Number Theory with python PROGRAMMING

Remainders

Lecture 2

Justin Stevens

Outline

Sum of First n Triangular Numbers I

Example. Find the sum of the first n triangular numbers.

Solution. We color the triangular numbers blue. We compute the top row by beginning with the circled 0 and adding the triangular number below it.

$$\begin{array}{ccccccccccccccccc}
0 & & 1 & & 4 & & 10 & & 20 & & 35 & & 56 & & 84 & & 120 \\
 & \color{blue}{1} & & \color{blue}{3} & & \color{blue}{6} & & \color{blue}{10} & & \color{blue}{15} & & \color{blue}{21} & & \color{blue}{28} & & \color{blue}{36} &
\end{array}$$

What are the two rows directly below this?

$$\begin{array}{ccccccccccccccccc}
0 & & 1 & & 4 & & 10 & & 20 & & 35 & & 56 & & 84 & & 120 \\
 & \color{blue}{1} & & \color{blue}{3} & & \color{blue}{6} & & \color{blue}{10} & & \color{blue}{15} & & \color{blue}{21} & & \color{blue}{28} & & \color{blue}{36} & \\
 & & 2 & & 3 & & 4 & & 5 & & 6 & & 7 & & 8 & & \\
 & & & 1 & & 1 & & 1 & & 1 & & 1 & & 1 & & &
\end{array}$$

Since the third row is constant, we expect our formula to be cubic.

Sum of First n Triangular Numbers II

Example. Find the sum of the first n triangular numbers.

Let $p(n) = an^3 + bn^2 + cn + d$. Can you find a, b, c, and d?

From the circled number, $p(0) = 0 \implies d = 0$. Plugging in $p(1) = 1, p(2) = 4$, and $p(3) = 10$ gives:

$$\begin{cases} a + b + c = 1 \\ 8a + 4b + 2c = 4 \\ 27a + 9b + 3c = 10. \end{cases}$$

Solving this system gives $(a, b, c) = (\frac{1}{6}, \frac{1}{2}, \frac{1}{3})$. Hence,

$$p(n) = \frac{1}{6}n^3 + \frac{1}{2}n^2 + \frac{1}{3}n = \boxed{\frac{n(n+1)(n+2)}{6}}.$$

Properties of Divisibility

- **Transitive Property:** If $d \mid m$ and $m \mid n$, then $d \mid n$.
- **Linear Combinations:** If $d \mid n_1$ and $d \mid n_2$, then $d \mid n_1 c_1 + n_2 c_2$.
- **Dividing a Sum:** If $d \mid n_1, d \mid n_2, \cdots, d \mid n_k$, then $d \mid \sum_{j=1}^{k} n_j$.
- **Cancellation:** If $dc \mid nc$, then $d \mid n$.

Equivalent Remainder

Example. When we divide the numbers $1059, 1417$, and 2312 by an integer $d > 1$, the remainder is the integer r. Find d and r.

Solution. By the division algorithm, there exists three integer quotients q_1, q_2, and q_3 such that

$$\begin{aligned} 1059 &= dq_1 + r \\ 1417 &= dq_2 + r \\ 2312 &= dq_3 + r. \end{aligned}$$

We subtract the equations in pairs to get:

$$358 = d(q_2 - q_1),\ 895 = d(q_3 - q_2),\ 1253 = d(q_3 - q_1).$$

Hence, d must divide $358 = 2 \cdot 179,\ 895 = 5 \cdot 179,\ 1253 = 7 \cdot 179.$

We therefore conclude that $d = \boxed{179}$.

Now, dividing 1059 by 179 gives $1059 = 179 \cdot 5 + 164$. Therefore, $r = \boxed{164}$.

Outline

Calendar Math I

Modular Arithmetic is incredibly powerful and is used in cryptography, computer science, chemistry, music, and many other places.

