 50

If for any integer $k \neq 27$ and $\left(a - k^{2015}\right)$ is divisible by $(27-k)$, what is the last two digits of a?

(ref: 2621)

Practice 51

Find the least non-negative residue of $70! \pmod{5183}$.

(ref: 2739)

Practice 52

Let x be an integer and p is a prime divisor of $(x^6+x^5+\cdots+1)$. Show that $p=7$ or $p\equiv 1 \pmod 7$.

(ref: 3795)

Practice 53

Let x be an integer and p is an odd prime divisor of x^2+1. Show that $p\equiv 1 \pmod 4$.

(ref: 3796)

Practice 54

Let p be an odd prime number. For positive integer k satisfying $1\le k\le p-1$, the number of divisors of $kp+1$ between k and p exclusive is a_k. Find the value of $a_1+a_2+\ldots+a_{p-1}$.

(ref: 3841 - Japan)

Practice 55

Let p be an odd prime divisor of number (a^2+1) where a is an integer. Show that $p\equiv 1 \pmod 4$.

(ref: 3870)

Practice 56

For positive integers n and k, let $f(n,k)$ be the remainder when n is divided by k, and for $n>1$ let $F(n)=\max\limits_{1\le k\le \frac{n}{2}} f(n,k)$. Find the remainder when $\sum\limits_{n=20}^{100} F(n)$ is divided by 1000.

(ref: 208 - AIME)

Practice 57

Let sequence $g(n)$ satisfy $g(1)=0, g(2)=1, g(n+2)=g(n+1)+g(n)+1$ where $n\ge 1$. Show that if n is a prime greater than 5, then $n \mid g(n)[g(n)+1]$.

(ref: 2699 - IMO)

Part III

Solution

Copyrighted material, issued at 5/11/2026 11:00:20 PM

Practice 1

What is the units digit of 13^{2012}?

(ref: 1186 - AMC8)

We note that the ending digit of 3^k repeats every 4 terms: 3, 9, 7, 1, 3, $\cdots$. Because 2012 is a multiple of 4, thus the ending digits of 13^{2012} is the same as 3^4 which is $\boxed{1}$.

Alternatively, it is also possible to solve this problem using the (-1) technique.

$$13^{2012} \equiv 3^{2012} \equiv 9^{1006} \equiv (-1)^{1006} \equiv \boxed{1} \pmod{10}$$

Practice 2

What is the tens digit of $2015^{2016} - 2017$?

(ref: 2913 - AMC10)

Firstly, $2015^{2016} \equiv 15^{2016} \pmod{100}$.

It is easy to verify that $(k > 1)$, $15^k \equiv 25 \pmod{100}$ when k is even, and $15^k \equiv 75 \pmod{100}$ when k is odd.

Therefore 15^{2016} will end with 25 which leads to the final answer as $\boxed{0}$.

Practice 3

Let $a > b > c$ be three positive integers. If their remainders are 2, 7, and 9 respectively when being divided by 11. Find the remainder when $(a+b+c)(a-b)(b-c)$ is divided by 11.

(ref: 122)

$$(a+b+c)(a-b)(b-c) \equiv (2+7+9)(2-7)(7-9) = 180 \equiv \boxed{4} \pmod{11}$$

Practice 4

What is the last digit of 9^{2015}?

(ref: 272)

$$9^{2015} \equiv (-1)^{2015} \equiv -1 \equiv \boxed{9} \pmod{10}$$

Practice 5

What are the last two digits of 8^{88}?

(ref: 273)

$$8^{88} \equiv 2^{264} \equiv \left(2^{10}\right)^{26} \times 2^4 \equiv 24^{26} \times 16 \equiv 76^{13} \times 16 \equiv 76 \times 16 \equiv \boxed{16} \pmod{100}$$

Practice 6

Find the remainder when $3^{2015} + 4^{2015}$ is divided by 5?

(ref: 274)

$$3^{2015} + 4^{2015} \equiv (3^2)^{1007} \times 3 + (-1)^{2015} \equiv (-1)^{1007} \times 3 - 1 \equiv \boxed{1} \pmod{5}$$

Practice 7

Find the remainder when $9 \times 99 \times 999 \times \cdots \times \underbrace{99\cdots9}_{999}$ is divided by 1000.

(ref: 280 - AIME)

Note that $\underbrace{99\cdots9}_{k} \equiv 999 \equiv -1 \pmod{1000}$ when $k \geq 3$. The original expression is congruent to

$$9 \times 99 \times \underbrace{(-1)(-1)\cdots(-1)}_{997} \equiv 891 \times (-1) \equiv \boxed{109} \pmod{1000}$$

Practice 8

The number 2^{29} is a nine-digit number whose digits are all distinct. Which digit of 0 to 9 does not appear?

(ref: 311)

By the MOD by 9 technique, the sum of these digits must be congruent to 2^{29} (mod 9) which is (-4) (see below). Hence, the missing digit is $\boxed{4}$.

$$2^{29} \equiv (2^3)^9 \times 2^2 \equiv (-1)^9 \times 4 \equiv -4 \pmod 9$$

Practice 9

A box contains gold coins. If the coins are equally divided among six people, four coins are left over. If the coins are equally divided among five people, three coins are left over. If the box holds the smallest number of coins that meets these two conditions, how many coins are left when equally divided among seven people?

(ref: 991 - AMC8)

We note that the remainder is always two less than the divisor when the coins are distributed among six or five people. Therefore, the number of coin must be two less than the least common multiple of 6 and 5, which is 28. It follows the answer is $\boxed{0}$.

Practice 10

Let four positive integers a, b, c, and d satisfy $a + b + c + d = 2015$. Prove $a^3 + b^3 + c^3 + d^3$ cannot be an even number.

(ref: 1120)

It is easy to show that regardless of integer n's parity, it always hold that $n^3 \equiv n$ (mod 2) because any power of n will not change odd even parity. Therefore,

$$a^3 + b^3 + c^3 + d^3 \equiv a + b + c + d \equiv 2015 \equiv 1 \pmod 2$$

Practice 11

What is the tens digit of 7^{2011}?

