Introduction to Modular Arithmetic

CaptainFlint

May 30, 2015

Part I
Introduction

Numbers are sometimes thought of as they appear on the number line: stretching infinitely out in each direction. The normal system of arithmetic is based on the ways numbers relate to each other on the number line. Other times, numbers are thought of repeating in a cycle. For example, 6 A.M. is thought of as the same time, even though it is never experienced more than once. In this article we will discover a system of arithmetic using this number system.

Modular arithmetic is an arithmetic system using only the integers $0, 1, 2, \ldots, a-1$. When we work this way, we say we are working modulo a, and the modulus of the system is a.

Part II
Modular Congruences

We will start with a problem:

1 Problem

We have a clock with six numbers on its face: $0, 1, 2, 3, 4$, and 5. The clock only hand moves clockwise from 0 to 1 to 2 to 3 to 4 to 5 and back again to 0.

1. What number is the hand pointing at after 12 ticks?
2. What number is the hand pointing at after 28 ticks?
3. What number is the hand pointing at after 42 ticks?
4. What number is the hand pointing at after 1337 ticks?

Solution: We list the first 30 numbers in the list and the first 30 positive integers side by side:

1	2	3	4	5	0	1	2	3	4	5	6
1	2	3	4	5	*0*	7	8	9	10	11	*12*
1	2	3	4	5	0	13	14	15	16	17	18
1	2	3	4	5	0	19	20	21	22	23	24
1	2	3	*4*	5	0	25	26	27	*28*	29	30

We can see that the answers to parts 1 and 2 are $\underline{0}$ and $\underline{4}$, respectively. We can also notice that each number on the left grid is the remainder of each number on the right grid when divided by 6. Hence, we see that the

answer to part 3 is the remainder when $42 \div 6$, which is 0, and that the answer to part 4 is $1337 \div 6$, which is 5.

2 Congruence

Two integers are said to be **equivalent** (or **congruent**) modulo a if their difference is a multiple of a. We shorten "modulo" to "mod", and use the symbol $\equiv$ to denote congruence. For example,

$$12 \equiv 0 \pmod 6 \text{ and } 32 \equiv 16 \pmod 4.$$

For integers x and y, $y \equiv x \pmod a$ if and only if $m \mid x - y$. Hence, for an integer z, we have $x - y = za$. Isolating z gives us $z = \frac{x-y}{a}$. If z is an integer, then $y \equiv x \pmod a$.

Also, for positive integers x and y, $x \equiv y \pmod a$ if and only if

$$x = z_1 a + w$$
$$y = z_2 a + w$$

where z_1, z_2, and w are integers, and $0 \leq w < a$.

3 Exercises

3.1 Exercise 1

Are 31 and 24 congruent modulo 9?

3.2 Exercise 2

Are 45 and 15 congruent modulo 3?

Part III
Residues

4 Introduction

We say that b is the modulo-a residue of n when $c \equiv b \pmod a$, and $0 \leq b < a$.

5 Residue Classes

We begin with a problem.

5.1 Problem

List the integers between -70 and 70 whose modulo 12 residues are 10.

5.2 Solution

An integer is congruent to 10 mod 12 if it can be written as $12a + 10$ for any integer a. This gives us the inequality

$$-70 < 12a + 10 < 70.$$

Subtracting 10 form all sides gives use

$$-80 < 12n < 60,$$

and dividing by 12 gives

$$-6\frac{2}{3} < n < 5.$$

Thus, we have

$$\begin{array}{rcrcrcr}
n & = & -6: & & 12(-6)+10 & = & -62 \\
n & = & -5: & & 12(-5)+10 & = & -50 \\
n & = & -4: & & 12(-4)+10 & = & -38 \\
n & = & -3: & & 12(-3)+10 & = & -26 \\
n & = & -2: & & 12(-2)+10 & = & -14 \\
n & = & -1: & & 12(-1)+10 & = & -2 \\
n & = & 0: & & 12(0)+10 & = & 10 \\
n & = & 1: & & 12(1)+10 & = & 22 \\
n & = & 2: & & 12(2)+10 & = & 34 \\
n & = & 3: & & 12(3)+10 & = & 46 \\
n & = & 4: & & 12(3)+10 & = & 58
\end{array}$$

Hence, all integers b such that $-70 < b < 70$ and $b \equiv 10 \pmod{12}$ are

$$\{-62, -50, -38, -26, -14, -2, 10, 22, 34, 46, 58\}.$$

5.3 Definition of a Residue Class

The integers congruent to $x \pmod{a}$ are known as a **residue class**. (Residue classes are also known as equivalence classes or congruence classes.) For example, $\{-62, -50, -38, -26, -14, -2, 10, 22, 34, 46, 58\}$ is a residue class of $10 \pmod{12}$.

6 Exercises

6.1 Exercise 1

Determine the modulo-9 residue of each of the following.

1. 11
2. 45
3. 23
4. 434
5. 42
6. 1337

6.2 Exercise 2

Write each of the following integers in the form $3a + b$, where a and b are integers and $0 \leq b < 3$.

1. 43
2. 4
3. 100

4. 98
5. 42
6. -34
7. 1337

6.3 Exercise 3

Show that if $x \equiv y \pmod{a}$ and $y \equiv z \pmod{a}$, then $x \equiv z \pmod{a}$.

Part IV
Modular Addition & Subtraction

7 Introduction

Let a_1, a_2, b_1, and b_2 be integers such that

$$a_1 \equiv a_2 \pmod{n}$$
$$b_1 \equiv b_2 \pmod{n}.$$

We can add these, and get

$$a_1 + b_1 \equiv a_2 + b_2 \pmod{n}.$$

7.1 Proof

From the definition of congruence, we have

$$\tfrac{a_1 - a_2}{n} \text{ and } \tfrac{b_1 - b_2}{n}$$

are integers. Manipulating these expressions, we have

$$\frac{a_1 - a_2}{n} = \frac{a_1 + b_2 - a_2 - b_2}{n} = \frac{(a_1 + b_2) - (a_2 + b_2)}{n}.$$
$$\frac{b_1 - b_2}{n} = \frac{a_1 + b_1 - a_1 - b_1}{n} = \frac{(a_1 + b_1) - (a_1 + b_2)}{n}.$$

Since each of these quantities are integers, we have

$$a_1 + b_1 \equiv a_1 + b_2 \pmod{n}$$
$$a_1 + b_2 \equiv a_2 + b_2 \pmod{n}.$$

Putting this together, we have

$$a_1 + b_1 \equiv a_1 + b_2 \equiv a_2 + b_2 \pmod{n}.$$

From this we see that

$$a_1 + b_1 \equiv a_2 + b_2 \pmod{n}.$$

8 Exercises

8.1 Exercise 1

Is $54 + 42 \equiv 2 + 14 \pmod{8}$?

