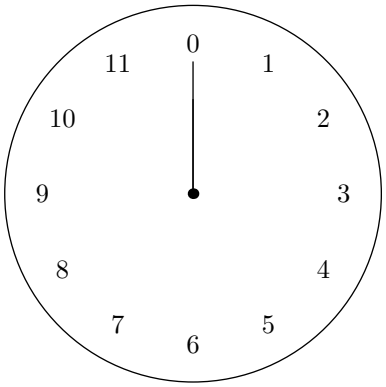
AMC/AIME Handout

Modular Arithmetic in the AMC and AIME

Author:
freeman66

For:
AoPS

Date:
May 13, 2020



It's time for modular arithmetic!

"I have a truly marvelous demonstration of this proposition which this margin is too narrow to contain." - Pierre de Fermat

Contents

§0 Acknowledgements

This was made for the Art of Problem Solving Community out there! I would like to thank Evan Chen for his evan.sty code. In addition, all problems in the handout were either copied from the Art of Problem Solving Wiki or made by myself.

Art of Problem Solving Community

Evan Chen's Personal Sty File

FREEMAN66's Website - Say Hi!

And Evan says he would like this here for evan.sty:

```
Boost Software License - Version 1.0 - August 17th, 2003
Copyright (c) 2020 Evan Chen [evan at evanchen.cc]
https://web.evanchen.cc/ || github.com/vEnhance
```

He also helped me with the hint formatting. I do honestly think that Evan is a LaTeXgod!
And finally, please do not make any copies of this document without referencing this original one. At least cite me when you are using this document.

§1 Introduction

§1.1 Number Theory

Number theory deals with the properties and relationships between numbers, especially positive integers.

Definition 1.1 (Prime & Composite) — If an integer has no positive divisors other than 1 and itself, it is said to be **prime**; otherwise, it is said to be **composite.** Note that 1 is considered composite.

Definition 1.2 (Multiples & Factors) — An integer a is said to be a **multiple** of another integer b if there exists an integer k such that $a = kb$. The integer b here is said to be called a **factor** or a **divisor** of a.

From this, we see that if a is a multiple of b, then b is a factor of a.

Definition 1.3 (Prime Factorization) — Any integer N can be written as the product of the primes it is divisible by. The **prime factorization** of N is

$$N = \prod_{p \in \mathbb{P}} p^{e_i} = 2^{e_1} \cdot 3^{e_2} \cdot 5^{e_3} \cdot \ldots,$$

where $\mathbb{P}$ is the set of positive primes and $\{e_i\}$ is a sequence of integers determining how many times the ith prime number can be divided out of N. For example, $144 = 2^2 \cdot 3^2$ and $35 = 5^1 \cdot 7^1$.

§1.2 Bases

To understand the notion of **base numbers**, we look at our own number system. We use the decimal, or base-10, number system. To help explain what this means, consider the number 2746. This number can be rewritten as $1234_{10} = 1 \cdot 10^3 + 2 \cdot 10^2 + 3 \cdot 10^1 + 4 \cdot 10^0$.

Note that each number in 1234 is actually just a placeholder which shows how many of a certain power of 10 there are. The first digit to the left of the decimal place (recall that the decimal place is to the right of the 6, i.e. 2746.0) tells us that there are six 10^0's, the second digit tells us there are four 10^1's, the third digit tells us there are seven 10^2's, and the fourth digit tells us there are two 10^3's.

Base-10 uses digits 0-9. Usually, the base, or **radix**, of a number is denoted as a subscript written at the right end of the number (e.g. in our example above, 2746_{10}, 10 is the radix).

To learn how to **convert** bases, read this.

§1.3 Divisibility

Let us first formally define **divisibility**.

Definition 1.4 (Divisibility) — Let $a, b \in \mathbb{Z}$. We say that b *divides* a if there exists an integer k such that $a = kb$. The number b is called a *divisor* or *factor* of a, and the number a is called a *multiple* of b. We write $b|a$ to denote that b divides a.

Theorem 1.5 (Division Theorem)

Let $a, b \in \mathbb{Z}$ with $b \neq 0$. Then there exist unique integers $q, r \in \mathbb{Z}$ such that $a = bq + r$ and $0 \leq r < |b|$.

Proof. First, note that if $a = 0$, then $q = 0, r = 0$ is the unique solution to the equation given.

We consider all other cases according to the signs of a and b.

Case 1: $b > 0, a > 0$. In order to prove the theorem, there are two parts: first, to show the existence of these integers q, r, and second, to show their uniqueness.

