The Art of Modular Arithmetic

Aryansh Shrivastava

A mathematician, like a painter or a poet, is a maker of patterns. If his patterns are more permanent than theirs, it is because they are made with ideas.

— G. H. Hardy, *A Mathematician's Apology*

Contents

0 Preface

> The sun himself is weak when he first rises, and gathers strength and courage as the day gets on.
>
> — Charles Dickens, *The Old Curiosity Shop*

§ 0.1 Purpose

Modular arithmetic, a cornerstone of numerous disciplines, reformulates arithmetic to leverage the raw properties of numbers. This exposition takes the nontraditional approach of teaching the subject from the perspective of math competitions such as the American Math Competitions (AMC) series[1], favoring intuition over formalism. It will appeal to both the mathematician and the applied scientist. And to anyone looking for a challenge.

§ 0.2 Notation

Though most notation is standard or introduced in-text, you should be familiar with the following specialized notation.

Notation	Definition
$\mathbb{Z}^C$ for some constraint C	the set all integers satisfying C (e.g., $\mathbb{Z}^+$ denotes the set of all positive integers)
$[a,b]$ for $a,b \in \mathbb{Z}^{\geq 0}$	the least common multiple (LCM) of a and b
(a,b) for $a,b \in \mathbb{Z}^{\geq 0}$	the greatest common divisor (GCD) of a and b, where $(0,0)$ is undefined
$\lfloor x \rfloor$ and $\lceil x \rceil$ for $x \in \mathbb{R}$	the floor (greatest integer less than or equal to) and ceiling (least integer greater than or equal to) functions of x, respectively

§ 0.3 Appetizer

Throughout this book, you will be guided by examples to experience discoveries firsthand[2], not fed results directly. The problems below establish a baseline for the prerequisite skills to understand these examples. Solve them to ensure you are ready to proceed[3].

Problem 1: What is the largest positive integer that divides 40 and 78? What about the smallest positive integer divisible by 40 and 78?

[1] This is the series of tests used to select the U.S. team for the International Mathematical Olympiad, among the valuable sources for the externally-sourced problems. All sources will be credited appropriately.

[2] There is an honor code for you to follow. Do not memorize the formulas presented. Instead, perform the thought experiments and make your best attempts at the examples and problems to build intuition. Read fragments of the presented solutions if you find yourself stuck, or ask a friend. If all else fails, consult the full solution and fill in the gaps. Only then will you see the true beauty in the math.

[3] All problems presented, including those below, have their solutions in the back of the book. Examples, exercises included to introduce concepts in-text, have their solutions immediately underneath for convenience.

Problem 2: A six place number is formed by repeating a three place number; for example, 256256 or 678678, etc. Find the GCD of all numbers of this form. (Source: 1959 AHSME #19)

Problem 3: One of the first 1234567 positive integers is chosen at random. Compute the probability that it is divisible by 3.

Problem 4: Find all integers x for which it can be said that the positive integer $2x + 9$ divides the positive integer $3x + 4$.

Problem 5: Prove that, for all primes p, the smallest positive integer whose factorial is divisible by p is p itself.

Problem 6: Find a closed form for the remainder of $a \div m$, where $a, m \in \mathbb{Z}^+$.[4]

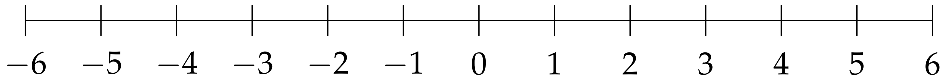
[4] Hint: Your answer should involve $\left\lfloor \frac{a}{m} \right\rfloor$.

1 Arithmetic—Modulo *m*

No facts are to me sacred; none are profane; I simply experiment, an endless seeker.
— Ralph Waldo Emerson, *Circles*

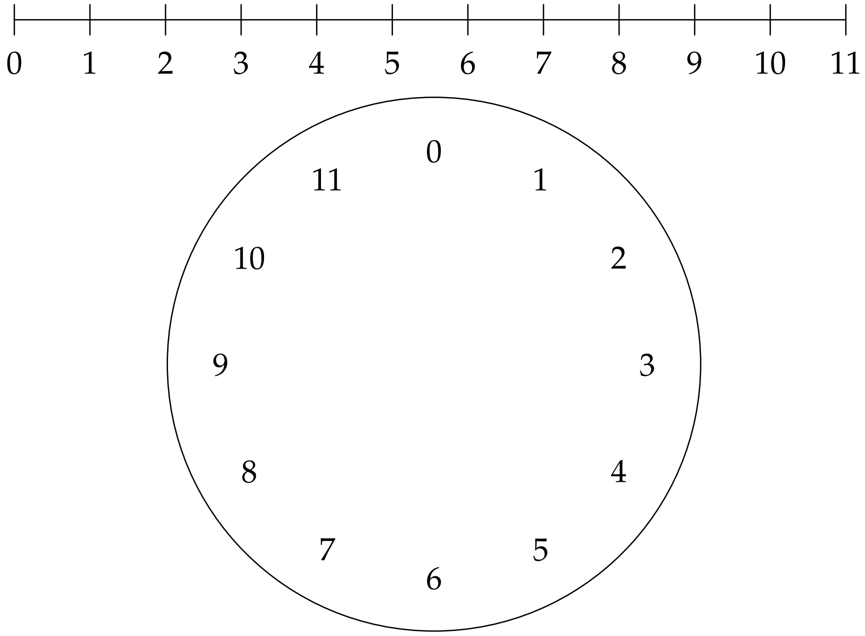
§ 1.1 A Thought Experiment

Imagine a number line.



As we're taught in school, we can count on this number line. Starting at 0, we can count up $1, 2, 3, 4, \ldots$ or down $-1, -2, -3, -4, \ldots$. Moreover, we can create a system of integer arithmetic out of movements on this number line. For instance, the sum $1 + 2 = 3$ can be interpreted as starting at the number 1 and moving two units to the right to 3.

But now imagine taking a piece of this number line and wrapping it around in a circle.



How could we count on this modified number line? Well, notice that this is almost the face of a clock, so we can imagine moving the hour hand! Because there are 12 hours on this clock, we say its **modulus** is 12. Starting at 0, we can count up clockwise $1, 2, 3, 4, \ldots$, but this time, after we reach 11, we loop back around to 0. Similarly, we can count down counterclockwise $11, 10, 9, 8, \ldots$, but when we reach 1, we loop back around to 0.

What about arithmetic? Wherever we start, if we ever move forward or backward by our 12-hour modulus, we end up exactly the same place we started. This enables us to create a system of integer arithmetic where an integer a corresponds to the time a hours after 0 (or $-a$ hours before 0 if $a < 0$).

Example 1: What hour on the clock does 2021 correspond to?

This question is asking us to start our hour hand at 0, move forward 2021 hours, and then determine the time. But like we said, for every 12-hour cycle we make, we end up back at 0. Effectively, we can divide our 2021 hours into 12-hour blocks until only r hours remain, where $0 \leq r \leq 11$. Then, our answer is just r (all that remains is to move forward r hours from 0).

To compute the answer r, we note that it is the remainder of the division $2021 \div 12$. Since $2021 \div 12 = 168\,\mathrm{R}\,5$, $r = \boxed{5}$. ■

Two integers a and b may be deemed "equal" in this system if they both correspond to the same hour on the clock. However, to prevent confusion when $a \neq b$ in standard arithmetic, we say that a and b are **congruent** and write this as $a \equiv b$. For example, because 2021, 17, and -19 all correspond to the same hour 5, we can write $2021 \equiv 17 \equiv -19 \equiv 5$.

§ 1.2 Generalization

Now, suppose we generalize the clock from our thought experiment to include m hours, 0 through $m-1$ for some $m \in \mathbb{Z}^{>1}$, so that m is now the modulus. We introduce some standard terminology.

First, we write the notion that two integers a and b correspond to the same hour on this general m-hour clock in **modular form** as

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

pronounced "a is congruent to b modulo m," where the $\pmod{m}$ **modular suffix** helps us keep track of the modulus m. This relation as a whole is known as a **modular congruence**.

In order to correspond to the same hour on the clock, a and b must differ by some whole number of m-hour cycles. That is, a and b differ by an integer multiple of m. This gives us an alternative **parametric form** to express the same notion:

$$a - b = mk;\, k \in \mathbb{Z}.$$

Lastly, the hour an integer a corresponds to on a modulus m clock, equivalently the remainder of the division $a \div m$, can be written in **modular remainder form** as

$$a \bmod m$$

(notice the omission of parentheses around the modular suffix) and is sometimes referred to as the **modular residue** of $a \pmod{m}$.

Example 2: Use modular definitions to justify $11 \equiv -3 \pmod{14}$. Convert the congruence into parametric form.

We have that $11 \equiv -3 \pmod{14}$ because $\boxed{\dfrac{11-(-3)}{14} = 1 \in \mathbb{Z}}$ by modular definition. In parametric form, this becomes $\boxed{11 - (-3) = (14)(1);\, 1 \in \mathbb{Z}}$. ■

You might be surprised to find that, even with the few tools derived thus far, we've unlocked the ability to solve new kinds of problems.

Problem 7: Claire adds the degree measures of the interior angles of a convex polygon and arrives at a sum of 2017. She then discovers that she forgot to include one angle. What is the degree measure of the forgotten angle? (Source: 2017 AMC 12A #11)

§ 1.3 Key Identities

To harness the power of any mathematical system, it is essential to establish its key identities. Fortunately, the key identities of modular arithmetic are not only intuitive but easy to formalize through conversion from modular form to parametric form and vice versa as we explore in the next example.