8.2 Exercise 2

Is $69 - 45 \equiv 18 - 15 \pmod 3$?

8.3 Exercise 3

Let a, b, and c be integers whose residues modulo 8 are 4, 5, and 7, respectively. Compute the residue of $a + b + c \pmod 8$.

Part V
Modular Multiplication

9 Introduction

Let a, b, c, and d be integers. If

$$\begin{aligned} a &\equiv b \pmod m \\ c &\equiv d \pmod m, \end{aligned}$$

then

$$ac \equiv bd \pmod m.$$

9.1 Proof

Since m is a divisor of $a - b$ and $c - d$, we have

$$\begin{aligned} a &= b + xm \\ c &= d + ym \end{aligned}$$

where x and y are integers. Expanding the product ac, we have

$$\begin{aligned} ac &= (b + xm)(d + ym) \\ &= bd + bym + dxm + xym^2 \\ &= bd + m(by + dx + xym). \end{aligned}$$

Since $ac - bd$ is multiple of m, we have

$$\begin{aligned} ac - bd &= bd + m(by + dx + xym) - bd \\ &= m(by + dx + xym). \end{aligned}$$

Therefore, $ac \equiv bd \pmod m$.

10 Exercises

10.1 Exercise 1

Is $9 \cdot 43 \equiv 8 \cdot 98 \pmod{23}$?

10.2 Exercise 2

Find the modulo 4 residue of 100!.

10.3 Exercise 3

The residues of 3 positive integers modulo 8 are $1, 4$, and 7. Find the residue of their products modulo 8.

Part VI
Modular Exponentiation

11 Introduction

Let a and b be integers, and c be a natural number. If $a \equiv b \pmod{m}$, then

$$a^c \equiv b^c \pmod{m}.$$

11.1 Proof

We have $a \cdot a \equiv b \cdot b \pmod{m} \implies a^2 \equiv b^2 \pmod{m}$. We can multiply factors of a and b to powers of a and b to show that the next highest power of a and b are also congruent.

$$\begin{aligned}
a \cdot a^2 &\equiv b \cdot b^2 \pmod{m} &\implies\quad a^3 &\equiv b^3 \pmod{m} \\
a \cdot a^3 &\equiv b \cdot b^3 \pmod{m} &\implies\quad a^4 &\equiv b^4 \pmod{m} \\
a \cdot a^4 &\equiv b \cdot b^4 \pmod{m} &\implies\quad a^5 &\equiv b^5 \pmod{m} \\
a \cdot a^5 &\equiv b \cdot b^5 \pmod{m} &\implies\quad a^6 &\equiv b^6 \pmod{m} \\
&&\vdots& \\
a \cdot a^{c-1} &\equiv b \cdot b^{c-1} \pmod{m} &\implies\quad a^c &\equiv b^c \pmod{m}
\end{aligned}$$

12 Exercises

12.1 Exercise 1

Is $24^{14} - 15^{14}$ divisible by 9?

12.2 Exercise 2

Find residue r such that $5^{6001} \equiv r \pmod{7}$.

Part VII
Modular Division

13 Introduction

There is no law of division in modular arithmetic. We can see this with the following example.

13.1 Example

We have the congruence

$$6 \equiv 16 \pmod{10},$$

which is true. Dividing by 2, we have

$$3 \equiv 8 \pmod{10},$$

which is clearly not true.

In the next part, we will see a concept called *modular inverse* that is analogous to division, but **there is no such thing as division in modular arithmetic.**

Part VIII
Modular Inverses

14 Introduction

The **multiplicative inverse** of an integer $a \pmod{m}$ is the integer a^{-1} such that

$$a \cdot a^{-1} \equiv 1 \pmod{m}.$$

15 Problems

15.1 Problem 1

15.1.1 Problem

Find the inverses of all mod 12 residues that have inverses.

15.1.2 Solution

We write out the entire modulo 12 multiplication table:

$\times$	0	1	2	3	4	5	6	7	8	9	10	11
0	0	0	0	0	0	0	0	0	0	0	0	0
1	0	$\boxed{1}$	2	3	4	5	6	7	8	9	10	11
2	0	2	4	6	8	10	0	2	4	6	8	10
3	0	3	6	9	0	3	6	9	0	3	6	9
4	0	4	8	0	4	8	0	4	8	0	4	8
5	0	5	10	3	8	$\boxed{1}$	6	11	4	9	2	7
6	0	6	0	6	0	6	0	6	0	6	0	6
7	0	7	2	9	4	11	6	$\boxed{1}$	8	3	10	5
8	0	8	4	0	8	4	0	8	4	0	8	4
9	0	9	6	3	0	9	6	3	0	9	6	3
10	0	10	8	6	4	2	0	10	8	6	4	2
11	0	11	10	9	8	7	6	5	4	3	2	$\boxed{1}$

From this, we see that all modulo 12 residues that have inverses are $1, 5, 7$, and 11, and that there exists no inverses for residues $2, 3, 4, 6, 8, 9$, and 10.

We can note that $1, 5, 7$, and 11 are relatively prime to 12, and $2, 3, 4, 6, 8, 9$, and 10 are not.

15.2 Problem 2

15.2.1 Problem

Prove that a^{-1} modulo n exists only if $\gcd(a, n) = 1$.

15.2.2 Solution

If a^{-1} exist, it is a solution to the congruence $ax \equiv 1 \pmod{n}$. Thus, for some value of x,

$$ax - yn = 1,$$

where y is an integer. We let $z = \gcd(a, n)$, which means that $z \mid ax$ and $z \mid yn$. A divisor of two integers is the divisor of their difference, which means that $z \mid (ax - yn)$. Since $ax - yn = 1$, $z \mid 1$. The only integer that is a divisor of 1 is 1, so $z = 1$. Therefore, a^{-1} exists if $\gcd(a, n) = 1$.

16 Exercises

16.1 Exercise 1

Does 6 modulo 25 have an inverse? Why?

16.2 Exercise 2

Find all possible residues modulo 20 that have inverses.

Part IX
How to Find Modular Inverses

Let's begin with a problem:

17 Problem

17.1 Problem

Find the inverse of 3 modulo 7.

17.2 Solution

We list the first few integers that are congruent to 1 (mod 7). They are

$$8, 15, 22, 29, \ldots$$

The term 15 is of the form $3x$, where $x = 5$. Thus, the inverse of 3 modulo 7 is $\boxed{5}$.

This method seems tedious for larger moduli and inverses. We need a systematic way to find inverses.