For the existence, for each $n \geq 0$ define $r_n = a - nb$. Let $S = \{r_n \mid r_n \geq 0\}$, that is, S is the set of those r_n that are nonnegative. Note that $r_0 = a > 0$, so S is nonempty. By the Well-Ordering Principle,, S has a minimum element, say $r_k = a - kb$. Then $a = kb + r_k$, by definition. Moreover, $r_{k+1} = a - (k+1)b = r_k - b < r_k$, so $r_{k+1} \notin S$, since r_k is the minimum of S. But this implies that $r_{k+1} < 0$, so $r_k - b < 0$, and hence $r_k < b$. Therefore, we have found integers k, r_k such that $a = kb + r_k$ and $0 \leq r_k < |b| = b$, and the existence of such integers is thus established.

For the uniqueness, suppose that $a = qb + r = q'b + r'$, where $q, q', r, r' \in \mathbb{Z}$ and $0 \leq r, r' < b$. By rearranging this equation, we have $qb - q'b = r' - r$, so $b(q - q') = r' - r$. Thus, $b|(r' - r)$. On the other hand, since $0 \leq r, r' < b$, we have that $-b < r' - r < b$. Note, if $q - q' > 0$, then $b(q - q') > b$, which is impossible. If $q - q' < 0$, then $b(q - q') < -b$, which is also impossible. Therefore, it must be the case that $q - q' = 0$, which implies $r' - r = 0$, and thus the representation of a is unique.

Case 2: $b < 0, a > 0$. Note that any presentation of $a = qb + r$ also implies $a = (-q)(-b) + r$. The choice of $-q, r$ are both exist and are unique by Case 1.

Case 3: $b > 0, a < 0$. By Case 1, we have a unique q, r such that $-a = (-q)b + r$, with $0 \leq r < b$. Hence there is a unique q, r such that $a = qb - r$, with $0 \leq r < b$. If $r = 0$, this is sufficient for the problem. If $r \neq 0$, we can write $a = (q-1)b + (b - r)$, then, and $0 < b - r < b$. Uniqueness will follow by an argument identical to that in Case 1.

Case 4: $b < 0, a < 0$. By Case 2, we have a unique q, r such that $-a = (-q)b + r$, with $0 \leq r < b$. Proceed as in Case 3 to construct a solution for a. □

Definition 1.6 (Quotient & Remainder) — Let $a, b \in \mathbb{Z}$, with $b \neq 0$ and let q, r be numbers such that $a = qb + r$, where $r < b$. We say that q is the *quotient* of a divided by b, and the r is the *remainder* of a divided by b.

Definition 1.7 (Greatest Common Divisor) — Let $a, b \in \mathbb{Z}$. An integer d is called a *greatest common divisor* of a, b, frequently abbreviated as a gcd of a, b if the following two conditions are met:

- $d|a$ and $d|b$, and
- if $q|a$ and $q|b$, then $q|d$.

Theorem 1.8 (Existence of GCD)

Let $a, b \in \mathbb{Z}$. Then a and b have a gcd.

Proof. First, if both a and b are 0, then 0 is a gcd for a and b, since 0 is divisible by q for every $q \in \mathbb{Z}$.

If a is negative, we can replace a with $-a$ without impacting the divisibility properties of a. Likewise, if b is negative, we can replace it with $-b$. Hence, we may proceed assuming that both a and b are nonnegative, and at least one of a, b is nonzero. Wolog, suppose that $a \neq 0$.

Define $X = \{n \in \mathbb{N} \mid n = au + bv \text{ for some } u, v \in \mathbb{Z}\}$. Notice that $a = a \cdot 1 + b \cdot 0$ and $a > 0$, so $a \in X$. Therefore, $X \neq \emptyset$, and X is a subset of $\mathbb{N}$, so by the Well Ordering Principle X has a minimum. Let $d = \min(X)$.

Claim 1. $d|a$.

Proof of Claim 1. By the Division Theorem, there exist unique $q, r \in \mathbb{Z}$ such that $a = qd + r$, and $0 \leq r < d$. Moreover, as $d \in X$, there exist $u, v \in \mathbb{Z}$ such that $d = au + bv$. Hence, we have

$$\begin{aligned} r &= a - qd \\ &= a - q(au + bv) \\ &= (1 - qu)a + (-qv)b. \end{aligned}$$

Hence, if $r > 0$, we must have $r \in X$. However, since $r < d$, we cannot have $r \in X$, since $d = \min(X)$. Therefore, $r = 0$, so $a = qd$ and $d|a$. □

By the same technique, we can establish the following claim:

Claim 2. $d|b$.

Hence, we have that d is a common divisor to both a and b. It remains to establish the second property for a gcd, namely, that if $q|a$ and $q|b$, we also have $q|d$.