Example 3: For $a, b, A, B \in \mathbb{Z}$ and $m \in \mathbb{Z}^{>1}$, if $a \equiv A \pmod{m}$ and $b \equiv B \pmod{m}$, prove each of the following.

- $a + b \equiv A + B \pmod{m}$
- $ab \equiv AB \pmod{m}$
- $a^n \equiv A^n \pmod{m}$ for $n \in \mathbb{Z}^{\geq 0}$

Using parametric form, if all $k \in \mathbb{Z}$ and $a, A \pmod{m}$ have common modular residue r_a while $b, B \pmod{m}$ have common modular residue r_b, we can write

$$\begin{aligned} a &= mk_a + r_a & \qquad b &= mk_b + r_b \\ A &= mk_A + r_a & \qquad B &= mk_B + r_b \end{aligned}$$

It follows that

$$(a + b) \bmod m = (A + B) \bmod m = (r_a + r_b) \bmod m$$
$$ab \bmod m = AB \bmod m = r_a r_b \bmod m,$$

proving the first two identities. For the third identity, the congruence reduces to the trivial $1 \equiv 1 \pmod{m}$ if $n = 0$ and an n-time application of the second identity otherwise (seeing as positive integer exponentiation is repeated multiplication). ■

Example 4: Use the fact[1] that $89 \equiv -1 \pmod{90}$ to find the remainder when 89^{2021} is divided by 90.

Using our exponentiation identity, we have

$$89 \equiv -1 \pmod{90} \implies 89^{2021} \equiv (-1)^{2021} \equiv -1 \equiv \boxed{89} \pmod{90}.$$

■

[1] In case you haven't realized by now, negative numbers are really powerful and often help simplify the arithmetic part of modular arithmetic.

Problem 8: In year N, the 300th day of the year is a Tuesday. In year $N+1$, the 200th day is also a Tuesday. On what day of the week did the 100th day of the year $N-1$ occur?[2] (Source: 2000 AMC 10 #25)

Problem 9: If n and m are integers and $n^2 + m^2$ is even[3], which of the following is impossible? (Source: 2014 AMC 8 #13)
(A) n and m are even **(B)** n and m are odd **(C)** $n+m$ is even **(D)** $n+m$ is odd
(E) none of these are impossible

Problem 10: When the sum

$$(1 \cdot 2 \cdot 3) + (2 \cdot 3 \cdot 4) + (3 \cdot 4 \cdot 5) + \cdots + (2018 \cdot 2019 \cdot 2020)$$

is evaluated, what is the units digit[4] of the result?

Unfortunately, division does not work as you would expect in congruences. For example, $3 \equiv 6 \pmod 3$, but we can't divide both sides of the congruence by 3 to obtain $1 \equiv 2 \pmod 3$ as this is obviously false. In fact, most expositions stop here and insist it is a dead end. However, there is a way to make division work if we're careful...

§ 1.4 Resolving the Division Anomaly

Let's delve right in with an example. As with all examples, pause and try to make progress on your own before reading on. As a warning, however, the example below is particularly involved, so feel free to refer to parts of the solution whenever you feel irrevocably stuck.

Example 5: For $a, b, d, m \in \mathbb{Z}$ with $d \neq 0$ and $m > 1$, suppose $ad \equiv bd \pmod m$. Find a way to correctly divide the congruence by d to write a congruence between a and b.

We don't know how to divide in congruences, but we do know how to divide in equations! This motivates us to convert our relation $ad \equiv bd \pmod m$ from modular congruence form to parametric equation form and then divide by d, giving us the following for $k \in \mathbb{Z}$:

$$ad - bd = mk$$

$$a - b = \frac{mk}{d}$$

Since $a, b \in \mathbb{Z}$, $a - b = \dfrac{mk}{d} \in \mathbb{Z}$.
Consequently, d can be written as the product of two integer factors in the form $d_m d_k$, where $\dfrac{m}{d_m} \in \mathbb{Z}$ and $\dfrac{k}{d_k} \in \mathbb{Z}$. Plugging this form in and rearranging yields a key insight:

$$\frac{mk}{d} = \frac{m}{d_m}\frac{k}{d_k}$$

[2] Hint: The day of the week corresponding to a certain day is given by its modular residue $\pmod 7$ because there are 7 days in a week.

[3] Hint: Even or odd parity is given by the modular residue $\pmod 2$.

[4] Hint: The units digit of a number is its modular residue $\pmod{10}$.

$$\frac{\frac{mk}{d}}{\frac{m}{d_m}} = \frac{k}{d_k} \in \mathbb{Z}$$

Now, as we have both $\frac{m}{d_m} \in \mathbb{Z}$ and $\frac{d}{d_m} = d_k \in \mathbb{Z}$, we obtain $\frac{(m,d)}{d_m} \in \mathbb{Z}$, from which follows another key insight:

$$\frac{\frac{m}{d_m}}{\frac{m}{(m,d)}} \in \mathbb{Z}.$$

Finally, since two integers multiply to an integer, we obtain a third and final insight by multiplying our two insights together:

$$\frac{\frac{mk}{d}}{\frac{m}{d_m}} \frac{\frac{m}{d_m}}{\frac{m}{(m,d)}} = \frac{\frac{mk}{d}}{\frac{m}{(m,d)}} = \frac{a-b}{\frac{m}{(m,d)}} \in \mathbb{Z}$$

In modular form, this becomes $a - b \equiv 0 \left(\bmod \frac{m}{(m,d)}\right) \implies \boxed{a \equiv b \left(\bmod \frac{m}{(m,d)}\right)}$. ■

Problem 11: Al, Bob, and Carl each have favorite numbers so that the sum of Al and Bob's favorite numbers has a units digit of 2, the sum of Bob and Carl's favorite numbers has a units digit of 4, and the sum of Al and Carl's favorite numbers has a units digit of 0. If their favorite numbers are all positive integers, what is the sum of all possible values of the units digit of the sum of their three favorite numbers?

2 Revisiting Divisibility Rules

> If you have built castles in the air, your work need not be lost; that is where they should be. Now put the foundations under them.
>
> — Henry David Thoreau, *Walden*

§ 2.1 The Magic of the Decimal Representation

All of the divisibility rules you were taught (e.g., the canonical sum of the digits divisibility for 3) have their roots in modular arithmetic. Let's derive some of them.

First, as you may recall, a number we generally see in standard arithmetic is said to be in its **decimal representation**. This means it can be easily expressed as the sum of multiples of powers of 10. All we have to do is read the digits off one by one.

Example 6: Write 2021 as the sum of powers of 10.

$2021 = \boxed{2 \cdot 10^3 + 0 \cdot 10^2 + 2 \cdot 10^1 + 1 \cdot 10^0}.$ ■

In general, a number like $\underline{d_1 d_2 d_3 \ldots d_n}$, where all d denote digits, can be written as the sum

$$10^{n-1}d_1 + 10^{n-2}d_2 + 10^{n-3}d_3 + \cdots + 10^0 d_n.$$

This alone establishes many useful divisibility rules.

Example 7: For many $m \in \mathbb{Z}^{>1}$, the divisibility rule of m can be obtained by considering the modular residue of the general decimal representation above $\pmod{m}$. For $k \in \mathbb{Z}^{>0}$, discover the divisibility rules of 2^k, 3, 5^k, 9, 10^k, and 11.

Modulo $2^k, 5^k$, or 10^k, all terms $10^i d_{n-i}$ for $i \geq k$ vanish to 0, leaving only those with $0 \leq i < k$. Therefore, the divisibility rule for $2^k, 5^k$, and 10^k is to consider the modular residue of the last k digits. For example,

$$99987\textcolor{red}{96} \equiv \textcolor{red}{96} \equiv 0 \pmod{2^2}$$

$$99987\textcolor{red}{96} \equiv \textcolor{red}{96} \equiv 21 \pmod{5^2}$$

$$99987\textcolor{red}{96} \equiv \textcolor{red}{96} \equiv 96 \pmod{10^2}$$

Modulo 3 and 9, all terms $10^i d_{n-i} \equiv 1^i d_{n-i} \equiv d_{n-i}$. Therefore, the divisibility rule for 3 and 9 is to consider the modular residue of the sum of the digits. For example,

$$123456789 \equiv 1 + 2 + 3 + \cdots + 9 \equiv \frac{9 \cdot 10}{2} \equiv 0 \pmod{9}$$

$$1723103 \equiv 1 + 7 + 2 + 3 + 1 + 0 + 3 \equiv 17 \equiv 1 + 7 \equiv 2 \pmod{3}$$

Lastly, modulo 11, all terms $10^i d_{n-i}$ become $(-1)^i d_{n-i}$. Therefore, the divisibility rule for 11 is to consider the modular residue of the alternating difference/sum (strictly from right to left) of the digits. For example,

$$1315 \equiv 5 - 1 + 3 - 1 \equiv 6 \pmod{11}$$

■

Problem 12: Eleven members of the Middle School Math Club each paid the same integer amount for a guest speaker to talk about problem solving at their math club meeting. In all, they paid their guest speaker $\$\underline{1A2}$. What is the missing digit A of this 3-digit number? (Source: 2014 AMC 8 #8)

Problem 13: The 5-digit number $\underline{2}\ \underline{0}\ \underline{1}\ \underline{8}\ \underline{U}$ is divisible by 9. What is the remainder when this number is divided by 8? (Source: 2018 AMC 8 #7)

Problem 14: The digits 1, 2, 3, 4, and 5 are each used once to write a five-digit number $PQRST$. The three-digit number PQR is divisible by 4, the three-digit number QRS is divisible by 5, and the three-digit number RST is divisible by 3. What is P? (Source: 2016 AMC 8 #24)

Problem 15: 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 $S(n+1)$? (Source: 2017 AMC 10A #20, 12A #18)
(A) 1 **(B)** 3 **(C)** 12 **(D)** 1239 **(E)** 1265

Problem 16: Let $S(n)$ denote the sum of the digits of a positive integer n with two digits or more. The digital root of a number is found by applying the function S to the number repeatedly until a one-digit number is obtained. For example, the digital root of 1234567 is 1. Let $f(n)$ denote the square of the positive integer with n digits, all of whose digits are 1. For example, $f(4) = 1111^2$. What is the digital root of $f(1) + f(2) + \cdots + f(2018)$?