18 Finding Modular Inverses with the Euclidean Algorithm

18.1 Introduction to the Euclidean Algorithm

Euclidean Algorithm is used for finding the GCD of a pair of numbers. It is also for finding coefficients x and y that, given a pair of relatively prime numbers a and b, would let us write $ax + by = 1$. If a and m are relatively prime integers, we can find integers x and y such that $ax + my = 1$. If we reduce this modulo m, we get

$$ax \equiv 1 \pmod{m}.$$

The integer x is the modular inverse of a.

Now, let's solve a problem using the Euclidean Algorithm.

18.2 Problem

18.2.1 Problem

Find the inverse of 37 modulo 97.

18.2.2 Solution

We turn this into the equation $37x + 97y = 1$, and solve for x. Then, we divide $97 \div 37$ to get a quotient of 2 and a remainder of 23. We compute $37 \div 23$, and get a quotient of 1 and a remainder of 14. Next, we compute $23 \div 14$, and we get a quotient of 1 and remainder 9. Dividing $14 \div 9$, we get quotient 1 and remainder 5. $9 \div 5$ has a quotient of 2 and a remainder of 4. Finally, $5 \div 4$ has a quotient 1 and remainder 1. From this we get the equations:

$$\begin{aligned} 97 &= 2 \cdot 37 + 23 \\ 37 &= 1 \cdot 23 + 14 \\ 23 &= 1 \cdot 14 + 9 \\ 14 &= 1 \cdot 9 + 5 \\ 9 &= 1 \cdot 5 + 4 \\ 5 &= 1 \cdot 4 + 1. \end{aligned}$$

We rearrange these equations to isolate the remainders:

$$\begin{aligned} 23 &= 97 - 2 \cdot 37 \\ 14 &= 37 - 1 \cdot 23 \\ 9 &= 23 - 1 \cdot 14 \\ 5 &= 14 - 1 \cdot 9 \\ 4 &= 9 - 1 \cdot 5 \\ 1 &= 5 - 1 \cdot 4. \end{aligned}$$

Substituting, we have:

$$\begin{aligned} 1 &= 5 - 1 \cdot 4 \\ &= 5 - (9 - 1 \cdot 5) \\ &= 2 \cdot 5 - 9 \\ &= 2(14 - 1 \cdot 9) - 9 \\ &= 2 \cdot 14 - 3 \cdot 9 \\ &= 2 \cdot 14 - 3(23 - 1 \cdot 14) \\ &= 5 \cdot 14 - 3 \cdot 23 \\ &= 5(37 - 1 \cdot 23) - 3 \cdot 23 \\ &= 5 \cdot 37 - 8 \cdot 23 \\ &= 5 \cdot 37 - 8(97 - 2 \cdot 37) \\ &= -8 \cdot 97 + 21 \cdot 37. \end{aligned}$$

Hence, $x = 21$, which means that the inverse of 37 modulo 97 is $\boxed{21}$, or $21 \cdot 37 \equiv 1 \pmod{97}$.

19 Exercises

19.1 Exercise 1

Find the inverse of 5 modulo 6.

19.2 Exercise 2

Find the inverse of 19 modulo 21.

19.3 Exercise 3

Find x such that $17x \equiv 1 \pmod{23}$.

Part X
Linear Congruences

20 Introduction

A linear congruence equation is a congruence that has a variable raised only to the first power. A linear congruence can be expressed as

$$ax \equiv b \pmod{n},$$

where a and b are integers, a modulus n, and variable x. For example, $4x \equiv 3 \pmod{6}$ is a linear congruence.

Let's start by solving a few simple linear congruences, and then move on to some harder problems.

21 Problems

21.1 Problem 1

21.1.1 Problem

Find the values of x where $0 \leq x < 5$ that satisfy the following linear congruences:

1. $x - 4 \equiv 0 \pmod{5}$.
2. $x - 1 \equiv 1 \pmod{5}$.
3. $x + 3 \equiv 1 \pmod{5}$.
4. $x + 12 \equiv 3 \pmod{5}$.

21.1.2 Solution

1. Since addition is a valid operation in modular arithmetic, we can add 4 to both sides. Thus, we have $x - 4 + 4 \equiv 0 + 4 \pmod{5} \implies x \equiv \boxed{4} \pmod{5}$.
2. As before, we add 1 to both sides of the congruence, which gives $x \equiv \boxed{2} \pmod{5}$.
3. Since subtraction is a valid operation in modular arithmetic, we can subtract 3 from both sides. Thus, we have $x \equiv -2 \equiv \boxed{3} \pmod{5}$.
4. Subtracting 12 from both sides, we have $x \equiv -9 \equiv \boxed{1} \pmod{5}$.

21.2 Problem 2

21.2.1 Problem

Find the values of x where $0 \leq x < 5$ that satisfy the following linear congruences:

1. $3x \equiv 1 \pmod 5$.
2. $3x \equiv 2 \pmod 5$.
3. $2x \equiv 3 \pmod 5$.
4. $12x \equiv 4 \pmod 5$.
5. $2x - 4 \equiv 2 \pmod 5$.

21.2.2 Solution

1. We can't divide both sides by 4, because there is no law of division in modular arithmetic. However, we can multiply by the modular inverse of 3 (mod 5), which is 2. Multiplying, we have $6x \equiv 2 \pmod 5$. Since $6 \equiv 1 \pmod 5$, we have $6x \equiv 1x \equiv x \pmod 5$. Thus, we have $x \equiv \boxed{2} \pmod 5$.
2. In this part, we again multiply $3x \equiv 2 \pmod 5$ by 3^{-1}, which is 2. Thus, we have $6x \equiv 4 \pmod 5 \implies x \equiv \boxed{4} \pmod 5$.
3. The inverse of $2 \pmod 5$ is 3. Multiplying, we have $6x \equiv 9 \pmod 5 \implies x \equiv 9 \pmod 5 \implies x \equiv \boxed{4} \pmod 5$.
4. The $12^{-1} \pmod 5$ is 3. Multiplying by 3, we have $36x \equiv 12 \pmod 5 \implies x \equiv 12 \pmod 5 \implies x \equiv \boxed{2} \pmod 5$.
5. We first add 4 to both sides and simplify:

$$\begin{aligned} 2x - 4 + 4 &\equiv 2 + 4 \pmod 5 \\ 2x &\equiv 6 \pmod 5 \\ 2x &\equiv 1 \pmod 5. \end{aligned}$$

   Since $2^{-1} \pmod 5$ is 3, we have $6x \equiv 3 \pmod 5 \implies x \equiv \boxed{3} \pmod 5$.

From these problems, we see that if the coefficient of the variable is relatively prime to the modulus, then we can get rid of the coefficient by multiplying both sides of the congruence by the inverse of the coefficient.