To that end, suppose that q is a common divisor of a and b, so that there exist integers k, ℓ such that $a = kq$ and $b = \ell q$. Then we have

$$d = au + bv = kqu + \ell qv = q(ku + \ell v),$$

and thus $q|d$.

Therefore, d meets the definition of a gcd for a, b, and thus a gcd must exist. □

Theorem 1.9 (Properties of GCD)

Let $a \in \mathbb{Z}$. Then

- $\gcd(a, 0) = a$.
- $\gcd(a, 1) = 1$.
- For all $k \in \mathbb{Z}$, $\gcd(a, ka) = a$

There also exists the **least common multiple**:

Definition 1.10 (Least Common Multiple) — The **least common multiple** of two numbers a, b is, like the greatest common factor, defined by its name. It is the smallest multiple m in which $a|m$ and $b|m$.

Theorem 1.11 (Product of LCM and GCM)

For integers a, b,

$$\gcd(a, b) \cdot \operatorname{lcm}(a, b) = ab.$$

What happens when $\gcd(a, b) = 1$? We call that **coprime**, or **relatively prime**:

Definition 1.12 (Coprime) — Let $a, b \in \mathbb{Z}$. We say that a and b are **coprime**, if a and b share no common factors. That is to say, a and b are coprime if $\gcd(a, b) = 1$. We write $a \perp b$ to denote that a and b are coprime.

Theorem 1.13 (Coprime Conditions)

Let $a, b \in \mathbb{Z}$ be nonzero, and let $d = \gcd(a, b)$. Then

- $\frac{a}{d}$ and $\frac{b}{d}$ are coprime.
- Write $a = dk$ for some $k \in \mathbb{Z}$. Then for $y \in \mathbb{Z}$, if $a|(dy)$, then $k|y$.

§1.4 Introduction to Modular Arithmetic

Let us start with a motivating example.

Remark 1.14. When learning a new topic, try to find the **motivation** behind every idea. This will allow you to realize when to use what idea!

Example 1.15

Suppose it is 1 : 00 now. What time will it be exactly 1000 hours from now?

Solution. The key to solving this problem is realizing that the times will repeat themselves every 12 hours. In other words, the time will be 1 : 00 whenever the number of hours from now is a multiple of 12.

What is the multiple of 12 that is closest to 1000? After some experimentation, we see that the closest multiple is 996, so 996 hours from now it will be 1 : 00 as well. Thus, exactly 1000 hours from now the time will be $\boxed{5:00}$. □

For example, because $4, 16, 1000$, and 4252 all share the same remainder when divided by 12, the following equation is valid:

$$4 \equiv 16 \equiv 1000 \equiv 4252 \pmod{12}.$$

§2 Modular Congruences

Let us start with a problem involving congruences:

Example 2.1

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 start by listing 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. □

§2.1 Congruences

Definition 2.2 (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 $y \equiv x \pmod a$.

Theorem 2.3 (Congruence Condition)

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

$$x = z_1 a + w, \text{ and}$$
$$y = z_2 a + w,$$

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

Example 2.4

How many positive integers less than 12 are relatively prime to 12?

§2.2 Fermat's Little Theorem and Euler's Totient Theorem

Solution. We know that $1, 5, 7$, and 11 are relatively prime to 12, so the answer is 4. □

What if we replaced 12 with 100? Or what if we used 10000? That would take a **very** long time. So instead we use **Euler's totient function**:

Definition 2.5 (Euler's Totient Function) — The totient function $\phi(n)$ is defined as the number of positive integers less than n that are relatively prime to n.

Remark 2.6. Definitions are very important. If we had defined it by the theorem, it would be so much harder to relate it to relatively prime. There also would have been no motivation for this idea.

Theorem 2.7 (Euler's Totient Function)
If $n = p_1^{e_1} p_2^{e_2} \cdots p_m^{e_m}$, then $\phi(n)$

$$\phi(n) = n\left(1 - \frac{1}{p_1}\right)\left(1 - \frac{1}{p_2}\right)\cdots\left(1 - \frac{1}{p_m}\right).$$

Now for a few identities:

- For prime p, $\phi(p) = p - 1$, because all numbers less than p are relatively prime to it.
- For relatively prime a, b, $\phi(a)\phi(b) = \phi(ab)$.
- In fact, we also have for any a, b that $\phi(a)\phi(b)\gcd(a, b) = \phi(ab)\phi(\gcd(a, b))$.
- If p is prime and $n \geq 1$,then $\phi(p^n) = p^n - p^{n-1}$.