§ 2.2 Make Your Own

As useful as the fundamental divisibility rules are, you sometimes need to combine them. For instance, the divisibility rule for 12 is a combination of those for 3 and 4.[1] Other times, you have to start from scratch and make your own.

Example 8: To test a number for divisibility by 7, prove that it suffices to remove its final digit and then subtract twice this digit from whatever remains. For example, we can say 434 is divisible by 7 because $43 - 2(4) = 35$ is.

Suppose the number is n. Removing its final digit leaves $\left\lfloor \frac{n}{10} \right\rfloor$, so its final digit is $n - 10\left\lfloor \frac{n}{10} \right\rfloor$. We are asked to prove that if

$$\left\lfloor \frac{n}{10} \right\rfloor - 2\left(n - 10\left\lfloor \frac{n}{10} \right\rfloor\right) \equiv 0 \pmod{7},$$

[1] To find the exact residue in such a combination, we need to solve a system of linear congruences, which we will get to in a later chapter.

then $n \equiv 0 \pmod{7}$. Simplifying gives

$$21 \left\lfloor \frac{n}{10} \right\rfloor + 5n \equiv 0 \pmod{7},$$

But now, since $21 \equiv 0 \pmod{7}$, the first term vanishes, and we are left with $n \equiv 0 \pmod{7}$ after dividing by 5. ■

Problem 17: If we instead subtract three times the final digit from what remains, we obtain a divisibility test for a different prime. What is it? (Source: Mandelbrot)

3 Exponential Remainders

> To live, I must have faith. I must trust myself to the totally unknown.
> — Alan Watts, *Man and Nature*

§ 3.1 Inductive Reasoning

Many of the important problems modular arithmetic solves involve finding the remainders of notoriously large exponents that cannot be computed by hand. In many cases, you'll find that it is enough to find the first few exponents of the base to see how the modular residues cycle. You can then induct the cycle to pin down the desired residue.

Example 9: What is the units digit of 2^{2021}?

We proceed with inductive reasoning by looking at the modular residues of the first few powers of 2 modulo 10.

$$\begin{aligned} 2^1 &\equiv 2 \pmod{10} \\ 2^2 &\equiv 4 \pmod{10} \\ 2^3 &\equiv 8 \pmod{10} \\ 2^4 &\equiv 6 \pmod{10} \\ 2^5 &\equiv 2 \pmod{10} \end{aligned}$$

Aha! Our residues cycle as $2, 4, 8, 6, 2, 4, 8, 6, \ldots$. Because each cycle has length 4 (four residues are contained inside the cycle), the 2018th residue will have position $2018 \bmod 4 = 2$ in the cycle. Therefore, because all residues with position 2 in their respective cycle have value 4, our answer is $\boxed{4}$. ■

Problem 18: A number m is randomly selected from the set $\{11, 13, 15, 17, 19\}$, and a number n is randomly selected from $\{1999, 2000, 2001, \ldots, 2018\}$. What is the probability that m^n has a units digit of 1? (Source: 2018 AMC 10A #19)

§ 3.2 Euler's Totient Theorem

For $m \in \mathbb{Z}^{>1}$, Euler's totient function $\phi(m)$ counts the number of positive integers not exceeding m relatively prime to m. It turns out this is a very useful function for us in modular arithmetic. Let's see how.

Example 10: For $m \in \mathbb{Z}^{>1}$, suppose the prime factorization of m is $\prod\limits_{k=1}^{n} p_k^{e_k}$, where all p are its prime divisors and e their exponents. To find $\phi(m)$, we could just look at the GCD of m with each of the first m positive integers, but devise a faster way using this information.

Consider the set of the first m positive integers. Because m is evenly divisible by all its prime divisors p and this is a continuous range of integers, the residues modulo all p are evenly distributed in this set. Now, we must count how many numbers in this set are relatively prime to m. Imagine constructing one such number. To be relatively prime to m, it cannot be divisible by any of the prime divisors p. For a given p, due to the even distribution, exactly $\frac{1}{p}$ of the numbers in the set are divisible by p (in other words, 0 modulo p). Therefore, the other $1 - \frac{1}{p}$ of the numbers are not. Because all p are independent, the overall fraction of the numbers that are not divisible by any of the p is given by the product $\prod \left(1 - \frac{1}{p}\right)$. But this is exactly $\frac{\phi(m)}{m}$. Therefore, we have

$$\boxed{\phi(m) = m \prod_{k=1}^{n} \left(1 - \frac{1}{p_k}\right)}.$$

■

Example 11: Compute $\phi(12)$ in two ways.

The prime factorization of 12 is $2^2 \cdot 3$, so $\phi(12) = 12 \cdot \frac{1}{2} \cdot \frac{2}{3} = \boxed{4}$. However, $\phi(12)$ also counts the number of positive integers not exceeding 12 relatively prime to 12. There are also four of these, $1, 5, 7,$ and 11, as expected. ■

Example 12: What is $\phi(p)$ for prime p?

All positive integers less than p (and all positive integers in general) are relatively prime to p. Therefore, $\phi(p) = \boxed{p - 1}$. ■

Example 13: For $m \in \mathbb{Z}^{>1}$, prove that $a^{\phi(m)} \equiv 1 \pmod{m}$ for all integers a such that $(a, m) = 1$. This is known as **Euler's totient theorem**.

Throughout this problem, suppose we work using modular arithmetic $\pmod{m}$. There are exactly m residues $0, 1, 2, \ldots, m - 1$ in this system. However, by the definition of ϕ, only $\phi(m)$ of these residues are relatively prime to m. Let $\mathcal{S}_m = \{n_1, n_2, \ldots, n_{\phi(m)}\}$ denote this special set of $\phi(m)$ residues. Now, suppose we multiply all residues in this set by a and mod out to find the residues, producing a new set $a\mathcal{S}_m = \{an_1 \bmod m, an_2 \bmod m, \ldots, an_{\phi(m)} \bmod m\}$ of residues. The crucial claim is that $\mathcal{S}_m = a\mathcal{S}_m$. This is because all elements remained distinct and relatively prime to m before and after being multiplied by a (as $(a, m) = 1$), and there were exactly $\phi(m)$ of them before and after. Therefore, if we multiply all the elements in $\mathcal{S}_m$ and all the elements in $a\mathcal{S}_m$, the two products must be congruent $\pmod{m}$:

$$n_1 \cdot n_2 \cdots n_{\phi(m)} \equiv an_1 \cdot an_2 \cdots an_{\phi(m)}$$

$$n_1 n_2 \cdots n_{\phi(m)} \equiv a^{\phi(m)} n_1 n_2 \cdots n_{\phi(m)} \pmod{m}$$

Dividing both sides by $n_1 n_2 \cdots n_{\phi(m)}$ without affecting the modulus m as this number is relatively prime, we get

$$a^{\phi(m)} \equiv 1 \pmod{m}$$

as desired. ■

Example 14: For $m, b \in \mathbb{Z}^{>1}$, show that $a^b \equiv a^{b \mod \phi(m)} \pmod{m}$ for all integers a such that $(a, m) = 1$.

We can write $b = \phi(m) \left\lfloor \frac{b}{\phi(m)} \right\rfloor + b \mod \phi(m)$. Substituting this in and using Euler's totient theorem gives us

$$a^{\phi(m)\lfloor b/\phi(m) \rfloor + b \mod \phi(m)} \equiv \left(a^{\phi(m)}\right)^{\lfloor b/\phi(m) \rfloor} a^{b \mod \phi(m)} \equiv a^{b \mod \phi(m)} \pmod{m}$$

■

Problem 19: What is the remainder when 69^{354} is divided by 89?

Problem 20: 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? (Source: 2017 AMC 10B #14)

Problem 21: What are the last two digits in the decimal representation of $2011^{2012^{2013}}$?

4 Linear Congruences

> I saw it once, I have no doubt; but now can't place its whereabouts. I try to think it, time and time; but what it is, won't come to mind.
>
> — Lang Leav, *Déjà Vu*

§ 4.1 Alluding Back to the Basics

We commence with this section by alluding back to the preliminary algebra of solving a linear equation. The typical method to solve these was performing the exact same arithmetic operations to both sides of the equation.

Example 15: Solve $2x - 1 = 3$ for x.

This is just regular algebra.

- $2x - 1 = 3$ (Given)
- $2x = 4$ (Add 1 to both sides)
- $x = \boxed{2}$ (Divide both sides by 2, yielding the answer)

■

As you may expect, we can also solve linear congruences in a similar algebraic way. We must be careful that division does not work the normal way in modular arithmetic and numbers other than integers do not exist. Also, keep in mind that while each linear congruence has at most one modular solution, that solution describes a whole infinite class of integers (sometimes referred to as a **residue class**).

Example 16: Find the first three positive integers x such that $2x - 1 \equiv 5 \pmod{12}$.