(ref: 1171 - AMC8)

We note that any power of 7^4 must end with 01.

$$7^{2011} = (7^4)^{502} \times 7^3 \equiv 01^{502} \times 43 \equiv 43 \pmod{100}$$

Hence the answer is $\boxed{D} = 4$.

Practice 12

What are the sign and units digit of the product of all the odd negative integers strictly greater than -2015?

(ref: 1259 - AMC10)

There are odd number of negative integers, therefore the sign is negative. Clearly, there is (-5) among them and all the other numbers are odd, hence, the units digit must be 5.

Practice 13

Three runners start running simultaneously from the same point on a 500-meter circular track. They each run clockwise around the course maintaining constant speeds of 4.4, 4.8, and 5.0 meters per second. The runners stop once they are all together again somewhere on the circular course. How many seconds do the runners run?

(ref: 1395 - AMC10)

While MOD cannot only be applied to integer, but conceptually this is equivalent to solving

$$4.4t \equiv 4.8t \equiv 5.0t \pmod{500}$$

Subtracting $4.4t$ leads to

$$0 \equiv 0.4t \equiv 0.6t \pmod{500}$$

This means that we need to find a t such that $0.4t$ and $0.6t$ are both multiples of 500. The first few ts which make $0.4t$ a multiple of 500 are 1250, 2500, $\cdots$. We find $\boxed{2500}$ is a solution.

Practice 14

When Ringo places his marbles into bags with 6 marbles per bag, he has 4 marbles left over. When Paul does the same with his marbles, he has 3 marbles left over. Ringo and Paul pool their marbles and place them into as many bags as possible, with 6 marbles per bag. How many marbles will be left over?

(ref: 1408 - AMC10)

The remainder will be $4 + 3 \equiv 7 \equiv \boxed{1} \pmod{6}$.

Practice 15

What is the tens digit in the sum $7! + 8! + 9! + ... + 2006!$

(ref: 1721 - AMC10)

When $k \geq 10$, $k!$ must be multiple of 100 whose last two digits will be 0. Therefore, the desired results is the same as the tens digit of 7!+8!+9!. We can compute $7! = 5040$, therefore

$$7! + 8! + 9! \equiv 40 + 40 \times 8 + 40 \times 8 \times 9 \equiv 40 + 20 + 80 \equiv 40 \pmod{100}$$

Practice 16

What is the units digit of the product $7^{23} \times 8^{105} \times 3^{18}$?

(ref: 1819 - MathCounts)

The last digit of 7^k repeats as 7, 9, 3, 1, 7, $\cdots$. Therefore 7^{23} ends with 3.

The last digit of 8^k repeats as 8, 4, 2, 6, 8, $\cdots$. Therefore 8^{105} ends with 8.

The last digit of 3^k repeats as 3, 9, 7, 1, 3, $\cdots$. Therefore 3^{18} ends with 9.

Hence, the units digit of $7^{23} \times 8^{105} \times 3^{18}$ is the same as the last digit of $3 \times 8 \times 9$ which is 6.

Practice 17

What is the smallest positive integer greater than 5 which leaves a remainder of 5 when divided by each of 6, 7, 8, and 9?

(ref: 2645 - BCML)

It will be the least common multiple of 6, 7, 8, and 9 plus 5, which is 509.

Practice 18

Determine the units digit of the sum $0! + 1! + 2! + \cdots + n! + \cdots + 20!$?

(ref: 2654 - BCML)

Where $n \geq 5$, $n!$ must be a multiple of 10 whose units' digit will be 0. Therefore, the original question is equivalent to finding the unit digit of

$$0! + 1! + 2! + 3! + 4! = 1 + 1 + 2 + 6 + 24 = 34$$

Therefore, the answer is $\boxed{4}$.

Practice 19

What is the last digit of 7^{222}?

(ref: 2741)

The last digit of 7^n rotates in the set of $\{7, 9, 3, 1\}$. Because $2222 \equiv 2 \pmod 4$, we find the answer is $\boxed{9}$.

Practice 20

Find the largest positive integer n such that $3^{1024} - 1$ is divisible by 2^n.

(ref: 2811)

Note that

$$3^{1024-1} = (3^{512} + 1)(3^{256} + 1)(3^{128} + 1) \cdots (3 + 1)(3 - 1)$$

All the 11 factors are even. Among them

- $(3 - 1)$ is clearly not divisible by 4.
- $(3 + 1)$ is a multiple of 4.
- We claim neither of the rest 9 terms is a multiple of 4.

The last conclusion holds because

$$3 \equiv -1 \pmod 4 \implies 3^{2k} \equiv 1 \pmod 4$$

Therefore, $n = 1 + 2 + 9 = \boxed{12}$.

Practice 21

If 738 consecutive integers are added together, where the 178^{th} number in the sequence is $4,256,815$, what is the remainder when this sum is divided by 6?

(ref: 3070 - MathCounts)

Because 736 is a multiple of 6, therefore, the remainders of the sum of these numbers divides 6 will equal

$$0 + 1 + 2 + \cdots + 5 \equiv 15 \equiv \boxed{3} \pmod 6$$

Practice 22

Prove that $7 \mid 8^n - 1$ for $n \geq 1$.

(ref: 3191)

Because $8^n - 1 \equiv 1^n - 1 \equiv 0 \pmod 7$, therefore the conclusion holds.

Practice 23

Show that $15 \mid 4^{2n} - 1$ for $n \geq 1$.

(ref: 3192)

Because $4^{2n} - 1 \equiv 16^n - 1 \equiv 1^n - 1 \equiv 0 \pmod{15}$, therefore the claim holds.

Practice 24

Prove that $5 \mid 4^{2n} - 1$ for $n \geq 1$.

(ref: 3194)

Because $4^{2n} - 1 \equiv (-1)^{2n} - 1 \equiv 0 \pmod 5$ holds for all $n \geq 1$, therefore the conclusion holds.

Practice 25

An integer N is selected at random in the range $1 \leq N \leq 2020$. What is the probability that the remainder when N^{16} is divided by 5 is 1?

(ref: 3743 - AMC10)

When $N \equiv 0 \pmod 5$, then $N^{16} \equiv 0 \pmod 5$.

