1 Exercises

1.1

True or false? $91 \equiv 0 \pmod 7$. $3+5+7 \equiv 5 \pmod{10}$. $-2 \equiv 2 \pmod 8$. $11^2 \equiv 1 \pmod 3$.

True. True. False. True.

1.2

Complete the proof.

Then we can write $km = a - b$, implying $m|(a-b)$, which is the condition for $a \equiv b \pmod m$.

1.3

To what least residue $\pmod{11}$ is each of 23, 29, 31, 37 and 41 congruent?

1, 7, 9, 4, 8.

1.4

Say ”n is odd” in three other ways.

$n \equiv 1 \pmod 2$. $\exists q \ni n = 2q + 1$. $2|(n-1)$.

1.5

Prove that $p|a$ iff $a \equiv 0 \pmod p$.

First prove $a \equiv 0 \pmod p \Rightarrow p|a$. $a \equiv 0 \pmod p \Rightarrow p|(a-0) \Rightarrow p|a$. Now prove the converse, $p|a \Rightarrow a \equiv 0 \pmod p$. $p|a \Rightarrow \exists k \ni pk = a = a - 0$. So, by definition, $a \equiv 0 \pmod p$.

1.6

Prove parts **(a)**, **(b)**, **(c)**, **(d)**.

(a) $a \equiv a \pmod m$. If this is so, then $m|a-a$, or $m|0$. This is true for any m, since $0m = 0$.
(b) If $a \equiv b \pmod m$, then $b \equiv a \pmod m$. $a \equiv b \pmod m \Rightarrow \exists k \ni km = a - b$. If we multiply both sides of the equation by $-k$, have $-km = b - a$. So, $m|(b-a)$, which is equivalent to $b \equiv a \pmod m$.
(c) If $a \equiv b \pmod m$ and $b \equiv c \pmod m$, then $a \equiv c \pmod m$. The first statement implies $m|(a-b)$, the second that $m|(b-c)$. Since $m|k_1 \wedge m|k_2 \Rightarrow m|(k_1 + k_2)$, we know that $m|a-b+b-c$, or in other words, $m|(a-c)$.
(d) If $a \equiv b \pmod m$ and $c \equiv d \pmod m$, then $a+c \equiv b+d \pmod m$. Know $m|(a-b)$ and $m|(c-d)$. Adding the two, get $m|(a-b+c-d)$, which can be written as $m|(a+c)-(b+d)$.

1.7

Construct a counterexample for $ab \equiv ac \pmod m \wedge a \not\equiv 0 \pmod m \Rightarrow b \equiv c \pmod m$ for modulus 10.

$5 * 3 \equiv 5 * 5 \pmod{10}$, but $3 \not\equiv 5 \pmod{10}$.

1.8

What values of x satisfy

$$(a)\ 2x \equiv 4 \pmod 7\,? \quad (b)\ 2x \equiv 1 \pmod 7\,?$$

(a) $x = 2 \pmod 7$.
(b) $x = 4 \pmod 7$.

1.9

What x will satisfy $2x \equiv 4 \pmod 6$?

$x = 2 \pmod 3$.

2 Problems

2.1

Find the least residue of 1492 $\pmod 4$, $\pmod{10}$, and $\pmod{101}$.

0, 2, 78.

2.2

Find the least residue of 1789 $\pmod 4$, $\pmod{10}$, and $\pmod{101}$.

1, 9, 72.

2.3

Prove or disprove that if $a \equiv b \pmod m$, then $a^2 \equiv b^2 \pmod m$.

In order for this to be true, $m|(a^2 - b^2)$, or equivalently, $m|(a-b)(a+b)$. That $m|(a-b)$ is a given, so $a^2 \equiv b^2 \pmod m$.

2.4

Prove or disprove that if $a^2 \equiv b^2 \pmod m$, then $a \equiv b$ or $-b \pmod m$.

Like in the previous exercise, we know that $m|(a-b)(a+b)$. This is only possible if at least one of $m|(a-b)$ or $m|(a+b)$ is true. $m|(a-b) \Rightarrow a \equiv b \pmod m$ and $m|(a+b) \Rightarrow a \equiv -b \pmod m$.

2.5

Find all m such that $1066 \equiv 1776 \pmod m$.

By definition, these are all $m \ni m|710$. From the prime decomposition, we know $710 = 2 * 5 * 71$. So, all combinations of $2^{a_1} * 5^{a_2} * 71^{a_2}$, $a_i \in \{0, 1\}$ have this property: $m \in \{1, 2, 5, 71, 10, 142, 355, 710\}$.

2.6

Find all m such that $1848 \equiv 1914 \pmod m$.