Our approach is to find the modular solution to the congruence first and then find the first three positive integers based on that solution. Adding 1 to both sides gives us

$$2x \equiv 6 \pmod{12}.$$

Now, we can divide both sides by 2, remembering to divide the modulus by $(2, 12) = 2$.

$$x \equiv 3 \pmod{6}$$

The first three positive integers in the residue class $3 \pmod{6}$ are $\boxed{3, 9, 15}$. ■

§ 4.2 Modular Inverses and the Extended Euclidean Algorithm

For $a, b \in \mathbb{Z}^{+}$ and $m \in \mathbb{Z}^{>1}$, our current method solves a linear congruence of the form $ax \equiv b \pmod{m}$ by dividing both sides by a and the modulus by (a, m). Of course, there is no guarantee that $a|b$, so we may have to add multiples of m to our original b until $a|b$. But what if it takes a very long time to find a suitable b? What if there is no suitable b because the congruence has no solutions?

For this, we invent the concept of the modular inverse.

Example 17: Let $a, m \in \mathbb{Z}^+$ and $m > 1$. Prove that $ax \equiv 1 \pmod{m}$ has a solution if and only if $(a, m) = 1$.

Note that there are two directions, if and only if, and thus two parts to our proof.

Let's begin with the if part. If $(a, m) = 1$, by Euler's totient theorem, we have

$$a^{\phi(m)} \equiv 1 \pmod{m}$$

We can rewrite this as

$$aa^{\phi(m)-1} \equiv 1 \pmod{m},$$

so we have demonstrated the solution $x \equiv a^{\phi(m)-1} \pmod{m}$.

Let's move on to the only if part. Because we are more familiar with equations than congruences, we can rewrite this in parametric form with parameter $k \in \mathbb{Z}$:

$$ax - mk = 1$$

We now prove this has a solution only if $(a, m) = 1$ using a proof by contradiction. Assume for the sake of contradiction that this equation has a solution and $(a, m) = c$ for some $c \in \mathbb{Z}^{>1}$. Then, because $c|a$ and $c|m$, $c|(ax - mk)$. But this means $c|1$, which is impossible unless $c = 1$, so we arrive at a contradiction. ■

In general, we write the solution to $ax \equiv 1 \pmod{m}$ from the previous problem as $x \equiv a^{-1} \pmod{m}$ and say that a^{-1} is the **modular inverse** of $a \pmod{m}$.[1]

Example 18: Find $5^{-1} \pmod{6}$. Use this to solve the congruence $5x \equiv 3 \pmod{6}$ without the division method from before.

Because $(5, 6) = 1$, 5^{-1} exists and we can continue. 5^{-1} is the number we multiply by $5 \pmod{6}$ to produce $1 \pmod{6}$. However, $5 \equiv -1 \pmod{6}$, and because $(-1)(-1) \equiv 1 \pmod{6}$, we have $5^{-1} \equiv -1 \equiv 5 \pmod{6}$.[2]

Moving on to the congruence, we need some way to omit the 5 coefficient on the left without division. But remember, $5^{-1} \cdot 5 \equiv 1 \pmod{6}$, so we can just multiply both sides by 5^{-1}.

$$5^{-1} \cdot 5x \equiv 3 \cdot 5^{-1} \pmod{6}$$

$$x \equiv 3 \cdot 5^{-1} \pmod{6}$$

[1] a^{-1} is not a shorthand for $\frac{1}{a}$ like in regular arithmetic! Remember, only integers exist in modular arithmetic.

[2] This is yet another example of the power of negative numbers in modular arithmetic.

As we know, $5^{-1} \equiv 5 \pmod{6}$, so we can finish off.

$$x \equiv 3 \cdot 5 \equiv 15 \pmod{6} \implies \boxed{x \equiv 3 \pmod{6}}.$$

■

In the previous example, we were able to find the modular inverse by using a clever observation. Often, however, such a trick won't be obvious. For example, we don't yet have the tools to find $33^{-1} \pmod{667}$ efficiently without trial and error. We could write it as $33^{\phi(667)-1} = 33^{615}$ using Euler's totient theorem, but it turns out we actually have to calculate 154 exponentials before we find the residue cycle. We will learn a way to alleviate this problem when we discuss systems of linear congruences and the Chinese remainder theorem later on, but for now, we have an even better approach.

Example 19: Prove that, for $a, b \in \mathbb{Z}^{\geq 0}$ and $a > b$, $(a, b) = (a - b, b)$. Use this to in turn prove that $(a, b) = (a \mod b, b)$. This is known as **the extended Euclidean algorithm.**

For any divisor $m \in \mathbb{Z}^{>1}$, suppose m is a divisor of both $a - b$ and b. We can write

$$a - b \equiv 0 \pmod{m}$$

$$b \equiv 0 \pmod{m}$$

Adding these congruences gives $a \equiv 0 \pmod{m}$. Therefore, any common divisor of $a - b$ and b must also be a divisor of a. Similarly, if m is a common divisor of both a and b, we can write

$$a \equiv 0 \pmod{m}$$

$$b \equiv 0 \pmod{m}$$

Subtracting these gives $a - b \equiv 0 \pmod{m}$. Therefore, any common divisor of a and b must also be a divisor of $a - b$. Taken together, these facts imply that all common divisors of a and b are the same as all common divisors of $a - b$ and b. Therefore, the maximum divisor in each of these groups is also the same, giving us the desired

$$(a, b) = (a - b, b).$$

Because repeated subtraction becomes division, applying the result repeatedly gives the extended Euclidean algorithm

$$(a, b) = (a \mod b, b).$$

■

Example 20: Use the extended Euclidean algorithm repeatedly to show that $(33, 667) = 1$.

Because $a \mod b$ is the remainder of $a \div b$, we can write each step (a, b) in the form

$$a = \left\lfloor \frac{a}{b} \right\rfloor \underline{b} + \underline{a \mod b},$$

where the key parts are underlined so that the next step is $(b, a \mod b)$. We can stop as soon as the $a \mod b$ becomes 1. Doing so gives

$$\begin{aligned} 667 &= 20 \cdot \underline{33} + \underline{7} \\ 33 &= 4 \cdot \underline{7} + \underline{5} \\ 7 &= 1 \cdot \underline{5} + \underline{2} \\ 5 &= 2 \cdot \underline{2} + \underline{1} \end{aligned}$$

Therefore, the GCD is 1. ■

Example 21: Use the equations from the last example backwards to work out $33^{-1} \pmod{667}$.

In general, we know that since $(a, b) = 1$ whenever $a^{-1} \pmod{b}$ exists, the very final remainder (which gives the GCD) in our repeated applications of the extended Euclidean algorithm process must always be 1. Therefore, the overall process must always look like this for $c, d \in \mathbb{Z}^{>1}$:

$$\begin{aligned} &\vdots \\ c &= \left\lfloor \frac{c}{d} \right\rfloor \underline{d} + \underline{c \mod d} \\ d &= \left\lfloor \frac{d}{c \mod d} \right\rfloor \underline{(c \mod d)} + \underline{1} \end{aligned}$$

Note that we can rewrite these equations as

$$\begin{aligned} &\vdots \\ \underline{c \mod d} &= c - \left\lfloor \frac{c}{d} \right\rfloor \underline{d} \\ \underline{1} &= d - \left\lfloor \frac{d}{c \mod d} \right\rfloor \underline{(c \mod d)} \end{aligned}$$

But this means that we can perform repeated substitutions as we work from the bottom to the top! For instance, from the last two equations,

$$\begin{aligned} \underline{1} &= d - \left\lfloor \frac{d}{c \mod d} \right\rfloor \underline{(c \mod d)} \\ &= d - \left\lfloor \frac{d}{c \mod d} \right\rfloor \left(c - \left\lfloor \frac{c}{d} \right\rfloor \underline{d} \right) \\ &= \underline{d} \left(1 + \left\lfloor \frac{d}{c \mod d} \right\rfloor \left\lfloor \frac{c}{d} \right\rfloor \right) - c \left\lfloor \frac{d}{c \mod d} \right\rfloor \end{aligned}$$

Then, $\underline{d}$ can be substituted from the equation right above (not shown), and so on. Once we get to the top, we'll have written an equation

$$ax + by = 1$$

for $x, y \in \mathbb{Z}$. From here, $\pmod{b}$ tells us that

$$ax \equiv 1 \pmod{b}$$

$$x \equiv a^{-1} \pmod{b},$$

and as we'll know what x is, we'll have our modular inverse! From the previous example,

$$\begin{aligned}
667 &= 20 \cdot \underline{33} + \underline{7} \\
33 &= 4 \cdot \underline{7} + \underline{5} \\
7 &= 1 \cdot \underline{5} + \underline{2} \\
5 &= 2 \cdot \underline{2} + \underline{1}
\end{aligned}$$

Thus,

$$\begin{aligned}
\underline{7} &= 667 - 20 \cdot \underline{33} \\
\underline{5} &= 33 - 4 \cdot \underline{7} \\
\underline{2} &= 7 - 1 \cdot \underline{5} \\
\underline{1} &= 5 - 2 \cdot \underline{2}
\end{aligned}$$

$$\begin{aligned}
1 &= 5 - 2 \cdot \underline{2} \\
&= 5 - 2 \cdot (7 - 1 \cdot \underline{5}) \\
&= 3 \cdot \underline{5} - 2 \cdot 7 \\
&= 3 \cdot (33 - 4 \cdot \underline{7}) - 2 \cdot 7 \\
&= 3 \cdot 33 - 14 \cdot \underline{7} \\
&= 3 \cdot 33 - 14 \cdot (667 - 20 \cdot \underline{33}) \\
&= 283 \cdot \underline{33} - 14 \cdot 667
\end{aligned}$$

Therefore, our inverse is $\boxed{283 \pmod{667}}$. ■

Problem 22: Prove that two consecutive positive integers are always relatively prime.