There isn't much to learn about the Totient Function, since it appears very rarely. Let us turn to its relation with **modular arithmetic**. There are always the problems that ask for the last two/three/four/etc. digits of some large operation (for example, 102^{43}. Even using a calculator won't help. So instead, we use the following methods:

Theorem 2.8 (Fermat's Little Theorem)
Let p be a prime number and a be an integer relatively prime to p. Then

$$a^{p-1} \equiv 1 \pmod{p}.$$

Remark 2.9. However, remember: only use powerful techniques when you have to. If the problem is find the last digit of 2^4, the following methods will be *overkill*.

Let's try an example:

Example 2.10
Find the remainder when 2^{304} is divided by 7.

Solution. Using Fermat's Little Theorem with $a = 2$ and $p = 7$, we get

$$2^6 \equiv 1 \pmod{7}.$$

Note that

$$2^{304} = 2^{300} \cdot 2^4 = (2^6)^{50} \cdot 2^4,$$

so

$$(2^6)^{50} \cdot 2^4 \equiv 1^{50} \cdot 16 \equiv 16 \equiv 2 \pmod{7}.$$

□

Notice how Fermat's Little Theorem doesn't directly answer the problem, but by taking out all the 2^6s, we were able to get our answer. However, this leaves us with an issue - what if the modulo isn't prime? For example, to find the last digit, we have to take mod 10, but 10 isn't prime. How can we solve the problem?

Theorem 2.11 (Euler's Totient Theorem)
Let a and n be relatively prime integers. Then

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

Remark 2.12. Notice that this is a generalized form of Fermat's Little Theorem.

Let's turn to an example:

Example 2.13
Find the last two digits of 3^{83}.

Solution. We know that this is the same as taking mod 100. Using Euler's Totient Theorem with $a = 3$ and $n = 100$, we get

$$3^{\phi(100)} \equiv 1 \pmod{100}.$$

Using the formula for finding $\phi(n)$, we get $\phi(100) = 40$. Thus,

$$3^{40} \equiv 1 \pmod{100}.$$

Notice that

$$3^{83} = 3^{80} \cdot 3^3 = (3^{40})^2 \cdot 3^3,$$

so

$$(3^{40})^2 \cdot 3^3 \equiv 1^2 \cdot 27 \equiv 27 \pmod{100},$$

so the last two digits are 27. □

§2.3 Exercises

Exercise 2.14. How many numbers under 1000 are relatively prime to 1000?

Exercise 2.15. Find the value of $\phi(12)$ and $\phi(1001)$.

Exercise 2.16. Find the last two digits of 312^{84}.

Exercise 2.17. Find the last two digits of $6^{40} + 8^{40}$. (Note: this question is hard! You cannot apply any of the theorems listed above on your first step, since 6 and 8 are not relatively prime to 100)

Exercise 2.18. Find $\phi(\phi(1000))$.

Exercise 2.19. Jimmy takes a one digit number to the fourth power and the last digit is 1. He takes it to the fifth power and the last digit is 3. What is his number?

§3 Residues

§3.1 Introduction

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

§3.2 Residue Classes

We begin with a problem.

Example 3.1

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

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 from all sides gives us

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

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

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

□

We can now define a residue class.

Definition 3.2 (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 $10 \pmod{12}$.

§3.3 Exercises

Exercise 3.3. Determine the modulo-9 residue of each of the following.

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

Exercise 3.4. 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

Exercise 3.5. Show that if $x \equiv y \pmod{a}$ and $y \equiv z \pmod{a}$, then $x \equiv z \pmod{a}$.

§4 Operations in Modular Arithmetic

§4.1 Modular Addition & Subtraction

Theorem 4.1 (Modular Addition and Subtraction)

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

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

Proof. From the definition of congruence, we have

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

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

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

□

Exercise 4.2. Is $54 + 42 \equiv 2 + 14 \pmod 8$? Is $69 - 45 \equiv 18 - 15 \pmod 3$?

Exercise 4.3. Let a, b, and c be integers whose residues modulo 8 are 4, 5, and 7, respectively. Compute the residue of $a + b + c \pmod 8$.

§4.2 Modular Multiplication

Theorem 4.4 (Modular Multiplication)

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

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

then

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

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

$$a = b + xm$$
$$c = d + ym$$

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, $ac \equiv bd \pmod m$. □

Exercise 4.5. Is $9 \cdot 43 \equiv 8 \cdot 98 \pmod{23}$?

Exercise 4.6. Find the modulo 4 residue of 100!.

Exercise 4.7. The residues of 3 positive integers modulo 8 are $1, 4$, and 7. Find the residue of their products modulo 8.

§4.3 Modular Exponentiation

Theorem 4.8 (Modular Exponentiation)
Let a and b be integers, and c be a natural number. If $a \equiv b \pmod{m}$, then

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

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.

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

□

Exercise 4.9. Is $24^{14} - 15^{14}$ divisible by 9?

Exercise 4.10. Find residue r such that $5^{6001} \equiv r \pmod{7}$.