When $N \equiv \pm 1 \pmod 5$, then $N^{16} \equiv 1 \pmod 5$.

When $N \equiv \pm 2 \pmod 5$, then $N^{16} \equiv 2^{16} \equiv 4^8 \equiv (-1)^8 \equiv 1 \pmod 5$.

We note that 2020 is a multiple of 5. Therefore, the answer is $4/5$.

Practice 26

Let n be any positive integer, show that

$$(5n+1)(5n+2)(5n+3)(5n+4) \equiv -1 \pmod{25}$$

(ref: 4160)

$$\begin{aligned} & (5n+1)(5n+2)(5n+3)(5n+4) \\ = \; & ((5n+1)(5n+4))((5n+2)(5n+3)) \\ = \; & (25n^2+5n+4)(25n^2+5n+6) \\ = \; & (25n^2+5n)^2 + 10 \times (25n^2+5n) + 24 \\ \equiv \; & 24 \\ \equiv \; & -1 \pmod{25} \end{aligned}$$

Practice 27

Let m be the least positive integer divisible by 17 whose digits sum is 17. Find m.

(ref: 70 - AIME)

Let $s(m)$ be the digit sum of m. It must hold that

$$m \equiv s(m) \equiv 17 \equiv -1 \pmod{9}$$

Because m is a multiple of 17, let $m = 17k$ which means

$$17k \equiv -1 \pmod{9}$$

Obviously $k = 1$ is one solution, therefore its general solution is $k = 9n + 1$. Try $n = 0, 1, 2, 3, \cdots$ finding $m = \boxed{476}$ is the first positve solution that has $s(m) = 17$.

Practice 28

The positive integers N and N^2 both end in the same sequence of four digits $abcd$ when written in base 10, where digit a is not zero. Find the three-digit number abc.

(ref: 90 - AIME)

We know there are only two three-digit number whose squares end with themselves: 625 and 376. Therefore, N must end with either 625 or 376. There are some MOD tricks we can play to narrow down the choices, but it is not too hard to try all the possible thousands digit and find $N = 9376$. Therefore the answer is $\boxed{937}$.

Practice 29

Let integer a, b, and c satisfy $a+b+c=0$, prove $|a^{1999}+b^{1999}+c^{1999}|$ is a composite number.

(ref: 310)

Let $d = a^{1999} + b^{1999} + c^{1999}$, we are going to show that d is a multiple of 6 which means it is composite.

Firstly, d is a multiple of 2 because

$$d \equiv a^{1999} + b^{1999} + c^{1999} \equiv a + b + c \equiv 0 \pmod 2$$

Next, it is easy to show that $x^3 \equiv x \pmod 3$. This is because $x^3-x = (x-1)x(x+1)$ which is a product of three consecutive integers. One of them must be a multiple of 3. Hence $x^3 - x \equiv 0 \pmod 3$. It follows that

$$\begin{aligned} d &\equiv a \cdot a^{1998} + b \cdot b^{1998} + c \cdot c^{1998} \\ &\equiv a \cdot a^{666} + b \cdot b^{666} + c \cdot c^{666} \\ &\equiv a \cdot a^{222} + b \cdot b^{222} + c \cdot c^{222} \\ &\equiv a \cdot (a^{74})^3 + b \cdot (b^{74})^3 + c \cdot (c^{74})^3 \\ &\equiv a^{75} + b^{75} + c^{75} \\ &\equiv a + b + c \\ &\equiv 0 \pmod 3 \end{aligned}$$

This means d is a multiple of 3. Therefore, it must be a multiple of $2 \times 3 = 6$.

Practice 30

What are the last two digits in the sum of the factorials of the first 100 positive integers?

(ref: 1117)

When $k \geq 10$, $k!$ must be a multiple of 100 because its prime factorization contains two 5s and more than two 2s. Therefore, the desired result equals the last two digits of

$$1! + 2! + \cdots + 9! \pmod{100}$$

Let's compute these terms separately:

$$\begin{aligned}
1! &\equiv 1 \pmod{100}\\
2! &\equiv 2 \pmod{100}\\
3! &\equiv 6 \pmod{100}\\
4! &\equiv 24 \pmod{100}\\
5! &\equiv 20 \pmod{100}\\
6! &\equiv 20 \pmod{100}\\
7! &\equiv 40 \pmod{100}\\
8! &\equiv 20 \pmod{100}\\
9! &\equiv 80 \pmod{100}
\end{aligned}$$

Adding the numbers on the right side leads to the result $\boxed{13}$.

Practice 31

Let $k = 2008^2 + 2^{2008}$. What is the units digit of $k^2 + 2^k$?

(ref: 1608 - AMC10)

Firstly, 2008^2 must end with 4. Meanwhile the units digit of 2^k repeats every 4 numbers: 2, 4, 8, 6, 2, $\cdots$. This means that the end digit of 2^{2008} must end with 6. Therefore, k ends with 0 which implies k^2 ends with 0.

To determine the last digit of 2^k, it is sufficient to compute $k \pmod 4$ because we can utilize the repeating pattern observed above. It is easy to see that $k \equiv 0 \pmod 4$. Therefore, 2^k will end with 6.

Hence $k^2 + 2^k$ ends with $\boxed{6}$.

Practice 32

Farmer Hank has fewer than 100 pigs on his farm. If he groups the pigs five to a pen, there are always three pigs left over. If he groups the pigs seven to a pen, there is always one pig left over. However, if he groups the pigs three to a pen, there are no pigs left over. What is the greatest number of pigs that Farmer Hank could have on his farm?

(ref: 1869 - MathCounts)

Let the number of pigs be n, then the conditions are

$$\begin{cases}
n \equiv 3 \pmod{5}\\
n \equiv 1 \pmod{7}\\
n \equiv 0 \pmod{3}
\end{cases}$$

The standard way to solve such a system of congruent relations is to use the Chinese

Remainder Theorem which gives the answer as

$$x \equiv 3 \times 21 \times 1 + 1 \times 15 \times 1 \equiv \boxed{78} \pmod{105}$$

Alternatively, given a range is provided (less than 100), it is possible to guess it out. Firstly, by the first relation, we know x must end with either 3 or 8. Then, by the second relation, we know it is necessary to check multiples of 7 which end with 2 or 7. The largest such number less than 100 is 77. Finally, we find $77 + 1 = \boxed{78}$ indeed is a multiple of 3. Hence it is the final answer.