Consider a simplified calendar system where the days of the week stay the same, but there is now only one month with 365 days. If the year begins on a Monday, then the first 20 days of the year look like the table below:

Sun	Mon	Tue	Wed	Thu	Fri	Sat
	1	2	3	4	5	6
7	8	9	10	11	12	13
14	15	16	17	18	19	20

Example. What day of the week is day 31 on?

Calendar Math II

Example. What day of the week is day 31 on?

Solution. Extending our table two more rows:

Sun	Mon	Tue	$\boxed{\text{Wed}}$	Thu	Fri	Sat
	1	2	3	4	5	6
7	8	9	10	11	12	13
14	15	16	17	18	19	20
21	22	23	24	25	26	27
28	29	30	**31**	32	33	34

We call the days that are Wednesdays **congruent to 3 modulo 7**. This is because the days of the week cycle with period 7. From the table above:

$$31 \equiv 24 \equiv 17 \equiv 10 \equiv 3 \pmod 7.$$

Try dividing these numbers by 7.

Calendar Math III

Example. Analyze the congruence $31 \equiv 24 \equiv 17 \equiv 10 \equiv 3 \pmod 7$.

$$31 = 7 \cdot 4 + 3,\ 24 = 7 \cdot 3 + 3,\ 17 = 7 \cdot 2 + 3, 10 = 7 \cdot 1 + 3.$$

Every Wednesday is of the form $7q + 3$. We can rethink of the table as:

	Sun $7q$	Mon $7q+1$	Tue $7q+2$	Wed $7q+3$	Thu $7q+4$	Fri $7q+5$	Sat $7q+6$
$q=0$		1	2	3	4	5	6
$q=1$	7	8	9	10	11	12	13
$q=2$	14	15	16	17	18	19	20
$q=3$	21	22	23	24	25	26	27
$q=4$	28	29	30	31	32	33	34

Example. Determine the weekday of day 75, 100, and 133.

Calendar Math IV

Example. Determine the weekday of day 75, 100, and 133.

Sun	Mon	Tue	Wed	Thu	Fri	Sat
$7q$	$7q+1$	$7q+2$	$7q+3$	$7q+4$	$7q+5$	$7q+6$

Solution. We use the division algorithm!

- $75 = 7 \cdot 10 + 5$ which lies on a **Friday**.
- $100 = 7 \cdot 14 + 2$ which lies on a **Tuesday**.
- $133 = 7 \cdot 19 + 0$ which lies on a **Sunday**. □

In general, $n = 7q + r, \;\; 0 \le r < 7 \implies n \equiv r \pmod 7$.

Hence, $75 \equiv 5 \pmod 7$, $100 \equiv 2 \pmod 7$, and $133 \equiv 0 \pmod 7$.

Modulo Definition I

Generalizing our work with days of the week, we have this definition:

Definition. If $n = dq + r$ where $0 \leq r < d$, then $n \equiv r \pmod{d}$.

r is said to be a modulo d *residue*. These consist of all possible remainders upon division by d, namely $\{0, 1, 2, 3, \cdots, d-1\}$. This set is $\mathbb{Z}_d$.

An example is the **units digit**. The possible decimal units digit of a number are $0, 1, 2, 3, 4, 5, 6, 7, 8, 9$. These form the modulo 10 residues.

Residue Sets

Definition. A set $\{a_1, a_2, a_3, \cdots, a_n\}$ is called a **reduced residue set** if for every integer b, there exists exactly one index j such that $b \equiv a_j \pmod{n}$.

For example, $\{-41, 11, 2, 33, -7, 24, -1\}$ is a reduced residue set mod 7, since

$$\{-41, 11, 2, 33, -7, 24, -1\} \equiv \{1, 4, 2, 5, 0, 3, 6\} \pmod{7}.$$

However, $\{1, 2, 3, 4, 5, 6, 8\}$ is not since $1 \equiv 8 \pmod{7}$.

Modulo Definition II

Definition. If $n = dq + r$ where $0 \leq r < d$, then $n \equiv r \pmod{d}$.