§4.4 Modular Division

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

§4.5 Modular Inverses

Definition 4.11 (Modular Inverse) — The **multiplicative inverse** of an integer $a \pmod{m}$ is the integer

a^{-1} such that

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

Example 4.12

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

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. □

Theorem 4.13 (Existence of Modular Inverse)

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

Proof. 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 $\gcd(a, n) = 1$. □

Exercise 4.14. Does 6 modulo 25 have an inverse? Why?

Exercise 4.15. Find all possible residues modulo 20 that have inverses.

From the exercise above, it is pretty hard to find modular inverses. So how can we speed up the process? Let's start with an example:

Example 4.16

Find the inverse of 3 modulo 7.

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 rather tedious for larger moduli and inverses - we need a systematic way to find inverses. □

§4.6 The Euclidean Algorithm

The **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.

Theorem 4.17 (Euclidean Algorithm)

The Euclidean Algorithm is defined on input a, b, with $|a| > |b|$, and produces output $\gcd(a, b)$. The algorithm proceeds as follows:

- Initialize $r_0 = |a|$, $r_1 = |b|$.
- While $r_n > 0$: define r_{n+1} to be the remainder of r_{n-1} divided by r_n.
- If $r_n = 0$, then $r_{n-1} = \gcd(a, b)$.

Proof. Let a, b, q, r be as in the statement of the theorem. Let $d = \gcd(a, b)$. Notice that as $r = a - bq$, and both a and b are divisible by d, then r is divisible by d as well.

Moreover, suppose that d' is an integer such that $d'|r$ and $d'|b$. Then since $a = qb + r$, we must also have that $d'|a$. But then as $d = \gcd(a, b)$, we have that $d'|d$. Hence, any divisor of both r and b is also a divisor of d.

Therefore, d meets the definition of gcd for b and r. By uniqueness of the positive gcd, we therefore have that $d = \gcd(b, r)$. □

Now, let's try an example using the Euclidean Algorithm.

Example 4.18

Find the inverse of 37 modulo 97.

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 $21 \cdot 37 \equiv 1 \pmod{97}$. □

Exercise 4.19. Find the inverse of 5 modulo 6.

Exercise 4.20. Find the inverse of 19 modulo 21.

Exercise 4.21. Find x such that $17x \equiv 1 \pmod{23}$.

§5 Chinese Remainder Theorem

§5.1 Linear Congruences

Definition 5.1 (Linear Congruence Equation) — A **linear congruence equation** is a congruence that has a variable raised only to the first power.

Theorem 5.2 (Form of Linear Congruence)

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 examples.

Example 5.3

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. $x + 12 \equiv 3 \pmod 5$.

Solution. The numbering is the same as in the questions before:

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 $x \equiv -9 \equiv \boxed{1} \pmod 5$.

□

Example 5.4

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. $2x - 4 \equiv 2 \pmod 5$.

Solution. The numbering is the same as in the questions before:

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 $\pmod 5$, 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 examples, 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.

Exercise 5.5. Find all possible values of x such that $23x \equiv 14 \pmod{15}$.

Exercise 5.6. Find all possible values of x such that $23x + 234 \equiv 12 \pmod{15}$.

Exercise 5.7 (Introduction to Number Theory)**.** Let y be a positive integer. Prove that if $ay \equiv by \pmod{my}$ for integers a and b, then $a \equiv b \pmod m$.

Let's try a few systems of linear congruences.

Example 5.8

Find all x such that

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

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 $\boxed{x \equiv 0 \pmod{10}}$. □

Let's tackle a harder example.

Example 5.9

Find all possible values of x such that

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

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

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

□

Example 5.10

Find all x such that

$$\begin{aligned} x &\equiv 3 \pmod{4} \\ x &\equiv 2 \pmod{7}. \end{aligned}$$

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 $4 \pmod{7}$, which is 2. Thus, we have

$$\begin{aligned} 4a &\equiv 6 \pmod{7} \\ 2 \times 4a &\equiv 2 \times 6 \pmod{7} \\ 8a &\equiv 12 \pmod{7} \\ 8a &\equiv 5 \pmod{7} \\ 1a &\equiv 5 \pmod{7} \\ a &\equiv 5 \pmod{7}. \end{aligned}$$

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

$$\begin{aligned} 23 &\equiv 3 \pmod 4 \\ 23 &\equiv 2 \pmod 7 \end{aligned}$$

we subtract 23 from both sides of the congruences:

$$\begin{aligned} x - 23 &\equiv 3 - 3 \equiv 0 \pmod 4 \\ x - 23 &\equiv 2 - 2 \equiv 0 \pmod 7. \end{aligned}$$

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

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

□

Let us now turn to a few harder systems.