Practice 33

Let $f(n)$ denote the sum of the digits of n. Find $f(f(f(4444^{4444})))$.

(ref: 2216 - IMO)

This is a typical problem that can be solved by the MOD-by-9 method.

Because $4444^{4444} < 10000^{4444} = 10^{17776}$, we find that 4444^{4444} has at most 17776 digits, which means that $f(4444^{4444})$ can not be greater than $9 \times 17776 = 159984$. It follows that $f(f(4444^{4444}))$ can not be greater than $9 \times 5 = 45$. Similarly, $f(f(f(4444^{4444})))$ can not be greater than $3 + 9 = 12$.

Meanwhile, we have

$$f(f(f(4444^{4444}))) \equiv 4444^{4444} \pmod{9}$$

and

$$4444^{4444} \equiv (-2)^{4444} = 2^{4444} = 2^{4440} \times 2^4 = 64^{740} \times 16 \equiv 1^7 \times 7 \equiv 7 \pmod{9}$$

There is only one positive integer no greater than 12 which is congruent to 7 modulo 9. Hence, the answer is $\boxed{7}$.

Practice 34

What is the last digit of $17^{17^{17^{17}}}$?

(ref: 2540 - PUMaC)

We know that the last digit of 17^k repeats as 7, 9, 3, 1, 7, $\cdots$. Therefore it is sufficient to compute $17^{17^{17}} \pmod 4$ which is

$$17^{17^{17}} \equiv 1^{17^{17}} \equiv 1 \pmod{4}$$

Therefore, the final answer is $\boxed{7}$.

Practice 35

Compute $50^{250} \pmod{83}$.

(ref: 2740)

By Fermat's little theorem, we have $50^{82} \equiv 1 \pmod{83}$ because 83 is prime and $(83, 50) = 1$.

$$50^{250} = 50^{246} \cdot 50^4 = \left(50^{82}\right)^3 \times 2500^2 \equiv 1^3 \times 10^2 = 100 \equiv \boxed{17} \pmod{83}.$$

Practice 36

Find the smallest positive integer n so that $107n$ has the same last two digits as n.

(ref: 2805 - Harvard-MIT)

This is equivalent to solving the following equation

$$n \equiv 107n \pmod{100}$$

or

$$n \equiv 7n \pmod{100} \implies 6n \equiv 0 \pmod{100}$$

$$\therefore \quad 6n = 100k \implies n = 50 \cdot \frac{k}{3}$$

where k is an integer. Clearly, the smallest such positive integer is $\boxed{50}$.

Practice 37

Find 8 prime numbers, not necessarily distinct such that the sum of the squares of these numbers is 992 less than 4 times of the product of these numbers.

(ref: 2822)

We need to solve for prime numbers, p_i, $i = 1, 2, \cdots, 8$ such that

$$\sum_{i=1}^{8} p_i^2 + 992 = 4 \prod_{i=1}^{8} p_i$$

If any p_i is odd, then $p_i^2 \equiv 1 \pmod{8}$. Therefore, if all the p_i are odd, the left side of the above equation is a multiple of 8, but the right side is not. This means that at least one of p_i must be even.

However, if at least one of p_i is even, the right side is divisible by 8. In this case, the left side cannot be a multiple of 8 unless all the p_i are even.

There is only one even prime which is 2. Setting all p_i as 2 does satisfy the above equation. Therefore, the only solution is

$$p_1 = p_2 = \cdots = p_8 = 2$$

Practice 38

Let $P(x)$ be a polynomial with integer coefficients satisfying both $P(0)$ and $P(1)$ are odd. Show that $P(x)$ has no integer zeros.

(ref: 2841)

If this is not true, then there exists an integer k such that $P(k) = 0$.

If k is even, then $P(k) \equiv P(0) \equiv 1 \pmod 2$. And, if k is odd, then $P(x) \equiv P(1) \equiv 1 \pmod 2$. Therefore, regardlessly, it always hold that

$$P(k) \equiv 1 \pmod 2$$

This means $P(k) \neq 0$, or k is not a zero of $P(x)$.

Practice 39

Show that if n is an integer greater than 1, then $(2^n - 1)$ is not divisible by n.

(ref: 3624 - Putnam)

If this claim does not hold, let's assume there exists an integer $n > 1$ such that $n \mid (2^n - 1)$. Then n must be an odd number because $2^n - 1$ is odd.

Let p be the least prime divisor of n, then $n \mid (2^n - 1)$ will imply $p \mid (2^n - 1)$, or equivalently, $2^n \equiv 1 \pmod p$. By Fermat's little theorem, we have $2^{p-1} \equiv 1 \pmod p$. Let $d = gcd(n, p - 1)$ then $2^d \equiv 1 \pmod p$. By definition of p, since $d \mid n$ and $d \leq p - 1 < p$, we get $d = 1$. Then $2 = 2^d \equiv 1 \pmod p$. This is a contradiction. Therefore, the previous assumption does not hold which means $(2^n - 1)$ is not divisible by n.

Practice 40

Does there exist a polynomial $P(x)$ such that $P(1) = 2015$ and $P(2015) = 2016$?

(ref: 3971)

Firstly, we know that if k is odd, then for any integer m, we must have $km \equiv m \pmod 2$.

Let $P(x) = a_n x^n + a_{n-1}x^{n-1} + \cdots + a_1 x + a_0$. Then

$$P(2015) \equiv a_n + a_{n-1} + \cdots + a_1 + a_0 = P(1) = 2015 \equiv 1 \pmod 2$$

But 2016 is even, Therefore it is impossible for $P(2015) = 2016$.

Practice 41

Find all prime number p such that both $4p^2 + 1$ and $6p^2 + 1$ are prime numbers.

(ref: 174 - Poland)

When $p = 5$, both $4p^2 + 1 = 101$ and $6p^2 + 1 = 151$ are prime. Therefore $p = 5$ is one solution. We are going to show that this is the only solution.