Problem 23: The remainder a two-digit positive integer leaves upon division by 9 is 1. The remainder it leaves upon division by 10 is 3. What is the remainder its tens digit leaves upon division by 3?

Problem 24: Prove that $\dfrac{21n+4}{14n+3}$ is irreducible for every natural number n. (Source: 1959 IMO #1)

Problem 25: The base-69 number system consists of the digits $0, 1, 2, \ldots, 9$ and $A_1, A_2, A_3, \ldots, A_{59}$ in that order. For instance, the base-10 number 2021 is $A_{20}A_{11}$ in base-69. In base-69, what is the smallest positive integer that can be multiplied by $A_{20}A_{11}$ for a product with a units digit of 3?

5 Linear Diophantines

> There are things known and there are things unknown, and in between are the doors of perception.
>
> — Aldous Huxley, *The Doors of Perception*

§ 5.1 The Modular Cloaking Method

Number theory studies the integers, and linear equations are the most fundamental of mathematical relationships. Uniting these ideas, we now investigate **linear Diophantine equations**, linear equations that permit only integer solutions. We already have all the tools we need.

Example 22: Use wishful thinking to find all integer solutions (x, y) to the equation $3x + 4y = 5$.

Since we have two variables and only one equation, we can't play our usual "isolate the variable" game...Or can we? Let's use wishful thinking. We want to be able to isolate, for example, x, so we need some way to get rid of y. But modular arithmetic is good at that: x and y have to be integers! Imagine wrapping a $\pmod 4$ invisibility cloak around the equation. $4y \equiv 0 \pmod 4$, so it will vanish, leaving only

$$3x \equiv 5 \equiv 9 \pmod 4 \implies x \equiv 3 \pmod 4.$$

From here, we can write the parametric equation $x = 4k + 3$, where $k \in \mathbb{Z}$. Plugging this back into the original equation and solving for y, we get

$$3(4k + 3) + 4y = 5 \implies y = -3k - 1.$$

Therefore, all (x, y) that satisfy this equation are $\boxed{(4k + 3, -3k - 1); k \in \mathbb{Z}}$. ■

Example 23: Extend your insights from the previous example to prove that $ax + by = c$, where all variables are integers, has a solution (x, y) if and only if $(a, b)|c$.

The modular cloaking method, as we'll call it, served us well last time. Let's try it again. Cloaking $\pmod b$ leaves

$$ax \equiv c \pmod b.$$

If we find the necessary and satisfactory constraints for which this congruence has a solution, we will have solved the original problem because, by the equation $ax + by = c$, y is guaranteed to exist as long as x does. There are two cases for a necessary and sufficient solution.

- $(a, b) = 1$, meaning $a^{-1} \pmod b$ exists and so does $x \equiv a^{-1}c \pmod b$.
- $(a, b) > 1$ but $(a, b)|c$, so we can divide both sides of the congruence by (a, b) and then multiply both sides by a^{-1} in the new modulus, giving $x \equiv a^{-1}\frac{c}{(a,b)} \left(\operatorname{mod} \frac{b}{(a,b)}\right)$.

Both cases can be conflated to form the single condition that $(a,b)|c$ as desired. ■

Problem 26: How many ways are there to write 2016 as the sum of twos and threes, ignoring order? (For example, $1008 \cdot 2 + 0 \cdot 3$ and $402 \cdot 2 + 404 \cdot 3$ are two such ways.) (Source: 2016 AMC 10A #14)

Problem 27: Penniless Pete's piggy bank has no pennies in it, but it has 100 coins, all nickels, dimes, and quarters, whose total value is $8.35. It does not necessarily contain coins of all three types. What is the difference between the largest and smallest number of dimes that could be in the bank? (Source: 2003 AMC 12B #7)

§ 5.2 The Extended Euclidean Algorithm Method

Wait a second. Haven't we seen linear Diophantines before this chapter? Just last chapter, the extended Euclidean algorithm on (a,b) gave us (x_0,y_0) such that

$$ax_0 + by_0 = 1,$$

where all variables are integers. Let's take a closer look.

Example 24: If we have (x_0,y_0) such that $ax_0 + by_0 = 1$, how can we find all (x,y) such that $ax + by = c$?

Multiplying both sides of this equation by c, we have

$$a(cx_0) + b(cy_0) = c.$$

This tells us that (cx_0, cy_0) is one specific (x,y). How can we find all (x,y)? Constructively, for a parameter $k \in \mathbb{Z}$, we can come up with $x = bk + cx_0$ and $y = -ak + cy_0$. Substituting these in gives us

$$a(bk + cx_0) + b(-ak + cy_0) = abk + a(cx_0) - abk + b(cy_0) = a(cx_0) + b(cy_0) = c.$$

Therefore, all (x,y) are given by $\boxed{(bk + cx_0, -ak + cy_0);\, k \in \mathbb{Z}}$. As an aside, if $(a,b) \neq 1$ in a general Diophantine $ax + by = c$ to start, we can fix the Diophantine by dividing out by (a,b) as we require $c|(a,b)$ regardless. ■

Example 25: Find all integer solutions (x,y) to the equation $3x + 4y = 5$, this time using the extended Euclidean algorithm. Show the parametric form obtained is equivalent to the one from before.

$(3,4) = 1$, so we can find (x_0,y_0) by the extended Euclidean algorithm on $(3,4)$:

$$4 = 3 \cdot 1 + 1$$

$$1 = 4 - 3 \cdot 1.$$

Therefore, (x_0,y_0) is $(-1,1)$. This gives us $(4k - 1 \cdot 5, -3k + 1 \cdot 5) = \boxed{(4k-5, -3k+5);\, k \in \mathbb{Z}}$. This is equivalent to the form $(4k+3, -3k-1)$ from before because $4k - 5 = 4(k-2) + 3$ and

$-3k + 5 = -3(k - 2) - 1.$ ■

Problem 28: A lattice point is a point in the plane with integer coordinates. How many lattice points are on the line segment whose endpoints are $(3, 17)$ and $(48, 281)$? (Include both endpoints of the segment in your count.) (Source: 1989 AHSME #16)

Problem 29: Elmo makes N sandwiches for a fundraiser. For each sandwich he uses B globs of peanut butter at \$0.04 per glob and J blobs of jam at \$0.05 per blob. The cost of the peanut butter and jam to make all the sandwiches is \$2.53. Assume that B, J, and N are positive integers with $N > 1$. What is the cost of the jam Elmo uses to make the sandwiches? (Source: 2006 AMC 10B #22)

6 Systems of Linear Congruences

> What is the reason for a unity? Many things have a plurality of parts. They are not merely complete aggregates but instead wholes beyond their parts.
>
> — Translation of Aristotle, *Metaphysics*

§ 6.1 The Chinese Remainder Theorem

This whole book, we've explored parallels between equations and congruences. For linear equations, we've discussed linear congruences. But consider systems of linear equations. Can we have systems of linear congruences? Let's start by discussing a central theorem.

The Chinese remainder theorem states that, for any system of linear congruences involving one variable that has at least one solution, it has exactly one unique solution modulo the LCM of all the moduli in the system. This follows as a consequence of the extended Euclidean algorithm, but the full proof is rather involved and will not be discussed here. The reader is strongly encouraged to look it up if interested.

§ 6.2 The Modular Cloaking Method (Reprise)

In the last chapter, we investigated a modular cloaking method to solve Diophantines. We can do the same for systems of linear congruences by turning them into Diophantines. As always, let's begin with an example.

Example 26: Solve the following system.

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

In parametric form x can be expressed as $3a + 2$ and $5b + 3$ for parameters $a, b \in \mathbb{Z}$. Hence, we can set these equal to get

$$3a + 2 = 5b + 3.$$

This is exactly like the Diophantine situation we analyzed in the previous section, so we can cloak $\pmod{3}$. This gives us

$$2b \equiv 2 \pmod{3} \implies b \equiv 1 \pmod{3} \implies b = 3c + 1;\ c \in \mathbb{Z}.$$

Now, recall

$$x = 5b + 3 = 5(3c + 1) + 3 = 15c + 8.$$

Therefore, $x \equiv \boxed{8 \pmod{15}}$. This solution is unique as the Chinese remainder theorem proclaims any solution modulo $[3, 5] = 15$ must be unique. ■

It is sometimes beneficial to use the Chinese remainder theorem backwards to destruct moduli and then reconstruct them.

Example 27: Find $33^{-1} \pmod{100}$ by noting that $100 = 25 \cdot 4$.

Because $100 = 25 \cdot 4$, if we find $33^{-1} \pmod{25}$ and $33^{-1} \pmod{4}$, we can combine them using a Chinese remainder theorem argument modulo $[4, 25] = 100$.

$$33 \equiv 8 \pmod{25} \implies 33^{-1} \equiv 8^{-1} \equiv 24^{-1} \cdot 3 \equiv -1 \cdot 3 \equiv -3 \equiv 22 \pmod{25}.$$

$$33 \equiv 1 \pmod{4} \implies 33^{-1} \equiv 1 \pmod{4}.$$

Therefore, our answer is x such that

$$x \equiv 22 \pmod{25}$$
$$x \equiv 1 \pmod{4}$$

In parametric form, x can be $25a + 22$ or $4b + 1$ for parameters $a, b \in \mathbb{Z}$. This gives the Diophantine

$$25a + 22 = 4b + 1.$$

Cloaking $\pmod{4}$ gives

$$25a + 22 \equiv a + 2 \equiv 1 \pmod{4} \implies a \equiv -1 \equiv 3 \pmod{4}.$$

Therefore, $a = 4c + 3$ for parameter $c \in \mathbb{Z}$. In turn,

$$x = 25a + 22 = 25(4c + 3) + 22 = 100c + 97 \implies x \equiv \boxed{97 \pmod{100}}.$$

■

Problem 30: Let $N = 123456789101112\ldots4344$ be the 79-digit number that is formed by writing the integers from 1 to 44 in order, one after the other. What is the remainder when N is divided by 45? (Source: 2017 AMC 10B #23)

Problem 31: Let m be the least positive integer divisible by 17 whose digits sum to 17. Find m. (Source: 2015 AIME II #3)

§ 6.3 The Modular Part Method

For systems with lots of congruences, the modular cloaking method becomes cumbersome. Fortunately, we have an alternative.