22 Exercises

22.1 Exercise 1

Find all possible values of x such that $23x \equiv 14 \pmod{15}$.

22.2 Exercise 2

Find all possible values of x such that $23x + 234 \equiv 12 \pmod{15}$.

22.3 Exercise 3

Let y be a positive integer. Prove that if $ay \equiv by \pmod{my}$ for integers a and b, then $a \equiv b \pmod{m}$. (Introduction to Number Theory)

Part XI
Systems of Linear Congruences

Let's begin with some problems.

23 Simple Systems of Linear Congruences

23.1 Problem 1

23.1.1 Problem

Find all x such that

$$\begin{aligned} x &\equiv 0 \pmod{2} \\ x &\equiv 0 \pmod{5}. \end{aligned}$$

23.1.2 Solution

From the first congruence, we see that x is divisible by 2. From the second, we see that x is also divisible by 5. Thus x is divisible by 10, or $\boxed{x \equiv 0 \pmod{10}}$.

This problem was quite easy. Let's try a harder one.

23.2 Problem 2

23.2.1 Problem

Find all possible values of x such that

$$\begin{aligned} x &\equiv 1 \pmod{3} \\ x &\equiv 0 \pmod{7} \end{aligned}$$

23.2.2 Solution

From the second congruence, we see that x is divisible by 7. We list the first few nonnegative multiples of 7.

$$7, 14, 21, 28, 35, 42, 49, 56, 63, 70, \ldots$$

We now list all integers in that list that have a remainder of 1 when divided by 3. They are

$$7, 28, 49, 70, \ldots$$

All these terms differ by lcm[3, 7], or 21. Thus $x \equiv 7 \pmod{21}$.

However, we are *guessing* this is the solution. We write $x \equiv 7 \pmod{21}$ algebraically as

$$x = 21y + 7$$

where y is an integer. Since $21y + 7 \equiv 0 \pmod{7}$ and $21y + 7 \equiv 1 \pmod{3}$, we see that

$$\boxed{x \equiv 7 \pmod{21}}.$$

23.3 Problem 3

23.3.1 Problem

Find all x such that

$$x \equiv 3 \pmod 4$$
$$x \equiv 2 \pmod 7.$$

23.3.2 Solution

This problem would be hard to solve using the method in the previous problem. We need a systematic way to solve this.

The first congruence tell us that $x \equiv 3 \pmod 4$. We write this algebraically as

$$x = 4a + 3,$$

where a is an integer.

The second congruence tells us that $x \equiv 2 \pmod 7$. We write this algebraically as

$$x = 7b + 2,$$

where b is an integer.

Thus, we have to system of equations:

$$x = 4a + 3 = 7b + 2.$$

We rearrange the equation as $4a + 1 = 7b$, and mod 7 to get

$$4a + 1 \equiv 0 \pmod 7.$$

We subtract 1 from both sides of this congruence, and get

$$4a \equiv -1 \pmod 7 \implies 4a \equiv 6 \pmod 7.$$

We multiply the congruence by the inverse of 4 (mod 7), which is 2. Thus, we have

$$4a \equiv 6 \pmod 7$$
$$2 \times 4a \equiv 2 \times 6 \pmod 7$$
$$8a \equiv 12 \pmod 7$$
$$8a \equiv 5 \pmod 7$$
$$1a \equiv 5 \pmod 7$$
$$a \equiv 5 \pmod 7.$$

We substitute $a = 5$ into the equation $x = 4a + 3 = 7b + 2$, and get $x = 23$. However this is not the only solution, because we expect the solution to be a congruence.

Since

$$23 \equiv 3 \pmod 4$$
$$23 \equiv 2 \pmod 7$$

we subtract 23 from both sides of the congruences:

$$x - 23 \equiv 3 - 3 \equiv 0 \pmod 4$$
$$x - 23 \equiv 2 - 2 \equiv 0 \pmod 7.$$

From this, we see that $x - 23$ is divisible by both 4 and 7, which are relatively prime, so $x - 23 \equiv 0 \pmod{28}$. Thus, all values of x that satisfy the congruence are

$$\boxed{x \equiv 23 \pmod{28}}.$$

24 Harder Systems of Linear Congruences

24.1 Problem 1

24.1.1 Problem

Find all x such that

$$\begin{aligned} x &\equiv 1 \pmod 2 \\ x &\equiv 2 \pmod 3 \\ x &\equiv 0 \pmod 5. \end{aligned}$$

24.1.2 Solution

We know that the solution to a system of two linear congruences is another congruence. If we take two congruences and solve them, we get a single congruence. We can then combine this congruence with the third remaining congruence, thus solving the whole system.

We begin by finding all x such that

$$\begin{aligned} x &\equiv 1 \pmod 2 \\ x &\equiv 2 \pmod 3. \end{aligned}$$

Turning these into an algebraic form, we have

$$x = 2a + 1 = 3x + 2.$$

We rearrange to get $3x = 2a - 1$, and take the modulo 3, and get

$$2a - 1 \equiv 0 \pmod 3.$$

We solve for a in this congruence by adding 1 to both sides and multiplying by the inverse of 2 (mod 3), which is 2. Thus, we have

$$\begin{aligned} 2a - 1 &\equiv 0 \pmod 3 \\ 2a &\equiv 1 \pmod 3 \\ 2 \times 2a &\equiv 2 \times 1 \pmod 3 \\ 4a &\equiv 2 \pmod 3 \\ 1a &\equiv 2 \pmod 3 \\ a &\equiv 2 \pmod 3. \end{aligned}$$

Substituting $a = 2$ into $x = 2a + 1 = 3x + 2$ we have $x = 5$. Thus,

$$\begin{aligned} 5 &\equiv 1 \pmod 2 \\ 5 &\equiv 2 \pmod 3. \end{aligned}$$

Subtracting 5 from the congruences, we have

$$\begin{aligned} x - 5 &\equiv 1 - 1 \equiv 0 \pmod 2 \\ x - 5 &\equiv 2 - 2 \equiv 0 \pmod 3. \end{aligned}$$

Thus, $x - 5$ is a multiple of both 2 and 3, and because $\gcd(2, 3) = 1$, we have $x - 5 \equiv 0 \pmod 6 \implies x \equiv 5 \pmod 6$.