When $p \equiv \pm 1 \pmod 5$, we have $4p^2 + 1 \equiv 0 \pmod 5$. This means that $(4p^2 + 1)$ is a multiple of 5 which cannot be prime.

Meanwhile, when $p \equiv \pm 2 \pmod 5$, we have $6p^2 + 1 \equiv 0 \pmod 5$. This means that $(6p^2 + 1)$ is a multiple of 5 which is not prime.

Practice 42

Ms. Math's kindergarten class has 16 registered students. The classroom has a very large number, N, of play blocks which satisfies the conditions:

- If 16, 15, or 14 students are present in the class, then in each case all the blocks can be distributed in equal numbers to each student, and
- There are three integers $0 < x < y < z < 14$ such that when x, y, or z students are present and the blocks are distributed in equal numbers to each student, there are exactly three blocks left over.

Find the sum of the distinct prime divisors of the least possible value of N satisfying the above conditions.

(ref: 190 - AIME)

N must be a common multiple of 14, 15, and 16. Let k be their least common multiple, i.e. $k = 2^4 \cdot 3 \cdot 5 \cdot 7$. Then, $N = q \cdot k$.

Because 1, 2, 3, 4, 5, 6, 7, 8, 10, and 12 all divide k, so $x, y, z = 9, 11, 13$. Then we have the following three modulo equations:

$$\begin{aligned} nk &\equiv 3 \pmod 9 \\ nk &\equiv 3 \pmod{11} \\ nk &\equiv 3 \pmod{13} \end{aligned}$$

This means that nk must be three more than a common multiple of 9, 11, and 13, or $nk = 9 \times 11 \times 13 \times p + 3$ where p is an integer. Meanwhile, it must be divisible by k. Therefore there exists an integer q such that

$$\begin{aligned} 9 \times 11 \times 13 \times p + 3 &= 2^4 \times 3 \times 5 \times 7 \times 1 \\ 429 \times p + 1 &= 560 \times q \end{aligned}$$

This is a classic linear indeterminate equation. The least positive integer solution is $(p, q) = (171, 131)$. Setting $p = 171$ into $(9 \times 11 \times 13 \times p + 3)$ and factorizing find the distinct prime divisors are 2, 3, 5, 7, and 131. Their sum is $\boxed{148}$.

Practice 43

Let $\mathcal{S}$ be the set of all perfect squares whose rightmost three digits in base 10 are 256. Let $\mathcal{T}$ be the set of all numbers of the form $\frac{x-256}{1000}$, where x is in $\mathcal{S}$. In other words, $\mathcal{T}$ is the set of numbers that result when the last three digits of each number in $\mathcal{S}$ are truncated. Find the remainder when the tenth smallest element of $\mathcal{T}$ is divided by 1000.

(ref: 219 - AIME)

Firstly, we note that if x^2 ends with 256, then $(x + 1000)^2$ must end with 256 too because $(x + 1000)^2 \equiv x^2 \pmod{1000}$. Hence, we just need to focus on numbers less than 1000.

Next, x^2 ends with 256 is equivalent to say $x^2 - 256 = 1000 \cdot k$ where k is an integer. This implies $(x + 16)(x - 16)$ is a multiple of $10000 = 2^3 \times 5^3$.

Now because $x + 16 \not\equiv x - 16 \pmod 5$, therefore $(x + 16)$ and $(x - 16)$ cannot both be multiples of 5. Hence, one of them must be a multiple of $5^3 = 125$.

Meanwhile, because $x + 16 \equiv x - 16 \pmod 4$, therefore both of them must be multiples of 4. Otherwise, if neither of them is a multiple of 4, then $(x + 16)(x - 16)$ cannot be a multiple of $2^3 = 8$.

Combining both facts means one of $(x+16)$ and $(x-16)$ is a multiple of $125 \times 4 = 500$ or $x = 500n \pm 16$. Now, it is just a matter to check 16, $(500 - 16)$, $(500 + 16)$, and $(1000 - 16)$. Squares of all of them end with 256.

Therefore, the 10^{th} smallest qualifying number is $(2000 + 500 - 16) = 2484$. And the desired answer is

$$\frac{2484^2 - 256}{1000} \equiv \boxed{170} \pmod{1000}$$

Practice 44

The number 2017 is prime. Let $S = \sum_{k=0}^{62} \binom{2014}{k}$. What is the remainder when S is divided by 2017?

(ref: 474 - AMC12)

First, let's simplify C_{2014}^k as

$$\begin{aligned} C_{2014}^k &\equiv \frac{2014 \times 2013 \times \cdots (2014-k+1)}{k!} \\ &\equiv \frac{(-3)(-4)\cdots(-k-2}{k!)} \\ &\equiv (-1)^k C_{k+2}^k \\ &\equiv (-1)^k C_{k+2}^2 \\ &\equiv (-1)^k \times \frac{(k+2)(k+1)}{2} \end{aligned}$$

When k is even, let $k = 2m$. Then the sum of those "even" terms in the above expression equals

$$\sum_{m=0}^{31} \frac{(2m+2)(2m+1)}{2} = \sum_{m=0}^{30} (2m^2+3m+1)$$

When k is odd, let $k = 2m+1$. Then the sum of those "odd" terms above equals

$$\sum_{m=0}^{30} (-1) \times \frac{(2m+3)(2m+2}{2} = -\sum_{m=0}^{30} (2m^2+5n+3)$$

Adding them together we have

$$S = 2 \times 31^2 - 2\sum_{m=0}^{30} m + 3 \times 31 + 32 - 3 \times 31 = \boxed{1024}$$

Practice 45

Seven students count from 1 to 1000 as follows:

- Alice says all the numbers, except she skips the middle number in each consecutive group of three numbers. That is, Alice says 1, 3, 4, 6, 7, 9, . . ., 997, 999, 1000.
- Barbara says all of the numbers that Alice doesn't say, except she also skips the middle number in each consecutive group of three numbers.
- Candice says all of the numbers that neither Alice nor Barbara says, except she also skips the middle number in each consecutive group of three numbers.
- Debbie, Eliza, and Fatima say all of the numbers that none of the students with the first names beginning before theirs in the alphabet say, except each also skips the middle number in each of her consecutive groups of three numbers.
- Finally, George says the only number that no one else says.