By definition, these are all $m \ni m|66$. From the prime decomposition, we know $710 = 2 * 3 * 11$. So, all combinations of $2^{a_1} * 3^{a_2} * 11^{a_2}$, $a_i \in \{0, 1\}$ have this property: $m \in \{1, 2, 3, 11, 6, 22, 33, 66\}$.

2.7

If $k \equiv 1 \pmod 4$, then what is $6k + 5$ congruent to $\pmod 4$?

3.

2.8

Show that every prime (except 2) is congruent to 1 or 3 $\pmod 4$.

Assume $\exists p \neq 2$ such that p is prime and p not congruent to 1 or 3. By **Theorem 2**, we know that this means p must be congruent to 0 or 2. If $p \equiv 0 \pmod 4$, then $4|p$, and since 4 is not prime, neither is p. If $p \equiv 2 \pmod 4$, then $4|p-2$. For this to be true, p must be even. If p is even and not 2, then p is not prime.

2.9

Show that every prime (except 2 or 3) is congruent to 1 or 5 (mod 6).

Assume $\exists p \notin \{2,3\}$ such that p is prime and p not congruent to 1 or 5. By **Theorem 2**, we know that this means p must be congruent to 0, 2, 3, or 4. If $p \equiv 0 \pmod 6$, then $6|p$, and since 6 is not prime, neither is p. If p congruent to 2 or 4 (mod 6), then p must be even, and thus not prime. If p congruent to 3 (mod 6), then $6|p-3$. If $\exists k \ni 6k = p-3$, then $p = 6k+3$, meaning $3|p$. Since we know $p \neq 3$, this means p is not prime.

2.10

What can primes (except 2, 3, or 5) be congruent to (mod 30)?

As observed in the previous exercises, $p \equiv k \pmod{30} \Rightarrow (30-k)|p$. If 30 and k have a common divisor j, we can write $j(30/j - k/j)|p$, meaning $j|p$ and p is not prime. Such j must be all $j \in [1,29] \ni x|j, x \in \{2,3,5\}$ (we can exclude the trivial $k = 0$ case). So, the k that remain are $k \in \{1,7,11,13,17,19,23,29\}$.

2.11

In the multiplication $31415 * 92653 = 2910\ 93995$, one digit in the product is missing and all the others are correct. Find the missing digit without doing the multiplication.

$31415 * 92653 \equiv (3+1+4+1+5)(9+2+6+5+3) \equiv 14 * 25 \equiv (1+4)(2+5) \equiv 35 \equiv 8 \pmod 9$.
$291093995 \equiv 2+9+1+0+9+3+9+9+5 \equiv 47 \equiv 2 \pmod 9$.
For the equation to work, the missing digit must be 6.

2.12

Show that no square has as its last digit 2, 3, 7, or 8.

For a number k^2 to have as its last digit j, we must have $k^2 \equiv j \pmod{10}$. Every $k \in \mathbb{Z}$ must have a least residue $\in [0,9]$. $0^2 \equiv 0, 1^2 \equiv 1, 2^2 \equiv 4, 3^2 \equiv 9, 4^2 \equiv 6, 5^2 \equiv 5, 6^2 \equiv 6, 7^2 \equiv 9, 8^2 \equiv 4, 9^2 \equiv 1 \pmod{10}$. None of these residues $\in \{2,3,7,8\}$.

2.13

What can the last digit of a fourth power be?

Analogously to the previous exercise:
$0^4 \equiv 0, 1^4 \equiv 1, 2^4 \equiv 6, 3^1 \equiv 1, 4^4 \equiv 6, 5^4 \equiv 5, 6^4 \equiv 6, 7^4 \equiv 1, 8^4 \equiv 6, 9^4 \equiv 1 \pmod{10}$.
This implies that the last digit of a fourth power can be 0, 1, 5, or 6.

2.14

Show that the difference of two consecutive cubes is never divisible by 3.

Can write the consecutive cubes as k^3, $(k+1)^3 = k^3 + 3k^2 + 3k + 1$. So, the difference between the two is $3k^2 + 3k + 1 \equiv 1 \pmod 3$.

2.15

Show that the difference of two consecutive cubes is never divisible by 5.

Can write the difference between two cubes as $3k^2+3k+1 = 3k^2+3k+(5-4)$. For this to be divisible by 5, $3k^2+3k+5 \equiv 3k^2+3k \equiv 4 \pmod 5$. We know that any k has to be $\equiv j \pmod 5, j \in [0,4]$. Consider all the possible congruences of $3k^2+3k$:

$$3*0^2+3*0 \equiv 0, \quad 3*1^2+3*1 \equiv 1, \quad 3*2^2+3*2 \equiv 3,$$
$$3*3^2+3*3 \equiv 1, \quad 3*4^2+3*4 \equiv 3 \pmod 5$$

Since none of these are $\equiv 4 \pmod 5$, we've shown $5 \nmid (k+1)^3 - k^3$.