Now we have the following system of congruences:

$$\begin{aligned} x &\equiv 5 \pmod 6 \\ x &\equiv 0 \pmod 5. \end{aligned}$$

We list the first few multiples of 5:

$$5, 10, 15, 20, 25, 30, 35, 40, 45, 50, 55, 60, 65, 70, \ldots$$

We see that $5, 35, 65 \cdots$ are congruent to 5 (mod 6). These differ by 30, so we see that $x \equiv 5 \pmod{30}$. However, we need to check our solution. Writing $x \equiv 5 \pmod{3}0$ into an algebraic form ($x = 30a + 5$), and taking the mod 5 and mod 6, we have

$$\begin{aligned} 30a + 5 &\equiv 0 \pmod{5} \\ 30a + 5 &\equiv 5 \pmod{6}. \end{aligned}$$

Therefore, all x such that satisfy

$$\begin{aligned} x &\equiv 1 \pmod{2} \\ x &\equiv 2 \pmod{3} \\ x &\equiv 0 \pmod{5}. \end{aligned}$$

are

$$x \equiv 5 \pmod{30}.$$

25 Chinese Remainder Theorem

We start with a problem as usual.

25.1 Problem

25.1.1 Problem

Find all integers x such that

$$\begin{aligned} x &\equiv 1 \pmod{10}, \\ x &\equiv 4 \pmod{12}. \end{aligned}$$

25.1.2 Solution

We write the equations in an algebraic form, and get

$$x = 10a + 1 = 12b + 4.$$

We rearrange, and get

$$10a = 12b + 3.$$

However, one side of this equation is even, and the other is odd. Thus, this system has no solutions for x.

Combining earlier results, we see the following:

$$\begin{aligned} &\begin{cases} x \equiv 0 \pmod{2}, \\ x \equiv 0 \pmod{5} \end{cases} && \Rightarrow && x \equiv 0 \pmod{10} \\ &\begin{cases} x \equiv 1 \pmod{3}, \\ x \equiv 0 \pmod{7} \end{cases} && \Rightarrow && x \equiv 7 \pmod{21} \\ &\begin{cases} x \equiv 3 \pmod{4}, \\ x \equiv 2 \pmod{7} \end{cases} && \Rightarrow && x \equiv 23 \pmod{28} \\ &\begin{cases} x \equiv 1 \pmod{10}, \\ x \equiv 4 \pmod{12} \end{cases} && \Rightarrow && \text{no solutions} \end{aligned}$$

We can see that the GCD of the first 3 systems moduli are relatively prime, and the fourth are not. This gives the following result:

25.2 Chinese Remainder Theorem

The **Chinese Remainder Theorem** states that where m and n are relatively prime integers, then the system of congruences

$$\begin{aligned} x &\equiv a \pmod{m}, \\ x &\equiv b \pmod{n} \end{aligned}$$

always has a solution in integers x. Furthermore, the solution is of the form $x \equiv c \pmod{mn}$.

26 Exercises

26.1 Exercise 1

Find all x such that

$$\begin{aligned} x &\equiv 3 \pmod{4} \\ x &\equiv 5 \pmod{9}. \end{aligned}$$

26.2 Exercise 2

Find all x such that

$$\begin{aligned} x - 3 &\equiv 4 \pmod{2} \\ 4x + 2 &\equiv 0 \pmod{5}. \end{aligned}$$

26.3 Exercise 3

Find the smallest possible positive value of n such that

$$\begin{aligned} n &\equiv 4 \pmod{5} \\ n &\equiv 3 \pmod{6} \\ n &\equiv 2 \pmod{7}. \end{aligned}$$

Part XII
Problems

27 Problem 1: 2014 AMC8

The 7-digit numbers $\underline{74A52B1}$ and $\underline{326AB4C}$ are each multiples of 3. What is the smallest possible value of C?

28 Problem 2: 2010 AIME I

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

29 Problem 3: 2010 AMC 10B

Positive integers a, b, and c are randomly and independently selected with replacement from the set $\{1, 2, 3, \ldots, 2010\}$. What is the probability that $abc + ab + a$ is divisible by 3?

30 Problem 4: 2010 AMC 12A

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

31 Problem 5: 1995 AHSME

Consider the triangular array of numbers with 0,1,2,3,... along the sides and interior numbers obtained by adding the two adjacent numbers in the previous row. Rows 1 through 6 are shown.

$$\begin{array}{ccccccccccc}
 & & & & 0 & & & & & & \\
 & & & 1 & & 1 & & & & & \\
 & & 2 & & 2 & & 2 & & & & \\
 & 3 & & 4 & & 4 & & 3 & & & \\
4 & & 7 & & 8 & & 7 & & 4 & & \\
5 & 11 & & 15 & & 15 & & 11 & & 5 &
\end{array}$$

Let $f(n)$ denote the sum of the numbers in row n. What is the remainder when $f(100)$ is divided by 100?

32 Problem 6: 1999 AMC8

What is the remainder when 1999^{2000} is divided by 5?

33 Problem 7: 2009 AMC 10B

What is the remainder when $3^0 + 3^1 + 3^2 + \ldots + 3^{2009}$ is divided by 8?

34 Problem 8: 2013 USAJMO

Are there integers a and b such that $a^5b + 3$ and $ab^5 + 3$ are both perfect cubes of integers?

Part XIII
Solutions

In this part we have solutions to all the exercises in this manual.

35 Part II Exercises

35.1 Exercise 1

Remember that for integers a and b, $a \equiv b \pmod{m}$ if and only if $a - b$ is a multiple of m. $31 - 24 = 7$, and 7 is not divisible by 9. Thus

$$31 \not\equiv 24 \pmod{9}.$$

35.2 Exercise 2

As before, we see if $45 - 15$ is divisible by 3. Since $45 - 15 = 30$, and $30 = 3 \cdot 10$,

$$45 \equiv 15 \pmod{3}.$$

36 Part III Exercises

36.1 Exercise 1

1. $11 \equiv \boxed{2} \pmod 9$.
2. $45 \equiv \boxed{0} \pmod 9$.
3. $23 \equiv \boxed{5} \pmod 9$.
4. $434 \equiv \boxed{2} \pmod 9$.
5. $42 \equiv \boxed{6} \pmod 9$.
6. $1337 \equiv \boxed{5} \pmod 9$.

36.2 Exercise 2

1. $43 = 3 \cdot 14 + 1$.
2. $4 = 3 \cdot 1 + 1$.
3. $100 = 3 \cdot 33 + 1$.
4. $98 = 3 \cdot 32 + 2$.
5. $42 = 3 \cdot 14 + 0$.
6. $-34 = 3 \cdot (-12) + 2$.
7. $1337 = 3 \cdot 445 + 2$.

36.3 Exercise 3

36.3.1 Solution 1

Since $x \equiv y \pmod a$, we have $x - y = am$ for some integer m. Since $y \equiv z \pmod a$, we have $y - z = an$ for some integer n. Adding these equations, we get

$$\begin{aligned}(x-y)+(y-z) &= am + an \\ x + (-y+y) - z &= a(m+n) \\ x - z &= a(m+n).\end{aligned}$$

Since $m + n$ is an integer, $x - z$ is a multiple of a. Thus, $x \equiv z \pmod a$.