What number does George say?

(ref: 1457 - AMC10)

Such a puzzle is clearly related to modular arithmetics. Let's try to find the pattern.

- Alice skips all the numbers n which satisfies $n \equiv 2 \pmod 3$. Her group contains 3 numbers. Each group produces one number for Barbara to process.
- Barbara's group contains 3 numbers provided by Alice which is equivalent to $3^2 = 9$ original numbers. It is easy to find out that all the number Barbara skips are $n \equiv (3 + 2) \pmod{3^2}$ or $n \equiv 5 \pmod 9$
- Similarly, Candice's group will contain $3^3 = 27$ original numbers and skip those $n \equiv (9 + 5) \pmod{3^3}$ or $n \equiv 14 \pmod{27}$
- Debbie: $n \equiv 27 + 41 \pmod{3^4}$ or $n \equiv 41 \pmod{81}$
- Eliza: $n \equiv 81 + 41 \pmod{3^5}$ or $n \equiv 122 \pmod{243}$
- Fatima: $n \equiv 243 + 122 \pmod{3^6}$ or $n \equiv 365 \pmod{729}$

There is only number n not exceeding 1000 which satifies $n \equiv 365 \pmod{729}$ which is $\boxed{365}$.

Practice 46

The number obtained from the last two non-zero digits of 90! is equal to n. What is n?

(ref: 1508 - AMC10)

First, the number of trailing zero equals the number of divisor 5 that 90! has. This equals

$$\left\lfloor \frac{90}{5} \right\rfloor + \left\lfloor \frac{90}{5^2} \right\rfloor = 21$$

This means that 90! has 21 trailing zeros. Let $N = \frac{90!}{10^{21}}$. Then the desired answer n equals $N \pmod{100}$.

Clearly, N still has more than two divisors of 2. Hence, $N \equiv 0 \pmod 4$. In order to calculate $N \pmod{100}$, we just need to compute $N \pmod{25}$.

By the conclusion of practice 26, we know $(5k+1)(5k+2)(5k+3)(5k+4) \equiv -1 \pmod{25}$. In order to use this conclusion, let

$$M = 1 \times 2 \times 3 \times 4 \times \underline{1} \times 6 \times \cdots \times 86 \times 87 \times 88 \times 89 \times \underline{8}$$

That is, to eliminate all 5 from 90!, i.e. $5 \to 1$, $10 \to 2$, $\cdots$, $25 \to 1$, $\cdots$, $90 \to 18$. Then, we have

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

The 2^{nd} last line above is corresponding to all the numbers which divides 5, but not 25. The last line is corresponding to those numbers which are multiple of 25. Therefore

$$M \equiv (-1)^{10} \times (-1)^3 \times (16 \times 17 \times 19)(1 \times 2 \times 3) \equiv 24 \pmod{25}$$

Meanwhile, we have $2^{21} \equiv (2^{10})^2 \times 2 \equiv (-1)^2 \times 2 \equiv 2 \pmod{25}$. It follows that

$$N = \frac{M}{2^{21}} \equiv \frac{24}{2} \equiv 12 \pmod{25}$$

Together with the fact of $N \equiv 0 \pmod 4$, we found $N \equiv \boxed{12} \pmod{100}$

Practice 47

Prove that if p and p^2+8 are prime, then p^3+8p+2 is prime.

(ref: 2217)

First, when $p=2$, $p^2+8=12$ is not a prime. Next, when $p=3$, both $p^2+8=17$ and $p^3+8p+2=53$ are prime.

Therefore, the conclusion holds when $p \leq 3$. Now, let's show that when $p>3$, (p^2+8) cannot be a prime.

In this case, given p is prime, we have have $p \not\equiv 0 \pmod 3$. However,

$$p^2+8 \not\equiv 0 \pmod 3 \implies p^2 \not\equiv 1 \pmod 3 \implies p \not\equiv \pm 1 \pmod 3$$

This is impossible because one of $p \equiv 0 \pmod 3$ and $p \equiv \pm 1 \pmod 3$ must hold.

Practice 48

What is the smallest positive integer n such that $20 \equiv n^{15} \pmod{29}$?

(ref: 2614 - PUMaC)

By Fermat's Little Theorem, we have $a^{28} \equiv 1 \pmod{29}$ for all positive integers a which are not multiples of 29.

It follows that $a^{14} \equiv \pm 1 \pmod{29}$, so $a^{15} \equiv \pm a \pmod{29}$ for all such a. Therefore, if $a^{15} \equiv 20 \pmod{29}$, then $\pm a \equiv 20 \pmod{29}$.

We know that $9^{14} = 3^{28} \equiv 1 \pmod{29}$, so $9^{15} \equiv 9 \pmod{29}$.

Next we try $a=20$, and we find that $20^{14} \equiv 49^{14} \equiv 7^{28} \equiv 1 \pmod{29}$, and so $20^{15} \equiv 20 \pmod{29}$. Therefore, the answer is $\boxed{20}$.

Practice 49

Given that there are 24 primes between 3 and 100, inclusive, what is the number of ordered pairs (p,a) with p prime, $3 \leq p < 100$, and $1 \leq a < p$ such that the sum $a+a^2+a^3+\cdots+a^{(p-2)!}$ is not divisible by p?

(ref: 2615 - PUMaC)

If $a=1$, then the sum just becomes $(p-2)!$, which is never divisible by p. So since there are 24 odd primes between 2 and 100, there are 24 solutions of the form $(p,1)$.

Next, suppose $a \neq 1$. The sum can then be written as

$$a + a^2 + \cdots + a^{(p..2)!} = a\frac{a^{(p..2)!} - 1}{a - 1} = \frac{a}{a-1} \cdot (a^{(p..2)!} - 1)$$

Since $1 < a < p$, the term $\frac{a}{(a-1)}$ does not contribute to whether the sum is divisible by p. So it sufficient to consider the term $a^{(p-2)!} - 1$. Now look at the following cases.

