Modular Arithmetic Part 1 Handout

James Stewart

13 May 2024

Credit to evan.sty for the LaTeX package.

§1 Modular Arithmetic Part 1 Handout

§1.1 Introduction

Definition 1.1. If m, n, and k are integers, we have

$$n \equiv m \pmod{k}$$

if and only if $n - m$ is an multiple of $k > 1$. If $n \equiv m \pmod{k}$, we say that n is congruent to $m \pmod{k}$.

Definition 1.2. The **residue** of $m \pmod{k}$ is the value n for which $0 \leq n < k$ and $n \equiv m \pmod{k}$.

Theorem 1.3

If $m \equiv a \pmod{k}$ and $n \equiv b \pmod{k}$, then $m + n \equiv a + b \pmod{k}$.

Proof. If $m \equiv a \pmod{k}$, there exists an integer c so that $m - a = ck$ (since $m - a$ is a multiple of k). Similarly, there exists an integer d so that $n - b = dk$. Adding these two equations gives

$$m - a + n - b = ck + dk.$$

Therefore, we have

$$m + n - a - b = k(c + d),$$

so $m + n \equiv a + b \pmod{k}$. □

Theorem 1.4

Prove that

$$(m + ak)(n + bk) \equiv mn \pmod{k}$$

for all integers m, n, a, b, k.

Proof. Expanding, we are left to prove that

$$mn + mbk + akn + abk^2 \equiv mn \pmod{k}.$$

Subtracting mn from both sides, we have to prove that

$$k(mb + an + abk) \equiv 0 \pmod{k}.$$

Since $mb+an+abk$ is an integer, $k(mb+an+abk) = k(mb+an+abk)-0$ is a multiple of k and therefore

$$k(nq + lm + lqk) \equiv 0 \pmod{k}.$$

□

Theorem 1.5

Define positive integers a and b which have units digits m and n, respectively. The units digit of mn is the units digit of ab.

Proof. By the previous theorem,

$$(m + 10r)(n + 10s) \equiv mn \pmod{10}$$

for some r and s. We can choose r and s so that $m + 10r = a$ and $n + 10s = b$ (since $m \equiv a \pmod{10}$ and $n \equiv b \pmod{10}$). Since $m + 10r = a$ and $n + 10s = b$,

$$ab \equiv mn \pmod{10}$$

and $ab - mn$ is a multiple of 10. Therefore, ab and mn have the same units digit. □

Example 1.6

How many numbers in the list $1, 2, \ldots, 1000$ are congruent to $1 \pmod{10}$?

If a number is congruent to $1 \pmod{10}$, then its units digit must be 1. There are $\boxed{100}$ numbers that have a units digit of 1 in the list: $0 \cdot 10 + 1, 1 \cdot 10 + 1, \ldots, 99 \cdot 10 + 1$.

Example 1.7

A positive integer n is randomly selected. Find the probability that it is congruent to $3 \pmod{7}$.

Recall that if $n \equiv 3 \pmod{7}$, then n leaves a remainder of 3 when divided by 7. If we choose n randomly, there are 7 possible remainders: $0, 1, 2, 3, 4, 5, 6$. The probability that we have a remainder of 3 is $\boxed{\frac{1}{7}}$.

§1.2 Inverses and Systems

Definition 1.8. For positive integers m and n satisfying $\gcd(m, n) = 1$, the inverse of $m \pmod{n}$ is the unique integer m^{-1} where

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

Example 1.9

Find the smallest positive integer n that satisfies the following property:

$$4n \equiv 8 \pmod{5}.$$

Since $8 \pmod{5} \equiv 3 \pmod{5}$, we are trying to find the smallest n satisfying

$$4n \equiv 3 \pmod{5}.$$

Multiplying both sides by

$$4^{-1} \pmod{5} \equiv 4 \pmod{5},$$

we know that

$$n \equiv 12 \pmod{5},$$

so our answer is $\boxed{2}$.

Example 1.10

Find the smallest positive integer n that satisfies the following properties:

$$n \equiv 2 \pmod{5}$$

$$n \equiv 3 \pmod{7}.$$

We know that

$$n = 5a + 2 = 7b + 3$$

for some integers a and b. We focus on

$$5a + 2 = 7b + 3.$$

Taking this equation $\pmod{5}$, we know that

$$2 \equiv 2b + 3 \pmod{5}.$$

Simplifying, we have

$$4 \equiv 2b \pmod{5}.$$

The smallest value is $b = 2$, so our answer is $7 \cdot 2 + 3 = \boxed{17}$.

Example 1.11

Find the second-smallest positive integer n that satisfies the following properties:

$$n \equiv 1 \pmod{2}$$

$$n \equiv 1 \pmod{3}$$

$$n \equiv 1 \pmod{4}$$

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

We know that

$$n = 2a + 1 = 3b + 1 = 4c + 1 = 5d + 1$$

for some integers a, b, c, and d. We know that

$$n - 1 = 2a = 3b = 4c = 5d.$$

Since a, b, c, and d are integers, $n - 1$ must be a multiple of 2, 3, 4, and 5. The smallest possible value of n is 1, and the second smallest is $1 + \text{lcm}(2, 3, 4, 5) = \boxed{61}$.

Example 1.12

Find the smallest positive integer n that satisfies the following properties:

$$n \equiv 1 \pmod 2$$

$$n \equiv 2 \pmod 3$$

$$n \equiv 3 \pmod 4$$

$$n \equiv 4 \pmod 5.$$

We know that

$$n = 2a + 1 = 3b + 2 = 4c + 3 = 5d + 4$$

for some integers a, b, c, and d. We can replace $a_1 = a + 1$, $b_1 = b + 1$, $c_1 = c + 1$, and $d_1 = d + 1$:

$$n = 2a_1 - 1 = 3b_1 - 1 = 4c_1 - 1 = 5d_1 - 1.$$

We continue as we did in the previous problem: $n+1$ must be a multiple of $\text{lcm}(2, 3, 4, 5) = 60$. Our answer is $\boxed{59}$.