36.3.2 Solution 2

Since $x \equiv y \pmod a$, x and y share the same column of a a-column counting grid since x and y have the same residue. Similarly, $y \equiv z \pmod a$, so y and c are also in the same column. This column has x, y, and z, so $x \equiv z \pmod a$.

37 Part IV Exercises

37.1 Exercise 1

$$\begin{aligned} 54 + 42 &\equiv 2 + 14 \pmod 8 \\ 6 + 2 &\equiv 2 + 6 \pmod 8 \\ 0 &\equiv 0 \pmod 8. \end{aligned}$$

Thus, $54 + 42 \equiv 2 + 14 \pmod 8$.

37.2 Exercise 2

$$\begin{aligned} 69 - 45 &\equiv 18 - 15 \pmod 3 \\ 0 - 0 &\equiv 0 - 0 \pmod 3 \\ 0 &\equiv 0 \pmod 3. \end{aligned}$$

Thus, $69 + 45 \equiv 18 + 15 \pmod 8$.

37.3 Exercise 3

The remainder when $a + b + c$ is divided by 8 is the modulo-8 residue of $a + b + c$. We sum the modulo-8 residues of a, b, and c:

$$a + b + c \equiv 4 + 5 + 7 \equiv 16 \equiv \boxed{0} \pmod 8.$$

38 Part V Exercises

38.1 Exercise 1

$$\begin{aligned} 9 \cdot 43 &\equiv 8 \cdot 98 \pmod{23} \\ 9 \cdot 20 &\equiv 8 \cdot 6 \pmod{23} \end{aligned}$$

Thus, we have

$$\begin{aligned} 9 &\equiv 8 \pmod{23} \\ 20 &\equiv 6 \pmod{23}, \end{aligned}$$

neither of which is true. Thus $9 \cdot 43 \not\equiv 8 \cdot 98 \pmod{23}$.

38.2 Exercise 2

$100! = 100 \cdot 99! \equiv 0 \cdot 99! \equiv \boxed{0} \pmod 4$.

38.3 Exercise 3

The product of three integers are congruent modulo 8 to the product of the modulo 8 residues of the three integers. Multiplying, we have

$$1 \cdot 4 \cdot 7 \equiv 28 \equiv \boxed{4} \pmod 8.$$

39 Part VI Exercises

39.1 Exercise 1

We add 15^{14} to both sides of the congruence, and get

$$24^{14} \equiv 15^{14} \pmod 9.$$

From the law for modular exponentiation we have $24 \equiv 15 \pmod 9 \implies 9 \equiv 0 \pmod 9$. Thus $24^{14} - 15^{14}$ is divisible by 9.

39.2 Exercise 2

Since $5^6 = 1 \pmod 7$, we split 5^{6001} into as many powers of 5^6 as possible:

$$5^{6001} = 5^1 \cdot 5^{6000} = 5^1 \cdot (5^6)^{1000} \equiv 5 \cdot 1^{1000} \equiv 5 \cdot 1 \equiv \boxed{5} \pmod 7.$$

40 Part VIII Exercises

40.1 Exercise 1

Since $\gcd(6, 25) = 1$, $6 \pmod{25}$ has an inverse.

40.2 Exercise 2

Let n be an integer such that $0 \leq n < 20$. In order for n to have a residue modulo 20, $\gcd(n, 20)$ must be 1. Listing all integers less than 20 that are relatively prime to 20, we have

$$\{1, 3, 7, 9, 11, 13, 17, 19\}.$$

41 Part IX Exercises

41.1 Exercise 1

We list the first few integers that are equivalent to $1 \pmod 6$. They are

$$1, 7, 13, 19, 25, 31, 37, \ldots$$

Of these 25 is of the form $5x$, where $x = 5$. Thus the inverse of $5 \pmod 6$ is $\boxed{5}$.

41.2 Exercise 2

We turn this into the equation $19x + 21y = 1$, and solve for x using the Euclidean Algorithm.

$21 \div 19$ has a quotient of 1 and a remainder of 2. $19 \div 2$ has a quotient of 2 and a remainder of 1. This gives us the equations

$$21 = 1 \cdot 19 + 2$$
$$19 = 2 \cdot 9 + 1.$$

Rearranging, we get

$$2 = 21 - 1 \cdot 19$$
$$1 = 19 - 2 \cdot 9.$$

Substituting, we get

$$\begin{aligned} 1 &= 19 - 2 \cdot 9 \\ &= 19 - (21 - 1 \cdot 19) \cdot 9 \\ &= 19 - 21 \cdot 9 + 19 \cdot 9 \\ &= 10 \cdot 19 - 9 \cdot 21 \end{aligned}$$

Thus $x = \boxed{10}$.

41.3 Exercise 3

We turn this into the equation $17x + 23y = 1$, and solve for x.

$23 \div 17$ has a quotient of 1 and a remainder of 6. $17 \div 6$ has a quotient of 2 and a remainder of 5. $6 \div 5$ has a quotient of 1 and a remainder of 1. This gives us the following equations:

$$\begin{aligned} 23 &= 1 \cdot 17 + 6 \\ 17 &= 2 \cdot 6 + 5 \\ 6 &= 1 \cdot 5 + 1. \end{aligned}$$

Isolating the remainders, we get

$$\begin{aligned} 6 &= 23 - 1 \cdot 17 \\ 5 &= 17 - 2 \cdot 6 \\ 1 &= 6 - 1 \cdot 5. \end{aligned}$$

We substitute, and work our way up the list. Finally, we get $-4 \cdot 17 + 3 \cdot 23$. Reducing modulo 23, we get $-4 \cdot 17 \equiv 1 \pmod{23} \implies 19 \cdot 17 \equiv 1 \pmod{23}$. Thus $x = \boxed{19}$.

42 Part X Exercises

42.1 Exercise 1

We multiply $23x \equiv 14 \pmod{15}$ by the inverse of $23 \pmod{15}$, which is 2. Multiplying, we get

$$\begin{aligned} 23x &\equiv 14 \pmod{15} \\ 2 \cdot 23x &\equiv 2 \cdot 14 \pmod{15} \\ 1x &\equiv 28 \pmod{15} \\ x &\equiv 28 \pmod{15} \\ x &\equiv 13 \pmod{15}. \end{aligned}$$

42.2 Exercise 2

We subtract 234 from both sides, and simplify modulo 15.

$$\begin{aligned} 23x + 234 &\equiv 12 \pmod{15} \\ 23x + 234 - 234 &\equiv 12 - 234 \pmod{15} \\ 23x &\equiv -22 \pmod{15} \\ 23x &\equiv 3 \pmod{15}. \end{aligned}$$

We multiply by the inverse of $23 \pmod{15}$, and get

$$\boxed{x \equiv 6 \pmod{5}}.$$

42.3 Exercise 3

We have $ay - by = myn$, where n is an integer. Diving by y, we get

$$a - b = mn \implies a \equiv b \pmod{m}.$$

This is useful for congruences where a, b, and m have a common divisor.