- If $p = 3$, then the sum is just a which isn't divisible by p. So $(3, 2)$ is a valid solution.
- If $p = 5$, then the sum is just

  $$\frac{a}{a-1} \cdot (a^6 - 1) \equiv \frac{a}{a-1} \cdot (a^2 - 1) \equiv a(a+1) \pmod 5$$

  by Fermat's Little Theorem. Plugging in $a = 2, 3, 4$ shows that $(5, 2)$ and $(5, 3)$ are the only solutions here.
- If $p > 5$, then $2 \neq (p-1)/2$. Moreover, we also have $2 \mid (p-2)!$ and $(p-1)/2 \mid (p-2)!/2$ since $1 < 2, (p-1)/2 < p-2$. Thus $(p-1) \mid (p-2)!$, so by Fermat's Little Theorem $a^{(p-2)!} - 1 \equiv \pmod p$. Thus the sum is always divisible by p in this case, and there are no solutions here.

Thus there is a total of $\boxed{27}$ solutions.

Practice 50

If for any integer $k \neq 27$ and $\left(a - k^{2015}\right)$ is divisible by $(27 - k)$, what is the last two digits of a?

(ref: 2621)

Let $f(k) = a - k^{2015}$. Because $(k - 27) \mid f(k)$, we have $f(27) = 0$, i.e. 27 is a root of $f(k)$. This means that $a - 27^{2015} = 0$ which implies that the last two digits of a is the same as those of 27^{2015}.

$$27^{2015} = 3^{6045} = (3^4)^{1511} \times 3 = 81^{1511} \times 3$$

Now by applying the "quick way to find the tens digit" trick, we know the tens digit of 81^{1511} is 8. Meanwhile, its units digit obviously is 1. Hence, 81^{1511} ends with 81 which leads to 27^{2015} ends with $\boxed{43}$.

Practice 51

Find the least non-negative residue of $70! \pmod{5183}$.

(ref: 2739)

Because $5183 = 71 \times 73$, let'sstart by finding the residues of 70! mod 71 and 73.

By Wilson's theorem, $70! \equiv -1 \pmod{71}$.

Next, let $k = 70! \pmod{73}$. Then $71 \times 72 \times k \equiv 70! \times 71 \times 72 \pmod{73} \implies (-2)(-1)k \equiv 72! \pmod{73} \implies 2k \equiv -1 \pmod{73}$.

Note that $2 \times 37 = 74 \equiv 1 \pmod{73}$. So $37 \cdot 2k \equiv 37 \cdot (-1) \pmod{73} \implies k \equiv -37 \equiv 36 \pmod{73}$.

Thus, $70! \equiv -1 \pmod{71}$ and $70! \equiv 36 \pmod{73}$.

Applying CRT to solve these two equations yields: $70! = \boxed{1277} \mod 5183$.

Practice 52

Let x be an integer and p is a prime divisor of $(x^6 + x^5 + \cdots + 1)$. Show that $p = 7$ or $p \equiv 1 \pmod{7}$.

(ref: 3795)

Obviously, if $x = 1$, then $p = 7$.

When $x \neq 1$, then p divides $\frac{x^7-1}{x-1}$. Hence, $x^7 \equiv 1 \pmod{p}$. This implies $p \not| x$. Then, by Fermat's little theorem, we have $x^{p-1} \equiv 1 \pmod{p}$. This is followed by

$$x^{(7,p-1)} \equiv 1 \pmod{p}$$

where $(7, p-1)$ is the greatest common divisor of 7 and $(p-1)$.

If $p \not\equiv 1 \pmod{7}$, i.e. $7 \not| (p-1)$, then $(7, p-1) = 1$. This will lead to $x \equiv 1 \pmod{p}$ by the equation above. Then,

$$x^6 + x^5 + \cdots + 1 \equiv 1^6 + 1^6 + \cdots + 1^6 \equiv 7 \pmod{p}$$

and

$$p \mid (x^6 + x^5 + \cdots + 1) \implies x^6 + x^5 + \cdots + 1 \equiv 0 \pmod{p}$$

This will lead to the conclusion $p = 7$. Hence, we find the claim holds.

Practice 53

Let x be an integer and p is an odd prime divisor of $x^2 + 1$. Show that $p \equiv 1 \pmod{4}$.

(ref: 3796)

Because p is odd, suppose $p \not\equiv 1 \pmod 4$, then $p \equiv 3 \pmod 4$.

Let $p = 4k + 3$ where k is an integer. Then

$$p \mid x^2 + 1 \implies x^2 \equiv -1 \pmod p$$
$$\therefore \quad x^{p-1} = x^{4k+2} = (x^2)^{2k+1} \equiv (-1)^{2k+1} \equiv -1 \pmod p$$

However, by Fermat's little theorem, we should have

$$x^{p-1} \equiv 1 \pmod p$$

These two relations will force $p = 2$ which is a contradiction to the fact p is odd.

Practice 54

Let p be an odd prime number. For positive integer k satisfying $1 \le k \le p - 1$, the number of divisors of $kp + 1$ between k and p exclusive is a_k. Find the value of $a_1 + a_2 + \ldots + a_{p-1}$.

(ref: 3841 - Japan)

Let's first examine a few simplest cases and try to find some clues from these trials.

When $p = 3$:

$p = 3$	k	$kp + 1$	a_i	*divisors*
	1	4	1	(2)
	2	7	–	–
		$a_1 + a_2 =$	1	(2)

When $p = 5$:

$p = 5$	k	$kp + 1$	a_i	*divisors*
	1	6	2	(2, 3)
	2	11	–	–
	3	16	1	(4)
	4	21	–	–
		$a_1 + \cdots + a_4$	3	(2, 3, 4)

When $p = 7$:

$p = 7$	k	$kp + 1$	a_i	*divisors*
	1	8	2	(2, 4)
	2	15	2	(3, 5)
	3	22	–	–
	4	29	–	–
	5	36	1	(6)
	6	43	–	–
		$a_1 + \cdots + a_6$	5	(2, 3, 4, 5, 6)

It appears that

- The answer is $\boxed{p-2}$,
- Every number in $2, 3, \cdots, p-1$ appears once and only once among the divisors, and
- The largest $kp+1$ (i.e. when $k = p-1$) does not have any qualified divisor.