Example 28: Solve the following system.

$$x \equiv 2 \pmod{3}$$
$$x \equiv 2 \pmod{4}$$
$$x \equiv 1 \pmod{5}$$

One way to approach the solution is to think of x as the sum of three modular parts: x_3, x_4, and x_5. We multiply the part corresponding to each modulus by all other moduli to ensure that the parts are independent.

$$x \equiv 4 \cdot 5x_3 + 3 \cdot 5x_4 + 3 \cdot 4x_5 \pmod{[3,4,5]}$$

The reason these coefficients ensure independence is that if we look at x in a given modulus, the irrelevant parts disappear. For instance, $\pmod 4$ or $\pmod 5$, the $\pmod 3$ part $4 \cdot 5x_3$ disappears, but $\pmod 3$, $4 \cdot 5x_3$ is all that remains. Now, we solve for x_3, x_4, x_5 by considering what happens in each modulus. $\pmod 3$, we have

$$x \equiv 4 \cdot 5x_3 \equiv 20x_3 \equiv 2x_3 \equiv 2 \pmod 3 \implies x_3 \equiv 1 \pmod 3.$$

This means we can just say $x_3 = 1$ (we don't need to worry about multiple values because one value is enough to find the residue class). $\pmod 4$, we have

$$x \equiv 3 \cdot 5x_4 \equiv 15x_4 \equiv -x_4 \equiv 2 \pmod 4 \implies x_4 \equiv -2 \equiv 2 \pmod 4.$$

We can just say $x_4 = 2$. $\pmod 5$, we have

$$3 \cdot 4x_5 \equiv 12x_5 \equiv 2x_5 \equiv 1 \equiv 6 \pmod 5 \implies x_5 \equiv 3 \pmod 5.$$

Thus, $x_5 = 3$. Substituting x_3, x_4, x_5 back in gives

$$x \equiv 4 \cdot 5 \cdot 1 + 3 \cdot 5 \cdot 2 + 3 \cdot 4 \cdot 3 \equiv 86 \equiv \boxed{26 \pmod{60}}.$$

■

§ 6.4 Neat Tricks

Sometimes, there is a neat trick to significantly speed up the solution.

Example 29: Solve the following system.

$$\begin{aligned} x &\equiv 3 \pmod 4 \\ x &\equiv 6 \pmod 7 \end{aligned}$$

We can rewrite the system as

$$\begin{aligned} x &\equiv -1 \pmod 4 \\ x &\equiv -1 \pmod 7 \end{aligned}$$

That is,

$$\begin{aligned} x + 1 &\equiv 0 \pmod 4 \\ x + 1 &\equiv 0 \pmod 7 \end{aligned}$$

But this just means

$$x + 1 \equiv 0 \pmod{[4,7]} \implies x \equiv \boxed{27 \pmod{28}}.$$

■

Problem 32: What is the smallest positive integer greater than 1 that leaves a remainder of 1 when divided by 4, 5, and 6? (Source: 2017 AMC 8 #12)

7 Solutions

The solution often turns out more beautiful than the puzzle.

— Richard Dawkins, *Unweaving the Rainbow*

§ 7.1 Solutions to Preface

Solution 1: Greedily, if we want to find the largest positive integer that divides 40 and 78, we need to selectively multiply together the largest power of each prime divisor common to both. This in fact forces us to choose the smallest exponents across all prime divisors. The prime factorization of 40 is $2^3 \cdot 5$, and that of 78 is $2 \cdot 3 \cdot 13$. The only prime divisor common to both is 2, and it is already of the largest power possible. By definition, this is the GCD, so we can write $\boxed{(40, 78) = 2}$.

To find the smallest positive integer divisible by both 40 and 78, we again take a greedy approach: selectively multiply together the smallest power of each prime divisor that satisfies the divisibility requirement. This in fact forces us to choose the largest exponents across all prime divisors. Using the prime factorizations mentioned earlier, this becomes $2^3 \cdot 3 \cdot 5 \cdot 13 = 1560$. By definition, this is the LCM, so we can write $\boxed{[40, 78] = 1560}$.

In retrospect, we could expedite the process of finding the GCD using the extended Euclidean algorithm, which we will cover when we visit linear congruences, and that of the LCM using the identity that

$$[40, 78] = \frac{40 \cdot 78}{(40, 78)}.$$

■

Solution 2: The number $\underline{abcabc}$ can be rewritten as $1000\underline{abc} + \underline{abc}$ (constructively, think of shifting the second $\underline{abc}$ three places to the right to make room for the first $\underline{abc}$). Therefore, it is just $1001\underline{abc}$, and since nothing more can be said about $\underline{abc}$, the answer is $\boxed{1001}$. ■

Solution 3: We must count the number of the first 1234567 positive integers divisible by 3 and divide that by 1234567. Given the magnitude of that number, this seems like no easy task. Regardless, we push through, in search of a pattern to exploit.

$$1, 2, 3, 4, 5, 6, 7, 8, 9, 10, 11, 12 \ldots$$

Aha! Every three numbers we count, we find precisely one positive integer divisible by 3, and this is no coincidence: it's the definition of divisibility. This already tells us that our probability will be close to $\frac{1}{3}$, but we can find the exact value. All we have to do is count the number of packages of three we can cut the first 1234567 positive integers into: $\left\lfloor \frac{1234567}{3} \right\rfloor$.

Our final answer becomes $\dfrac{\left\lfloor \dfrac{1234567}{3} \right\rfloor}{1234567} = \boxed{0.33333306\ldots}$, matching our $\dfrac{1}{3}$ approximation. ■

Solution 4: From the problem statement, we can extract the following requirements:

$$x \in \mathbb{Z}$$

$$2x+9 \in \mathbb{Z}^+ \implies x \in \mathbb{Z}^{\geq -4}$$
$$3x+4 \in \mathbb{Z}^+ \implies x \in \mathbb{Z}^{\geq -1}$$
$$3x+4 \geq 2x+9 \implies x \in \mathbb{Z}^{\geq 5}$$

Additionally, we require

$$\frac{3x+4}{2x+9} = 1 + \frac{x-5}{2x+9} \in \mathbb{Z}^+ \implies \frac{x-5}{2x+9} \in \mathbb{Z}^{\geq 0}.$$

This secondary requirement means that either $x = 5$ or

$$x-5 \geq 2x+9 \implies x \in \mathbb{Z}^{\leq -14}.$$

The second case is clearly impossible due to the strict $x \in \mathbb{Z}^{\geq 5}$ requirement from earlier, so the only valid integer x is $\boxed{5}$. ■

Solution 5: It is trivial by inspection that p satisfies this condition. Let the smallest positive such integer be k. For the sake of contradiction, assume that $k < p$ and $p|k!$. Then, $k!$ is the product of all positive integers less than p and p is present in the prime factorization of $k!$. Some of the positive integers in this product are themselves primes less than p, while others are less than p and have unique prime factorizations involving only primes less than p by the fundamental theorem of arithmetic. Thus, p cannot be present in prime factorization of $k!$, establishing contradiction. This means that $k = p$. ■

Solution 6: Because finding the remainder directly does not seem like an easy task, we first look for the quotient q. Because the quotient is the greatest number of times m goes into a, it is the integer part of $\dfrac{a}{m}$. But how do we truncate the fractional part? Apply the floor function!

$$q = \left\lfloor \frac{a}{m} \right\rfloor$$

Our remainder becomes $a - mq = \boxed{a - m\left\lfloor \dfrac{a}{m} \right\rfloor}$. ■

§ 7.2 Solutions to Arithmetic—Modulo *m*

Solution 7: Let x be the measure of the forgotten angle. The degree sum of the measures of the interior angles of an n-gon is $180(n-2)$, or $180(n-2) - x$ if we forget x. We can solve for x if we note that

$$180(n-2) - x \equiv -x \pmod{180}.$$

Claire's sum of $2017 \equiv 37 \equiv -143 \pmod{180}$, so $x \equiv 143 \pmod{180}$. In fact, since $x < 180$ due to the convex condition, $x = \boxed{143^\circ}$. ■

Solution 8: Instead of using names for the days of the week, we can use modular residues $\pmod 7$ (for 7 days in a week), allowing us to use modular arithmetic. Let Monday be $0 \pmod 7$, Tuesday be $1 \pmod 7$, and so on so that Sunday is $6 \pmod 7$. Now, the 300th day of year N is $1 \pmod 7$. Suppose year N has d days, where d is 365 or 366 depending on whether it's a leap year. Then, the number of days it takes to get from the 300th day of year N to the 200th of year $N+1$ is $d - 100$. Since the 200th of year $N+1$ is also $1 \pmod 7$, we can write

$$1 + d - 100 \equiv 1 \pmod 7 \implies d \equiv 2 \pmod 7.$$

Therefore, $d = 366$ and year N is indeed a leap year, and thus year $N-1$ is not. To go back from the 300th day of year N to the 100th of year $N-1$, we subtract $200 + 365 = 565$ days. This means our answer is the day of the week corresponding to $1 - 565 \equiv 3 \pmod 7$, or $\boxed{\text{Thursday}}$. ■