§1.3 Find $2^{100} \pmod 7$

Example 1.13

Find $2^{100} \pmod 7$.

We try to replace 100 with a small value in hope of finding a pattern.

$$2^1 \equiv 2 \pmod 7$$

$$2^2 \equiv 4 \pmod 7$$

$$2^3 \equiv 1 \pmod 7$$

$$2^4 \equiv 2 \pmod 7$$

$$2^5 \equiv 4 \pmod 7$$

$$2^6 \equiv 1 \pmod 7$$

It seems like $2, 4, 1, 2, 4, 1 \ldots$ repeats.

We need to prove that if we have one term that has already repeated (in this case, the first term that has already repeated is 2, 4, 1, **2**. Now, we prove that the next value is 4 (without finding 2^5). We know that $2^1 \cdot 2 \equiv 2^2 \pmod 7$, implying

$$2 \cdot 2 \equiv 4 \pmod 7.$$

In this sequence of powers of $2 \pmod 7$, we know that 4 *always* comes right after 2. Therefore, the next term in the sequence $2, 4, 1, 2$ will be 4. Similarly, we can prove that 1 always comes after 4, so the sequence is now

$$2, 4, 1, 2, 4, 1.$$

In addition, 2 always comes after 1, and the sequence will become

$$2, 4, 1, 2, 4, 1, 2.$$

We already know that 4 always comes after 2, and so on, so the sequence

$$2, 4, 1, 2, 4, 1, 2, 4, 1, \ldots$$

repeats.

We now know that $2^1 \equiv 2^4 \equiv 2^7 \equiv \cdots \equiv 2^{100} \equiv 2 \pmod 7$ and we are done.

Suppose that we are trying to find a pattern on $a^n \pmod c$ for small values of n. We find $a^x \equiv a^y \pmod k$ where $x < y$ (a^x and a^y leave the same remainder when divided by k). Then, the block of remainders $\pmod k$ from a^x to a^{y-1} (there will be $y - x$ remainders in the block) will repeat. In the case of the problem above, $x = 1$ and $y = 4$. As expected, there are $4 - 1 = 3$ remainders in the repeating block: $2, 4, 1$.

In general, try to find a pattern or a block of digits that repeats.

§1.4 Euler's Theorem

Theorem 1.14

Let p be a prime and a be a positive integer satisfying $\gcd(a, p) = 1$. We have

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

(Fermat's Little Theorem)

Example 1.15

Find the remainder when 32^{100} is divided by 101.

This is a direct application of Fermat's Little Theorem. If $a = 32$ and $p = 101$, we have

$$32^{100} \equiv \boxed{1} \pmod{101}.$$

Example 1.16

Find the remainder when 32^{101} is divided by 101.

In the previous problem, we saw that $32^{100} \equiv 1 \pmod{101}$. Multiplying this by 32, we have

$$32^{101} \equiv \boxed{32} \pmod{101}.$$

Definition 1.17. For a positive integer n, $\phi(n)$ is the number of integer values $0 < a \leq n$ for which $\gcd(a, n) = 1$.

Example 1.18

Find $\phi(100)$.

We want to find the number of integer values $0 < a \leq 100$ for which a is not a multiple of 2 or 5. If we randomly select a value for a in that range, there is a $\frac{1}{2}$ chance it will not be a multiple of 2 and a $\frac{4}{5}$ chance it will not be a multiple of 5. Since 2 and 5 are relatively prime,

$$\phi(100) = 100 \cdot \frac{1}{2} \cdot \frac{4}{5} = \boxed{40}.$$

Theorem 1.19

Let the prime factorization of n be

$$n = p_1^{a_1} p_2^{a_2} p_3^{a_3} \dots p_n^{a_n}.$$

We have

$$\phi(n) = n(1 - \frac{1}{p_1})(1 - \frac{1}{p_2})(1 - \frac{1}{p_3}) \dots (1 - \frac{1}{p_n}).$$

Theorem 1.20

Let a and n be relatively prime positive integers. We have

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

We notice that Fermat's Little Theorem is a case of this theorem when n is prime ($\phi(p) = p - 1$ for all primes p). (Euler's Theorem)

Example 1.21

Find the remainder when 19^{40} is divided by 100.

Applying Euler's Theorem to $a = 19$ and $n = 100$ gives $19^{\phi(100)} \equiv 1 \pmod{100}$. Since $\phi(100) = 40$, our answer is $\boxed{1}$.

§1.5 Problems

Problem 1

Find the units digit of $42387 \cdot 234895302$.

Problem 2

Let n be a positive integer congruent to $3 \pmod{5}$. Find the value of $7n \pmod{5}$.

Problem 3

Find $6^{2024} \pmod{5}$.

Problem 4

Find the units digit of 7^{800}.

Problem 5

Prove that 6^n ends in 6 for all positive integers n.

Problem 6

Find the remainder when 2^{100} is divided by 100.

Problem 7

Find the remainder when 3^{2002} is divided by 100.

Problem 8

A positive integer n is *strange* if and only if $7^n - 3^n$ is divisible by 10. Find the number of strange values of n between 1 and 2024, inclusive.

Problem 9

How many positive integers $n < 2024$ satisfy the property that $\gcd(n, 2024) > 1$?

Problem 10

Find the number of positive integers $1 \leq n \leq 2024$ for which $1^n + 2^n + 3^n + \cdots + 9^n \equiv 0 \pmod{10}$.