43 Part XI Exercises

43.1 Exercise 1

Converting into an algebraic form, we get

$$x = 4a + 3 = 9b + 5.$$

Rearranging, we get $4a = 9b + 2$. Taking this equation modulo 4, we get $9b + 2 \equiv 0 \pmod{4}$. We subtract 2 from both sides, and get

$$9b \equiv -2 \pmod{4} \implies 9b \equiv 2 \pmod{4}.$$

Since $9 \equiv 1 \pmod{4}$, we have $b \equiv 2 \pmod{4}$. We substitute b as 2 into $x = 9b + 5$, and solve for x:

$$x = 9 \cdot 2 + 5 = 18 + 5 = 23.$$

Since

$$\begin{aligned} 23 &\equiv 3 \pmod{4} \\ 23 &\equiv 5 \pmod{9}, \end{aligned}$$

we subtract 23 from both congruences:

$$\begin{aligned} x - 23 &\equiv 3 - 3 \equiv 0 \pmod{4} \\ x - 23 &\equiv 5 - 5 \equiv 0 \pmod{9}. \end{aligned}$$

Since $x - 23$ is divisible by 4 and 9, which are relatively prime,

$$\boxed{x \equiv 23 \pmod{36}}.$$

43.2 Exercise 3

We begin by isolating x in each of the congruences. In the first congruence, we add 3 to both sides, and simplify. Thus, $x \equiv 1 \pmod{2}$.

In the second equation, we subtract 2 from both sides, and get $4x \equiv 3 \pmod{5}$. Then we multiply by the inverse of 4 modulo 5, which is 4. Thus, we have $x \equiv 2 \pmod{5}$.

Now we have system

$$\begin{aligned} x &\equiv 1 \pmod{2} \\ x &\equiv 2 \pmod{5}. \end{aligned}$$

Rewriting this as in an algebraic form, we get

$$x = 2a + 1 = 5b + 2.$$

We subtract 1 from both sides, and get $2a = 5b + 1$. Taking the equation modulo 2, we get

$$5b + 1 \equiv 0 \pmod{2} \implies 5b \equiv -1 \pmod{2} \implies 5b \equiv 1 \pmod{2}.$$

Since $5 \equiv 1 \pmod 2$, we have

$$b \equiv 1 \pmod 2.$$

We substitute $b = 1$ into $x = 5b + 2$, and solve for x:

$$x = 5 \cdot 1 + 2 = 7.$$

Subtracting 7 from the congruences

$$\begin{aligned} x &\equiv 1 \pmod 2 \\ x &\equiv 2 \pmod 5. \end{aligned}$$

We get

$$\begin{aligned} x - 7 &\equiv 0 \pmod 2 \\ x - 7 &\equiv 0 \pmod 5. \end{aligned}$$

Thus, since $\gcd(2, 5) = 1$, we have

$$x - 7 \equiv 0 \pmod{10} \implies \boxed{x \equiv 7 \pmod{10}}.$$

43.3 Exercise 3

We begin by solving the first two congruences, which will create another congruence as the solution. We have

$$x = 5a + 4 = 6b + 3.$$

Subtracting 3 from all sides and reducing modulo 6, we have

$$5a + 1 \equiv 0 \pmod 6 \implies 5a \equiv -1 \pmod 6 \implies 5a \equiv 5 \pmod 6.$$

Multiplying by 5^{-1} (which is 5), we have

$$a \equiv 1 \pmod 6.$$

We substitute $a = 1$ into $x = 5a + 4 = 6b + 3$, and get $x = 9$. Since $\gcd(5, 6) = 1$, we have

$$x \equiv 9 \pmod{30}.$$

Now we have the system

$$\begin{aligned} x &\equiv 9 \pmod{30} \\ x &\equiv 2 \pmod 7. \end{aligned}$$

Algebraically, we can express this as $x = 7a + 2 = 30b + 9$. Rearranging we get

$$7a = 30b + 7,$$

and reducing modulo 7, we have

$$30b + 7 \equiv 0 \pmod 7.$$

Subtracting 7 from both sides and simplifying, we have

$$30b \equiv -7 \pmod 7 \implies 2b \equiv 0 \pmod 7.$$

We multiply by $2^{-1} = 4$, and get $b \equiv 0 \pmod 7$. Substituting $x = 0$ into $x = 7a + 2 = 30b + 9$, we get $x = 9$. Since $\gcd(7, 30) = 1$, we have

$$x \equiv 9 \pmod{210}.$$

The smallest positive integer that satisfies this is $x = \boxed{9}$.

44 Part XII Exercises

44.1 Solution to Problem 1

The sum of a number's digits $\mod 3$ is congruent to the number $\pmod 3$. $74A52B1 \mod 3$ must be congruent to 0, since it is divisible by 3. Therefore, $7+4+A+5+2+B+1 \mod 3$ is also congruent to 0. $7+4+5+2+1 \equiv 1 \pmod 3$, so $A+B \equiv 2 \pmod 3$. As we know, $326AB4C \equiv 0 \pmod 3$, so $3+2+6+A+B+4+C = 15+A+B+C \equiv 0 \pmod 3$, and therefore $A+B+C \equiv 0 \pmod 3$. We can substitute 2 for $A+B$, so $2+C \equiv 0 \pmod 3$, and therefore $C \equiv 1 \pmod 3$. The smallest number that satisfies the is $\boxed{1}$.
Solution from the AoPS Wiki.

44.2 Solution to Problem 2

Note that $999 \equiv 9999 \equiv \cdots \equiv \underbrace{99\cdots9}_{999\ 9\text{'s}} \equiv -1 \pmod{1000}$. That is a total of $999-3+1 = 997$ integers, so all those integers multiplied out are congruent to $-1 \pmod{1000}$. Thus, the entire expression is congruent to $(-1)(9)(99) = -891 \equiv \boxed{109} \pmod{1000}$.
Solution from the AoPS Wiki.

44.3 Solution to Problem 3

First we factor $abc+ab+a$ as $a(bc+b+1)$, so in order for the number to be divisible by 3, either a is divisible by 3, or $bc+b+1$ is divisible by 3.

We see that a is divisible by 3 with probability $\frac{1}{3}$. We only need to calculate the probability that $bc+b+1$ is divisible by 3.