2.16

Show that

$$d_k 10^k + d_{k-1}10^{k-1} + ... + d_1 10 + d_0 \equiv d_0 - d_1 + d_2 - d_3 + ... + (-1)^k d_k \pmod{11}$$

and deduce a test for divisibility by 11.

Subtracting the right from the left side:

$$(d_0 - d_0) + (10+1)d_1 + (10^2-1)d_2 + ... + (10^k + (-1)^k)d_k$$

This will be divisible by 11 as long as $11|(10^k+1)$ for odd k and $11|(10^k-1)$ for even k. Equivalently, can write $10^k \equiv 10 \pmod{11}$ for odd k, $10^k \equiv 1 \pmod{11}$ for even k. From the first, we know $10^k - 10 = 10(10^{k-1}-1) \equiv 0 \pmod{11}$. Since $11 \nmid 10$, it must be that $11|(10^{k-1}-1)$, with $k-1$ even. From the second, we have $10^k - 1 \equiv 0 \pmod{11}$. So, all we need to show is that $11|10^k - 1$, or equivalently, $10^k \equiv 1 \pmod{11}$ for even k. We can show by inspection that this works for $k=2$ ($10^2-1 = 99$). Assume the property holds for all $k \le r$ for some even r. Now examine $r+2$. $10^{r+2} = 100 * 10^r \equiv 100 \equiv 1 \pmod{11}$.

The test for divisibility is as follows: starting from the right digit, alternate between subtracting and adding the digits to its left. If the result is divisble by 11 (can iterate until 0), then the number is divisible by 11:

$$121 \longrightarrow 1-2+1 = 0 \Rightarrow 11|121$$

$$2357947691 \longrightarrow 1-9+6-7+4-9+7-5+3-2 = -11 \Rightarrow 11|2357947691$$

2.17

A says, "27,182,818,284,590,452 is divisible by 11." *B* says, "No, it isn't." Who is right?

Using our divisibility rule,

$$2-5+4-0+9-5+4-8+2-8+1-8+2-8+1-7+2 = -22 = -2*11$$

A is correct.

2.18

A *palindrome* is a number that reads the same backward as forward. Examples are 22, 1331, and 935686539.
(a) Prove that every four-digit palindrome is divisible by 11. **(b)** What about six-digit palindromes?

(a) Four-digit palindromes can be written as $d_0d_1d_1d_0$, with d_i representing the number's digits. Applying our divisibility rules, we get $d_0 - d_1 + d_1 - d_0 = 0$, which is divisible by 11. Therefore, the original four-digit number was as well. **(b)** Six-digit palindromes can be written as $d_0d_1d_2d_2d_1d_0$, Applying our divisibility rules, we get $d_0 - d_1 + d_2 - d_2 + d_1 - d_0 = 0$, therefore also divisible by 11.

2.19

Show that if $n \equiv 4 \pmod 9$, then n cannot be written as the sum of three cubes.

Write $n = a^3 + b^3 + c^3 \equiv 4 \pmod 9$. Consider the possible values of $x^3 \pmod 9$:

$$\begin{aligned} 0^3 &\equiv 0, \quad 1^3 \equiv 1, \quad 2^3 \equiv 8, \\ 3^3 &\equiv 0, \quad 4^3 \equiv 1, \quad 5^3 \equiv 8, \\ 6^3 &\equiv 0, \quad 7^3 \equiv 1, \quad 8^3 \equiv 8 \end{aligned}$$

There is no way to sum any 3 numbers $\in 0, 1, 8$ such that the sum is $\equiv 4 \pmod 9$.

2.20

Show that for $k > 0$ and $m \geq 1$, $x \equiv 1 \pmod{m^k}$ implies $x^m \equiv 1 \pmod{m^{k+1}}$.

We can rewrite $x \equiv 1 \pmod{m^k}$ as $x = qm^k + 1$, for some q. Taking both sides to the m^{th} power, get $x^m = (qm^k + 1)^m = \Sigma_{i=0}^{m} \binom{m}{i} (qm^k)^i$. By inspection, all terms of this equation where $i \geq 2$ will be divisible by m^{k+1}, since all $\forall k \in \mathbb{Z}^+,\ 2k \geq k+1$. Consider the $i = 1$ term, $\binom{m}{1}(qm^k) = mqm_k = qm^{k+1}$. So, if we subtract 1 from this equation, all terms are divisbly by m^{k+1}. Thus, $x^m \equiv 1 \pmod{m^{k+1}}$.