Hence, a hint for solve this problem app

We note that there are totally $(p-2)$ divisors $2, 3, \cdots, p-1$, and there are totally $(p-2)$ numbers in the form of $(kp+1)$, excluding the largest one. Therefore, the observation listed above seems to indicate that the original problem is equivalent to showing that every number in 2, 3, $\cdots$, $p-1$ divides on and only one number in the following list:

$$p+1, 2p+1, 3p+1, \cdots, (p-2)p+1$$

This claim can go further.

Claim: Fixed $m(1 < m < p)$, then m contribute exactly once in one of $a_1, a_2, \ldots, a_{m-1}$.

Proof. Consider the following $m-1$ numbers:

$$p+1, 2p+1, \ldots, (m-1)p+1,$$

since $\gcd(m, p) = 1$, and none of them equal to 1 modulo m, so the statement follows.

Hence the answer is $\boxed{p-2.}$

Practice 55

Let p be an odd prime divisor of number (a^2+1) where a is an integer. Show that $p \equiv 1 \pmod 4$.

(ref: 3870)

Because $p \mid a^2+1$, therefore $a^2 \equiv -1 \pmod p$.

Practice 56

For positive integers n and k, let $f(n,k)$ be the remainder when n is divided by k, and for $n > 1$ let $F(n) = \max\limits_{1 \le k \le \frac{n}{2}} f(n,k)$. Find the remainder when $\sum\limits_{n=20}^{100} F(n)$ is divided by 1000.

(ref: 208 - AIME)

We can find that

$20 \equiv 6 \pmod 7$

$21 \equiv 5 \pmod 8$

$22 \equiv 6 \pmod 8$

$23 \equiv 7 \pmod 8$

$24 \equiv 6 \pmod 9$

$25 \equiv 7 \pmod 9$

$26 \equiv 8 \pmod 9$

Observing these and we can find that the reminders are in groups of three continuous integers, considering this is true, and we get

$99 \equiv 31 \pmod{34}$

$100 \equiv 32 \pmod{34}$

So the sum is $5 + 3 \times (6 + ... + 31) + 32 \times 2 = 1512$, so the answer is $\boxed{512}$.

The Proof

The solution presented above does not prove why $F(x)$ is found by dividing x by 3. Indeed, that is the case, as rigorously shown below.

Consider the case where $x = 3k$. We shall prove that $F(x) = f(x, k+1)$. For all $x/2 >= n > k+1, x = 2n+q$, where $0 <= q <= n$. This is because $x > 3k+3 = 3n$ and $x < n$. Also, as n increases, q decreases. Thus, $q = f(x,n) < f(x,k+1) = k-2$ for all $n > k+1$. Consider all $n < k+1. f(x,k) = 0$ and $f(x,k-1) = 3$. Also, $0 < f(x,k-2) < k-2$. Thus, for $k > 5, f(x,k+1) > f(x,n)$ for $n < k+1$.

Similar proofs apply for $x = 3k+1$ and $x = 3k+2$. The reader should feel free to derive these proofs himself.

Generalized Solution

Lemma : Highest remainder when n is divided by $1 <= k <= n/2$ is obtained for $k_0 = (n + (3 - n \pmod 3)))/3$ and the remainder thus obtained is $(n - k_0 * 2) = [(n-6)/3 + (2/3) * n \pmod 3]$.

Note : This is the second highest remainder when n is divided by $1 <= k <= n$ and the highest remainder occurs when n is divided by $k_M = (n+1)/2$ for odd n and $k_M = (n+2)/2$ for even n.

Using the lemma above:

$\sum_{n=20}^{100} F(n) = \sum_{n=20}^{100} [(n-6)/3+(2/3)*n \pmod 3] = [(120*81/2)/3-2*81+(2/3)*81] = 1512$

So the answer is $\boxed{512}$

Proof of Lemma: It is similar to *TheProof* stated above.

Kris17

Practice 57

Let sequence $g(n)$ satisfy $g(1) = 0, g(2) = 1, g(n+2) = g(n+1) + g(n) + 1$ where $n \geq 1$. Show that if n is a prime greater than 5, then $n \mid g(n)[g(n)+1]$.

(ref: 2699 - IMO)

Let $f(n) = g(n) + 1$, then $f(1) = 1$, $f(2) = 2$, and $f(n+2) = f(n+1) + f(n)$. The solution to this sequence is

$$\begin{aligned} f(n) &= \frac{1}{\sqrt{5}} \cdot \left[\left(\frac{1+\sqrt{5}}{2} \right)^{n+1} - \left(\frac{1-\sqrt{5}}{2} \right)^{n+1} \right] \\ &= \frac{1}{2^n} \cdot \left(C_{n+1}^1 + 5C_{n+1}^3 + 5^2 C_{n+1}^5 + \cdots + 5^{\frac{n-1}{2}} C_{n+1}^n \right) \end{aligned}$$

Because n is a prime greater than 5, therefore $(2, n) = 1 \implies (2^n, n) = 1$ and $n \mid C_{n+1}^i$ where $3 \leq i \leq n-1$. Therefore, the previous relation will lead to

$$2^n f(n) \equiv C_{n+1}^1 + 5^{\frac{n-1}{2}} C_{n+1}^n \equiv (n+1)\left(1 + 5^{\frac{n-1}{2}}\right) \pmod n$$

It follows that

$$2^n [f(n) - 1] \equiv 1 + 5^{\frac{n-1}{2}} - 2^n \equiv -1 + 5^{\frac{n-1}{2}} \pmod n$$

by Fermat Little Theorem. Multiplying the last two equations gives

$$2^{2n} f(n)[f(n) - 1] \equiv 5^{n-1} - 1 \equiv 0 \pmod n$$

by Fermat Little Theorem again. Therefore

$$f(n)[f(n) - 1] \equiv 0 \pmod 5 \implies g(n)[g(n) + 1] \equiv 0 \pmod 5$$

Copyrighted material, issued at 5/11/2026 11:00:20 PM