We need $bc+b+1 \equiv 0 \pmod 3$ or $b(c+1) \equiv 2 \pmod 3$. Using some modular arithmetic, $b \equiv 2 \pmod 3$ and $c \equiv 0 \pmod 3$ or $b \equiv 1 \pmod 3$ and $c \equiv 1 \pmod 3$. The both cases happen with probability $\frac{1}{3} * \frac{1}{3} = \frac{1}{9}$ so the total probability is $\frac{2}{9}$.

Then the answer is $\frac{1}{3} + \frac{2}{3} \cdot \frac{2}{9} = \boxed{\frac{13}{27}}$.
Solution from the AoPS Wiki.

44.4 Solution to Problem 4

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 $N \pmod{100}$. If instead we find $N \pmod{25}$, we know that $N \pmod{100}$, what we are looking for, could be $N \pmod{25}$, $N \pmod{25}+25$, $N \pmod{25}+50$, or $N \pmod{25}+75$. Only one of these numbers will be a multiple of four, and whichever one that is will be the answer, because $N \pmod{100}$ has to be a multiple of 4.

If we divide N by 5^{21} by taking out all the factors of 5 in N, we can write N as $\frac{M}{2^{21}}$ where

$$M = 1 \cdot 2 \cdot 3 \cdot 4 \cdot 1 \cdot 6 \cdot 7 \cdot 8 \cdot 9 \cdot 2 \cdots 89 \cdot 18,$$

where every multiple of 5 is replaced by the number with all its factors of 5 removed. Specifically, every number in the form $5n$ is replaced by n, and every number in the form $25n$ is replaced by n.

The number M can be grouped as follows:

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

Where the first line is composed of the numbers in 90! that aren't multiples of five, the second line is the multiples of five and not 25 after they have been divided by five, and the third line is multiples of 25 after they have been divided by 25.

Using the identity at the beginning of the solution, 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 $2^{10} = 1024 \equiv -1 \pmod{25}$ (or simply the fact that $2^{21} = 2097152$ if you have your powers of 2 memorized), we can deduce that $2^{21} \equiv 2 \pmod{25}$. Therefore $N = \frac{M}{2^{21}} \equiv \frac{24}{2} \pmod{25} = 12 \pmod{25}$.

Solution from the AoPS Wiki

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

44.5 Solution to Problem 5

We sum the first few rows: $0, 2, 6, 14, 30, 62$. They are each two less than a power of 2, so we try to prove it:

Let the sum of row n be S_n. To generate the next row, we add consecutive numbers. So we double the row, subtract twice the end numbers, then add twice the end numbers and add two. That makes $S_{n+1} = 2S_n - 2(n-1) + 2(n-1) + 2 = 2S_n + 2$. If S_n is two less than a power of 2, then it is in the form $2^x - 2$. $S_{n+1} = 2^{x+1} - 4 + 2 = 2^{x+1} - 2$.

Since the first row is two less than a power of 2, all the rest are. Since the sum of the elements of row 1 is $2^1 - 2$, the sum of the numbers in row n is $2^n - 2$. Thus, using Modular arithmetic, $f(100) = 2^{100} - 2 \bmod 100$. $2^{10} = 1024$, so $2^{100} - 2 \equiv 24^{10} - 2 \equiv (2^3\cdot 3)^{10} - 2 \equiv 1024^3\cdot 81\cdot 81\cdot 9 - 2 \equiv 24^3\cdot 19^2\cdot 9 - 2 \equiv \boxed{74} \bmod 100$.

Solution from the AoPS Wiki

44.6 Solution to Problem 6

Since $1999 \equiv -1 \pmod 5$, we have $1999^{2000} \equiv (-1)^{2000} \equiv \boxed{1} \pmod 5$.

44.7 Solution to Problem 7

44.7.1 Solution 1

The sum of any four consecutive powers of 3 is divisible by $3^0 + 3^1 + 3^2 + 3^3 = 40$ and hence is divisible by 8. Therefore

$$(3^2 + 3^3 + 3^4 + 3^5) + \cdots + (3^{2006} + 3^{2007} + 3^{2008} + 3^{2009})$$

is divisible by 8. So the required remainder is $3^0 + 3^1 = \boxed{4}$.

Solution from the AoPS Wiki.

44.7.2 Solution 2

e have $3^2 = 9 \equiv 1 \pmod 8$. Hence for any k we have $3^{2k} \equiv 1^k = 1 \pmod 8$, and then $3^{2k+1} = 3 \cdot 3^{2k} \equiv 3 \cdot 1 = 3 \pmod 8$.

Therefore our sum gives the same remainder modulo 8 as $1 + 3 + 1 + 3 + 1 + \cdots + 1 + 3$. There are 2010 terms in the sum, hence there are $2010/2 = 1005$ pairs $1 + 3$, and thus the sum is

$$1005 \cdot 4 = 4020 \equiv 20 \equiv \boxed{4} \pmod 8.$$

Solution from the AoPS Wiki.

44.8 Solution to Problem 8

No, such integers do not exist. This shall be proven by contradiction, by showing that if $a^5b + 3$ is a perfect cube then $ab^5 + 3$ cannot be.

Remark that perfect cubes are always congruent to 0, 1, or -1 modulo 9. Therefore, if $a^5b+3 \equiv 0, 1, \text{ or} -1 \pmod 9$, then $a^5b \equiv 5, 6, \text{ or } 7 \pmod 9$.

If $a^5b \equiv 6 \pmod 9$, then note that $3|b$. (This is because if $3|a$ then $a^5b \equiv 0 \pmod 9$.) Therefore $ab^5 \equiv 0 \pmod 9$ and $ab^5 + 3 \equiv 3 \pmod 9$, contradiction.

Otherwise, either $a^5b \equiv 5 \pmod 9$ or $a^5b \equiv 7 \pmod 9$. Note that since a^6b^6 is a perfect sixth power, and since neither a nor b contains a factor of 3, $a^6b^6 \equiv 1 \pmod 9$. If $a^5b \equiv 5 \pmod 9$, then

$$a^6b^6 \equiv (a^5b)(ab^5) \equiv 5ab^5 \equiv 1 \pmod 9 \implies ab^5 \equiv 2 \pmod 9.$$

Similarly, if $a^5b \equiv 7 \pmod 9$, then

$$a^6b^6 \equiv (a^5b)(ab^5) \equiv 7ab^5 \equiv 1 \pmod 9 \implies ab^5 \equiv 4 \pmod 9.$$

Therefore $ab^5 + 3 \equiv 5, 7 \pmod 9$, contradiction.

Therefore no such integers exist.

Solution from the AoPS Wiki.