Solution 9: Parity is given by the residue $\pmod 2$, and each of n, m can be $0, 1 \pmod 2$ Thus, we have four cases $(n, m) \pmod 2$. Of these four cases, only $(0,0)$ and $(1,1)$ make $n^2 + m^2 \equiv 0 \pmod 2$. In both cases, $n + m \equiv 0 \pmod 2$, so $\boxed{\textbf{(D)}}$. ■

Solution 10: The units digit is given by the residue $\pmod{10}$. Computing the residues for the first few terms reveals the repeating pattern: $6, 4, 0, 0, 0 \pmod{10}$, with a sum of $6 + 4 + 0 + 0 + 0 \equiv 0 \pmod{10}$. This pattern repeats k times, leaving a remainder of $2018 \bmod 5 = 3$ terms, which are $6, 4, 0 \pmod{10}$, with a sum of $6 + 4 + 0 \equiv 0 \pmod{10}$. Thus, the answer is $0k + 0 \equiv \boxed{0} \pmod{10}$. ■

Solution 11: Let their numbers be a, b, c by name. Since the units digit is the residue $\pmod{10}$, we are given the following:

$$a + b \equiv 2 \pmod{10}$$
$$b + c \equiv 4 \pmod{10}$$
$$a + c \equiv 0 \pmod{10}$$

Adding the congruences gives us

$$2(a + b + c) \equiv 6 \pmod{10}$$

We can divide both sides of the congruence by 2 and the modulus by $(2, 10) = 2$:

$$a + b + c \equiv 3 \pmod 5$$

Going back to $\pmod{10}$, this means we have

$$a + b + c \equiv 3, 8 \pmod{10}.$$

Therefore, our answer is $3 + 8 = \boxed{11}$. ■

§ 7.3 Solutions to Revisiting Divisibility Rules

Solution 12: By the divisibility rule for 11,

$$2 - A + 1 \equiv 3 - A \equiv 0 \pmod{11} \implies A \equiv \boxed{3} \pmod{11}.$$

■

Solution 13: By the divisibility rule for 9,

$$2 + 0 + 1 + 8 + U \equiv 2 + U \equiv 0 \pmod 9 \implies U \equiv 7 \pmod 9.$$

Thus, $U = 7$. By the divisibility rule of 2^k, since $8 = 2^3$, the answer is $187 \bmod 8 = \boxed{3}$. ■

Solution 14: We have

$$\begin{gathered} 10Q + R \equiv 2Q + R \equiv 0 \pmod 4 \\ S \equiv 0 \pmod 5 \\ R + S + T \equiv 0 \pmod 3 \end{gathered}$$

Since $S \neq 0$, we have $S = 5$. Since R is either 2 or 4, we just try both. If $R = 2$, from the third congruence $T = 2$ as well, which is illegal. Thus, $R = 4$ and $T = 3$. From the first congruence, we have

$$2Q + 4 \equiv 0 \pmod 4 \implies Q \equiv 0 \pmod 2,$$

meaning $Q = 2$ and $P = \boxed{1}$. ■

Solution 15: By the divisibility rule of 9, $n \equiv S(n) \pmod 9$. Therefore, $S(n+1) \equiv n + 1 \equiv S(n) + 1 \equiv 1275 \equiv 1 + 2 + 7 + 5 \equiv 6 \pmod 9$. The only choice with a residue of 6 is $\boxed{\textbf{(D)}}$. ■

Solution 16: By the divisibility rule of 9, $n \equiv S(n) \pmod 9$. But this also means $S(n) \equiv S(S(n)) \pmod 9$. In fact, we can nest S as many times as we want, so imagine we just keep doing so until we find the digital root. This tells us that the digital root is just the $\pmod 9$ residue, or 9 if the residue is 0. Effectively, all we have to do is find the modular residue $\pmod 9$ of $f(1) + f(2) + \cdots + f(2018)$. However, note that $f(n) \equiv n^2 \pmod 9$ by another application of the divisibility rule. As such, by the sum of squares formula,

$$1^2 + 2^2 + \cdots + 2018^2 \equiv \frac{2018(2018+1)(2 \cdot 2018 + 1)}{6} \equiv \boxed{8} \pmod 9.$$

■

Solution 17: Let the prime be p. We have

$$\left\lfloor \frac{n}{10} \right\rfloor - 3\left(n - 10\left\lfloor \frac{n}{10} \right\rfloor\right) \equiv 0 \pmod p$$

$$31\left\lfloor \frac{n}{10} \right\rfloor + 4n \equiv 0 \pmod p.$$

By the same logic as in the example, $p = \boxed{31}$. ■

§ 7.4 Solutions to Exponential Remainders

Solution 18: Suppose we select a number m from the set. We have to examine exponents of $m \pmod{10}$ to see if we ever reach a 1. If and when we do, the residues cycle thereafter. To be precise, if we find the smallest $t \in \mathbb{Z}^+$ such that $m^t \equiv 1 \pmod{10}$,[1] then we can say that the residue will be 1 for all n that are multiples of t. We can find the smallest such t for each m through inductive reasoning. While no such t exists for 15, below are the correct values of t for each of the other residues:

$$11^1 \equiv 1 \pmod{10}$$
$$13^4 \equiv 1 \pmod{10}$$
$$17^4 \equiv 1 \pmod{10}$$
$$19^2 \equiv 1 \pmod{10}$$

Because the second set is a continuous range of $2018 - 1999 + 1 = 20$ integers and 20 is evenly divisible by all values of t, our overall probability is

$$\sum \frac{1}{5} \cdot \frac{1}{t} = \frac{1}{5}\left(1 + \frac{1}{4} + \frac{1}{4} + \frac{1}{2}\right) = \boxed{\frac{2}{5}}.$$

■

Solution 19: 89 is prime, so $\phi(89) = 88$. Then,

$$69^{354} \equiv 69^{354 \mod 88} \equiv 69^2 \equiv (-20)^2 \equiv 400 \equiv \boxed{44} \pmod{89}.$$

■

Solution 20: Because there is a continuous range of 2020 integers and $2020 \equiv 0 \pmod{5}$, N can be any $\pmod{5}$ residue with equal probability. Therefore, it suffices to consider all five possible residues r. For $r = 0$, the remainder is obviously 0. However, consider $0 < r \leq 4$ with $\phi(5) = 4$:

$$r^{16} \equiv r^{16 \mod 4} \equiv r^0 \equiv 1 \pmod{5}.$$

Therefore, the probability is $\boxed{\frac{4}{5}}$. ■

Solution 21: The last two digits are given by the $\pmod{100}$ residue, so we have $11^{2012^{2013}}$. By the binomial theorem[2],

$$(10+1)^{2012^{2013}} = \sum_{k=0}^{2012^{2013}} \binom{2012^{2013}}{k} 10^k 1^{2012^{2013}-k} = \sum_{k=0}^{2012^{2013}} \binom{2012^{2013}}{k} 10^k \equiv 10 \cdot 2012^{2013} + 1 \pmod{100}.$$

The units digit of $10 \cdot 2012^{2013} + 1$ will be 1 while the tens digit will be the units digit of 2012^{2013}.

[1] It is important to know that, in the general case modulo m, $\phi(m)$ is not necessarily the smallest such t and only one such t. In fact, the smallest such t is very closely tied to the concept of multiplicative order, beyond the scope of this book but very worth exploring for those interested.

[2] The reader should look this up if unfamiliar.

By inductive reasoning, the powers of 2 $\pmod{10}$ cycle with length 4, so[3]

$$2012^{2013} \equiv 2^{2013} \equiv 2^{2013 \mod 4} \equiv 2^1 \equiv 2 \pmod{10}.$$

Therefore, the answer is $\boxed{21}$. ■

§ 7.5 Solutions to Linear Congruences

Solution 22: Two consecutive positive integers can be represented by n and $n+1$ for $n \in \mathbb{Z}^+$. By the Euclidean algorithm, we have

$$(n, n+1) = (n, n+1-n) = (n, 1) = 1,$$

so two consecutive positive integers must be relatively prime. ■

Solution 23: Because the number is 3 $\pmod{10}$, its units digit is 3. Thus, if it has a tens digit of x, it can be expressed as $10x+3$. Using the 9 condition, we have

$$10x + 3 \equiv 1 \pmod 9 \implies x \equiv -2 \equiv 7 \pmod 9.$$

Therefore, the tens digit x can be written in the form $9t+7$ for some parameter $t \in \mathbb{Z}$. However, taking this $\pmod 3$ gives us

$$9t + 7 \equiv 7 \equiv \boxed{1} \pmod 3.$$

■

Solution 24: A fraction is irreducible if its numerator and denominator are relatively prime. We can use the Euclidean algorithm:

$$\begin{aligned}(21n+4, 14n+3) &= (21n+4-(14n+3), 14n+3)\\ &= (7n+1, 14n+3)\\ &= (7n+1, 14n+3-(7n+1))\\ &= (7n+1, 7n+2)\end{aligned}$$

Because $7n+1$ and $7n+2$ are consecutive positive integers, they are relatively prime, and thus the numerator and denominator are also relatively prime as desired. ■

Solution 25: By the same logic that the units digit of a base-10 positive integer is its remainder upon division by 10, the units digit of a base-69 positive integer is its remainder upon division by 69. Hence, we can do this problem $\pmod{69}$ without having to work with numbers base-69 and just convert to base-69 at the end. We need to find the smallest positive integer x such that

$$2021x \equiv 3 \pmod{69}.$$

Because $2021 \equiv 20 \pmod{69}$ and $(20, 69) = 1$, this reduces to

$$20x \equiv 3 \pmod{69} \implies x \equiv 20^{-1} \cdot 3 \pmod{69}.$$

[3] You might be tempted to use Euler's totient theorem here and reduce it to $2^{2013 \mod \phi(10)}$. However, $(2, 10) \neq 1$, so this is incorrect! Trickily enough, the bogus solution coincidentally yields the correct answer.