Example 5.11

Find all x such that

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

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 $5 \pmod 6$. 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

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

□

§5.2 Chinese Remainder Theorem

Before we dive right into Chinese Remainder Theorem (abbreviated CRT), let us look at an example that does **not** require CRT:

Example 5.12

Mr. Yu wants to divide the class into groups. When he tries to divide into groups of 3, 1 student is left over. When he tries to divide into groups of 4, 1 student is left over. And when he tries to divide into groups of 5, 1 student is left over. What is the least number of students he could have, assuming he has more than 1 student?

Solution. We simply write these equations in terms of mods. If the number of students he has is n, then

$$n \equiv 1 \pmod 3,$$

$$n \equiv 1 \pmod 4,$$

$$n \equiv 1 \pmod 5.$$

To the first two equations, we realize that one works. One also works for the third equation, but because we have to find the next greatest equation, we add $3 \cdot 4 \cdot 5$ to get $n = 61$. □

In general, we have

Theorem 5.13 (Special Case of Linear Congruences)
If $n \equiv c \pmod{m_1} \equiv c \pmod{m_2} \equiv \ldots \equiv c \pmod{m_k}$ (all of these variables are integers), then

$$n \equiv c \pmod{m_1 m_2 m_3 \ldots m_k} \equiv c \pmod{\operatorname{lcm}(m_1, m_2, m_3, \ldots, m_k)}.$$

This directly implies the following formula:

Corollary 5.14 (Special Case Corollary)
If

$$n \equiv c \pmod{m_1 m_2 m_3 \ldots m_k},$$

and

$$d | m_1 m_2 m_3 \ldots m_k$$

for some random integer d, then

$$n \equiv c \pmod d.$$

Let us return to CRT now. We start with an example as usual.

Example 5.15
Find all integers x such that

$$x \equiv 1 \pmod{10},$$
$$x \equiv 4 \pmod{12}.$$

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:

$$\begin{cases} x \equiv 0 \pmod 2, \\ x \equiv 0 \pmod 5 \end{cases} \Rightarrow x \equiv 0 \pmod{10}$$

$$\begin{cases} x \equiv 1 \pmod 3, \\ x \equiv 0 \pmod 7 \end{cases} \Rightarrow x \equiv 7 \pmod{21}$$

$$\begin{cases} x \equiv 3 \pmod 4, \\ x \equiv 2 \pmod 7 \end{cases} \Rightarrow x \equiv 23 \pmod{28}$$

$$\begin{cases} x \equiv 1 \pmod{10}, \\ x \equiv 4 \pmod{12} \end{cases} \Rightarrow \text{no solutions}$$

□

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:

§5.3 Chinese Remainder Theorem

Theorem 5.16 (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 $x \equiv c \pmod{mn}$.

Exercise 5.17. Find all x such that

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

Exercise 5.18. Find all x such that

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

Exercise 5.19. Find the smallest possible positive value of n such that

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

§6 Worked Out Examples

Example 6.1

A quick refresher:

(a) What are the remainders when $3333 + 4444$ and $3333 \cdot 4444$ are divided by 5?

(b) What is the remainder when 7^{2015} is divided by 48?

Solution. The numbering corresponds to the numbering above:

(a) We have $3333 \equiv 3 \pmod 5$ and $4444 \equiv 4 \pmod 5$, so $3333 + 4444 \equiv 3 + 4 \equiv 7 \equiv \boxed{2} \pmod 5$. Similarly, $3333 \cdot 4444 \equiv 3 \cdot 4 \equiv 12 \equiv \boxed{2} \pmod 5$. In general, we can take any integer and replace it with an integer within the same residue class. We can do this multiple times within a problem.

(b) At first, it seems that even modular arithmetic can't prevent this problem from becoming messy. However, upon further inspection, we can see that $7^2 = 49$, which leaves a remainder of 1 when divided by 48! Hence, we can write

$$7^{2015} \equiv 7 \cdot (7^2)^{1007} \equiv 7 \cdot 1^{1007} \equiv \boxed{7} \pmod{48}.$$

□

Example 6.2

What are the last two digits of the integer 17^{198}?

Solution. Note that $17^2 \equiv 289 \equiv -11 \pmod{100}$. Thus, the problem is simplified to computing $(-11)^{99} \equiv -11^{99} \pmod{100}$. Now note that by the Binomial Theorem

$$11^{99} = (10+1)^{99} = 10^{99} + \cdots + \binom{99}{2}10^2 + \binom{99}{1}10^1 + 1.$$

When this expansion is reduced modulo 100, all but the last two terms will go away since they are all divisible by 100, so $11^{99} \equiv \binom{99}{1} \cdot 10 + 1 \equiv 91 \pmod{100}$. As a result, $17^{198} \equiv -91 \equiv \boxed{09} \pmod{100}$. □

Remark 6.3. There are some instances where modular division works. Don't count on it all the time, however.

Example 6.4

A few proofs:

(a) Prove that any integer is divisible by 2^n iff the integer formed by its last n digits is also divisible by 2^n.

(b) Let $N = \overline{a_0 a_1 a_2 \ldots a_n}$ be an integer. (The bar above the previous expression suggests the variables are digits and that we are not multiplying them together.) Prove that N is divisible by 9 iff

$$a_0 + a_1 + a_2 + \cdots + a_n$$

is also divisible by 9.

Solution. (a) Let Y be the integer formed by the last n digits and let X be the integer formed by the digits to the left of these n digits. For example, in the 124564 case above, $X = 1245$ and $Y = 64$. Note that the integer can thus be written as $10^n X + Y$. Now note that $10^n \equiv (2^n)(5^n) \equiv 0 \pmod{2^n}$, so $10^n X + Y \equiv Y \pmod{2^n}$. This immediately implies the conclusion.

(b) Note that N can be written more mathematically as

$$N = a_0 \cdot 10^n + a_1 \cdot 10^{n-1} + a_2 \cdot 10^{n-2} + \cdots + a_{n-1} \cdot 10 + a_n.$$

We attempt to simplify this modulo 9. The key here is to note that $10 \equiv 1 \pmod 9$. This further implies that $10^2 \equiv 1 \pmod 9$, $10^3 \equiv 1 \pmod 9$, and so on. Making all the necessary substitutions gives

$$N \equiv a_0 + a_1 + a_2 + \cdots + a_n \pmod 9.$$

Thus N and the sum of the digits of N give the same remainder upon division by 9, implying the conclusion. □

Example 6.5

I am thinking of a number. All I can give to you is that if you triple my number, it leaves a remainder of 13 when divided by 17. Unfortunately, this is clearly not enough information to figure out my number. However, it is enough information to figure out what the remainder of my original number is when divided by 17. What is this remainder?

Solution. A one-line solution: $\frac{17+13}{3} = \boxed{10.}$ □

Example 6.6

Find the remainder when 5^{15} is divided by 128.

Solution. Apply the rules from before:

$$(5^3)^5 \equiv (-3)^5 \equiv -243 \equiv \boxed{13} \pmod{128}.$$

□

Example 6.7

Find the remainder when 12^9 is divided by 1000.

Solution. Apply the rules from before:

$$12^9 \equiv (1728)^3 \equiv (-272)^3 \equiv 984 \cdot (-272) \equiv (-16) \cdot (-272) \equiv \boxed{352} \pmod{1000}.$$

□

Example 6.8

Calculate $\gcd(67620, 66234)$.

Solution. This looks atrocious, but it's not really. First, we can write

$$67620 = 66234 * 1 + 1386.$$

Therefore, by the Euclidean Algorithm, we have that $\gcd(67620, 66234) = \gcd(66234, 1386)$.

Wash, rinse, repeat.

$$66234 = 1386 * 47 + 1092.$$

$$1386 = 1092 * 1 + 294.$$

$$1092 = 294 * 3 + 210.$$

$$294 = 210 * 1 + 84.$$

$$210 = 84 * 2 + 42.$$

$$84 = 42 * 2 + 0.$$

□

Example 6.9 (Paraguay 2012)

Define a list of numbers with the following properties:

- The first number of the list is a one-digit natural number.
- Each number (since the second) is obtained by adding 9 to the number before in the list.
- The number 2012 is in that list.

Find the first number of the list.

Solution. Notice that they all are of the same residue modulo 9. Thus,

$$2012 \equiv \boxed{5} \pmod 9.$$

□

Example 6.10 (AMC 8 2014)

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

Solution. Observe that

$$7 + 4 + A + 5 + 2 + B + 1 \equiv A + B + 19 \equiv A + B + 1 \pmod 3,$$

so $A + B \equiv 2 \pmod 3$. From the second number, we have

$$3 + 2 + 6 + A + B + 4 + C \equiv A + B + C \equiv 0 \pmod 3,$$

so we must have $C \equiv 1 \pmod 3$. Thus, $C = 1, 4, 7$, so our answer is $1 + 4 + 7 = \boxed{12}$. □

Example 6.11 (Mock AMC 10)

The integers a, b, c, and d are four distinct prime numbers. If $d = a^2b^2 - 49c^2$, then what is the minimum possible value of $a + b + c$?