It remains to calculate $20^{-1} \pmod{69}$, which we can do via the extended Euclidean algorithm on $(20, 69)$:

$$\begin{aligned} 69 &= 3 \cdot 20 + 9 \\ 20 &= 2 \cdot 9 + 2 \\ 9 &= 4 \cdot 2 + 1 \end{aligned}$$

$$\begin{aligned} 9 &= 69 - 3 \cdot 20 \\ 2 &= 20 - 2 \cdot 9 \\ 1 &= 9 - 4 \cdot 2 \end{aligned}$$

$$\begin{aligned} 1 &= 9 - 4 \cdot 2 \\ &= 9 - 4 \cdot (20 - 2 \cdot 9) \\ &= 9 \cdot 9 - 4 \cdot 20 \\ &= 9 \cdot (69 - 3 \cdot 20) - 4 \cdot 20 \\ &= 9 \cdot 69 - 31 \cdot 20 \end{aligned}$$

So $20^{-1} \equiv -31 \equiv 38 \pmod{69}$. This gives us

$$x \equiv 20^{-1} \cdot 3 \equiv 38 \cdot 3 \equiv 45 \pmod{69}.$$

In base-69, 45 becomes $\boxed{A_{36}}$. ■

§ 7.6 Solutions to Linear Diophantines

Solution 26: Suppose we invoke x twos and y threes. We have the Diophantine

$$2x + 3y = 2016.$$

Cloaking $\pmod{3}$, we get

$$2x \equiv 2016 \equiv 2 + 0 + 1 + 6 \equiv 0 \pmod{3} \implies x \equiv 0 \pmod{3}.$$

This means $x = 3k$ for parameter $k \in \mathbb{Z}$. Substituting this back in to the original equation and solving for y gives

$$2(3k) + 3y = 2016 \implies y = 672 - 2k.$$

Note that $x, y \geq 0$, so

$$3k \geq 0 \implies k \geq 0$$

$$672 - 2k \geq 0 \implies k \leq 336$$

Therefore, we must count the number of $k \in \mathbb{Z}^{[0,336]}$. There are $336 - 0 + 1 = \boxed{337}$ of these. ■

Solution 27: Let n, d, q be the numbers of nickels, dimes, and quarters, respectively. From the total value of \$8.35, we know

$$5n + 10d + 25q = 835 \implies n + 2d + 5q = 167.$$

From the 100 coins, we know

$$n + d + q = 100.$$

Subtracting the second equation from the first gives the Diophantine

$$d + 4q = 67,$$

through which we must find the difference between the largest and smallest possible values of d. Cloaking $\pmod 4$ gives

$$d \equiv 67 \equiv 3 \pmod 4.$$

Therefore, $d = 4k + 3$ for parameter $k \in \mathbb{Z}$. Substituting back in to solve for q gives

$$4k + 3 + 4q = 67 \implies q = 16 - k.$$

Since $d, q \geq 0$,

$$4k + 3 \geq 0 \implies k \geq 0$$
$$16 - k \geq 0 \implies k \leq 16.$$

Finally,

$$k \in \mathbb{Z}^{[0,16]} \implies d \in \mathbb{Z}^{[3,67]}.$$

The difference is $67 - 3 = \boxed{64}$. ■

Solution 28: Let the line segment be a set of points (x, y). We are already given $x \in \mathbb{Z}^{[3,48]}$ and $y \in \mathbb{Z}^{[17,281]}$. Other than these conditions, the line segment is defined by the equation of the line it is on. By a conversion from point-slope form into standard form, we have

$$y - 17 = \frac{281 - 17}{48 - 3}(x - 3) \implies 88x - 15y = 9.$$

Since $(88, 15) = 1$, the extended Euclidean algorithm gives

$$\begin{aligned} 88 &= 5 \cdot 15 + 13 \\ 15 &= 1 \cdot 13 + 2 \\ 13 &= 6 \cdot 2 + 1 \end{aligned}$$

$$\begin{aligned} 13 &= 88 - 5 \cdot 15 \\ 2 &= 15 - 1 \cdot 13 \\ 1 &= 13 - 6 \cdot 2 \end{aligned}$$

$$\begin{aligned}1 &= 13 - 6 \cdot 2\\ &= 13 - 6 \cdot (15 - 1 \cdot 13)\\ &= 7 \cdot 13 - 6 \cdot 15\\ &= 7 \cdot (88 - 5 \cdot 15) - 6 \cdot 15\\ &= 7 \cdot 88 - 41 \cdot 15\end{aligned}$$

Thus, $(x_0, y_0) = (7, 41)$, and $(x, y) = (15k + 7 \cdot 9, 88k + 41 \cdot 9)$; $k \in \mathbb{Z}$. Imposing the original conditions gives

$$3 \leq 15k + 7 \cdot 9 \leq 48 \implies -4 \leq k \leq -1$$

$$17 \leq 88k + 41 \cdot 9 \leq 281 \implies -4 \leq k \leq -1.$$

Therefore, $k \in \mathbb{Z}^{[-4,-1]}$, giving $\boxed{4}$ lattice points ■

Solution 29: Given the information for N sandwiches,

$$N(4B + 5J) = 253.$$

Since $N > 1$ and $253 = 11 \cdot 23$, $N = 11$. Therefore,

$$4B + 5J = 23.$$

As $(4, 5) = 1$, the extended Euclidean algorithm gives

$$5 = 4 \cdot 1 + 1$$

$$1 = 5 - 4 \cdot 1.$$

Therefore, $(B_0, J_0) = (-1, 1)$ and $(B, J) = (5k - 23, -4k + 23)$ for parameter $k \in \mathbb{Z}$. The positive integer condition means

$$5k - 23 > 0 \implies k \geq 5$$

$$-4k + 23 > 0 \implies k \leq 5.$$

Therefore, we must have $k = 5$, with $B = 2, J = 3$. The total cost is thus $3 \cdot 5 \cdot 11 = 165$ cents, or $\boxed{\$1.65}$. ■

§ 7.7 Solutions to Systems of Linear Congruences

Solution 30: We want the modular residue of $N \pmod{45}$. However, 45 isn't a very nice number, so let's break it down. We can write $45 = 9 \cdot 5$ and look at the residues of $N \pmod{9, 5}$ instead, combining them with a Chinese remainder theorem argument for $[9, 5] = 45$. By the divisibility rule for 9, the residue of $N \pmod 9$ is the same as that of the sum of its digits. But we can reuse the divisibility rule for 9 to regroup the digits and form an arithmetic series as well. In short, we have

$$N \equiv 1 + 2 + 3 + \cdots + 44 \equiv \frac{44 \cdot 45}{2} \equiv 0 \pmod{9}.$$

By the divisibility rule for 5, the residue of $N \pmod 5$ is the same as that of its last digit. Therefore, $N \equiv 4 \pmod 5$. Overall, we have

$$N \equiv 0 \pmod{9}$$

$$N \equiv 4 \pmod{5}$$

In parametric form, $N = 9a = 5b + 4$ for parameters $a, b \in \mathbb{Z}$. Cloaking this Diophantine $\pmod{5}$ gives

$$9a \equiv 4a \equiv 4 \pmod{5} \implies a \equiv 1 \pmod{5} \implies a = 5c + 1;\, c \in \mathbb{Z}.$$

Then,

$$N = 9a = 9(5c+1) = 45c + 9 \implies N \equiv \boxed{9} \pmod{45}.$$

■

Solution 31: By the divisibility rule for 9, m is congruent to the sum of its digits modulo 9. Thus,

$$m \equiv 17 \equiv 8 \pmod{9}.$$

Overall,

$$m \equiv 0 \pmod{17}$$
$$m \equiv 8 \pmod{9}$$

In parametric form, $m = 17a = 9b + 8$ for parameters $a, b \in \mathbb{Z}$. Cloaking $\pmod{9}$ gives

$$17a \equiv 8a \equiv 8 \pmod{9} \implies a \equiv 1 \pmod{9} \implies a = 9c + 1;\, c \in \mathbb{Z}.$$

Hence,

$$m = 17a = 17(9c+1) = 153c + 17 \implies m \equiv 17 \pmod{153}.$$

We now need to search for the smallest m with a sum of digits equal to 17. The only way to do this from here is trial and error.

- $17 \implies 1 + 7 = 8 \neq 17$
- $170 \implies 1 + 7 + 0 = 8 \neq 17$
- $323 \implies 3 + 2 + 3 = 8 \neq 17$
- $476 \implies 4 + 7 + 6 = 17$

Thus, $m = \boxed{476}$. ■

Solution 32: We want the smallest positive integer $x > 1$ such that

$$x \equiv 1 \pmod{4,5,6} \implies x - 1 \equiv 0 \pmod{4,5,6} \implies x - 1 \equiv 0 \pmod{[4,5,6]} \equiv 0 \pmod{60}.$$

Therefore, $x = \boxed{61}$. ■

8 Denouement

> Stories never really end…even if the books like to pretend they do. Stories always go on. They don't end on the last page, any more than they begin on the first page.
>
> — Cornelia Funke, *Inkspell*

As a closing remark, I hope you had as much fun solving through this book as I had writing it. While this is the end of the exposition, this is not the end of modular arithmetic. We have covered but the tip of the iceberg, and readers interested may continue their journey into more advanced topics such as multiplicative order, primitive roots, quadratic residues, generating functions, Pell equations, and more.

Best of luck!