Solution. Factor to get $d = (ab - 7c)(ab + 7c)$. Observe that d is prime, so we must have $ab - 7c = 1$. By trial and error, we find that $(a, b, c, d) = (3, 5, 2, 29)$ works, so our answer is $3 + 5 + 2 = \boxed{10}$. □

Example 6.12 (iTest 2007)
Find the remainder when $1 + 2 + \cdots + 2007$ is divided by 1000.

Solution. A simple addition in modular arithmetic:

$$\frac{2007 \cdot 2008}{2} \equiv 2007 \cdot 1004 \equiv 7 \cdot 4 \equiv \boxed{28} \pmod{1000}.$$

□

Example 6.13 (Purple Comet HS 2013)
There is a pile of eggs. Joan counted the eggs, but her count was off by 1 in the 1's place. Tom counted in the eggs, but his count was off by 1 in the 10's place. Raoul counted the eggs, but his count was off by 1 in the 100's place. Sasha, Jose, Peter, and Morris all counted the eggs and got the correct count. When these seven people added their counts together, the sum was 3162. How many eggs were in the pile?

Solution. We must have

$$3162 + 100a + 10b + c \equiv 0 \pmod{7},$$

where a, b, and c are each ± 1. Simplifying mod 7, we have $5 + 2a + 3b + c \equiv 0 \pmod{7}$. Observe that $(a, b, c) = (-1, 1, 1)$ works, so our answer is

$$\frac{3162 - 100 + 10 + 1}{7} = \boxed{439.}$$

□

Example 6.14 (Mandelbrot 2008-09)
Determine the smallest positive integer m such that $m^2 + 7m + 89$ is a multiple of 77.

Solution. We split it up mod 7 and mod 11.

Mod 7:

$$m^2 + 7m + 89 \equiv m^2 + 5 \equiv 0 \pmod{7},$$

so $m \equiv 3, 4 \pmod{7}$.

Mod 11:

$$m^2 + 7m + 89 \equiv m^2 - 4mm + 1 \equiv (m-2)^2 - 3 \equiv 0 \pmod{11},$$

so $m \equiv 7, 8 \pmod{11}$.

Now, we just combine these two equivalences in all four possible ways to find our minimum solution. It turns out that $m = \boxed{18}$ is the minimum. □

Remark 6.15. A common strategy is to split up the primes of the modulo, i.e.

$$p_1^{e_1}, p_2^{e_2}, p_3^{e_3}, \ldots,$$

where

$$N = \prod_{p \in \mathbb{P}} p^{e_i} = 2^{e_1} \cdot 3^{e_2} \cdot 5^{e_3} \cdot \ldots.$$

Example 6.16

Prove that every year, including any leap year, has at least one Friday 13-th.

Solution. It is enough to prove that each year has a Sunday the 1st. Now, the first day of a month in each year falls in one of the following days:

Month	Day of the Year	mod 7
January	1	1
February	32	4
March	60 or 61	4 or 5
April	91 or 92	0 or 1
May	121 or122	2 or 3
June	152 or 153	5 or 6
July	182 or183	0 or 1
August	213 or 214	3 or 4
September	244 or 245	6 or 0
October	274 or 275	1 or 2
November	305 or 306	4 or 5
December	335 or 336	6 or 0

(The above table means that, depending on whether the year is a leap year or not, that March 1st is the 50th or 51st day of the year, etc.) Now, each remainder class modulo 7 is represented in the third column, thus each year, whether leap or not, has at least one Sunday the 1st. □

§7 Problems

Problem 7.1 (AIME I 2010)**.** Find the remainder when $9 \times 99 \times 999 \times \cdots \times \underbrace{99\cdots9}_{999\ 9\text{'s}}$ is divided by 1000.

Problem 7.2 (AMC 10 B 2010)**.** 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?

Problem 7.3 (AMC 12 A 2010)**.** The number obtained from the last two nonzero digits of 90! is equal to n. What is n?

Problem 7.4 (AHSME 1995)**.** 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?

Problem 7.5 (AMC 8 1999)**.** What is the remainder when 1999^{2000} is divided by 5?

Problem 7.6 (AMC 10 B 2009)**.** What is the remainder when $3^0 + 3^1 + 3^2 + \ldots + 3^{2009}$ is divided by 8?

Problem 7.7. Prove the following results:

- If b is even and $b|a$, then a is even.
- If $a, b \in \mathbb{Z}$ and $a \geq 2$, then a does not divide one of b or $b+1$.
- If ab is even, then one of a or b is even.
- If $a|b$ and $b|c$, then $a|c$.

Problem 7.8 (USAJMO 2013)**.** Are there integers a and b such that a^5b+3 and ab^5+3 are both perfect cubes of integers?

§A Appendix A: List of Theorems, Corollaries, and Definitions

List of Theorems and Corollaries

List of Definitions