If $n_1 \equiv n_2 \pmod{d}$, then they leave the same remainder upon division by d:

$$n_1 = dq_1 + r$$
$$n_2 = dq_2 + r.$$

Hence, $n_1 - n_2 = d(q_1 - q_2) \implies d \mid n_1 - n_2$.

Modulo Addition/Subtraction

We add/subtract constants to the congruence $25 \equiv 11 \pmod 7$.

- Blue represents an addition of 2.
- Orange represents a subtraction of 3.

Sun	Mon	Tue	Wed	Thu	Fri	Sat
	1	2	3	4	5	6
7	8	9	10	**11**	12	13
14	15	16	17	18	19	20
21	22	23	24	**25**	26	27

Modulo Addition/Subtraction

We add/subtract constants to the congruence $25 \equiv 11 \pmod{7}$.

- Blue represents an addition of 2.
- Orange represents a subtraction of 3.

Sun	Mon	Tue	Wed	Thu	Fri	Sat
	1	2	3	4	5	6
7	8	9	10	**11**	12	13
14	15	16	17	18	19	20
21	22	23	24	**25**	26	27

Modulo Addition/Subtraction

We add/subtract constants to the congruence $25 \equiv 11 \pmod{7}$.

- Blue represents an addition of 2.
- Orange represents a subtraction of 3.

Sun	Mon	Tue	Wed	Thu	Fri	Sat
	1	2	3	4	5	6
7	8	9	10	**11**	12	13
14	15	16	17	18	19	20
21	22	23	24	**25**	26	27

Modulo Addition/Subtraction

We add/subtract constants to the congruence $25 \equiv 11 \pmod 7$.

- Blue represents an addition of 2.
- Orange represents a subtraction of 3.

Sun	Mon	Tue	Wed	Thu	Fri	Sat
	1	2	3	4	5	6
7	8	9	10	<u>**11**</u>	12	13
14	15	16	17	18	19	20
21	22	23	24	<u>**25**</u>	26	27

Adding 2 gives $27 \equiv 13 \pmod 7$ and subtracting 3 gives $22 \equiv 8 \pmod 7$.

Modulo Addition/Subtraction

We add/subtract constants to the congruence $25 \equiv 11 \pmod{7}$.

- Blue represents an addition of 2.
- Orange represents a subtraction of 3.

Sun	Mon	Tue	Wed	Thu	Fri	Sat
	1	2	3	4	5	6
7	8	9	10	**11**	12	13
14	15	16	17	18	19	20
21	22	23	24	**25**	26	27

Adding 2 gives $27 \equiv 13 \pmod{7}$ and subtracting 3 gives $22 \equiv 8 \pmod{7}$.

Theorem. If $n_1 \equiv n_2 \mod d$, then $n_1 + c \equiv n_2 + c \mod d$ for integer c.

Modulo Addition/Subtraction III

Sun	Mon	Tue	Wed	Thu	Fri	Sat
	1	2	**3**	4	5	6
7	8	**9**	**10**	11	12	13
14	15	**16**	17	18	19	20
21	22	23	24	25	26	27

Consider the congruences $16 \equiv 9 \pmod{7}$ and $10 \equiv 3 \pmod{7}$.

Adding these congruences produces Fridays: $26 \equiv 12 \pmod{7}$.

Tuesdays are of the form $7q_1 + 2$ and Wednesdays $7q_2 + 3$. Their sum is:

$$(7q_1 + 2) + (7q_2 + 3) = 7\,(q_1 + q_2) + 5.$$

This is a Friday!

Modulo Addition/Subtraction IV

Theorem. If m_1, m_2, n_1, n_2 are integers such that

$$m_1 \equiv m_2 \pmod{d}$$
$$n_1 \equiv n_2 \pmod{d},$$

then $m_1 + n_1 \equiv m_2 + n_2 \pmod{d}$.

Modulo Addition Puzzles

Example 1. Compute the remainder when the sum

$$3 + 8 + 13 + 18 + \cdots + 1003$$

is divided by 5.

Caesar Shift Cryptography

Example. Decode the secret message 'PDWK LV DZHVRPH'.

In order to encode this, I used something known as a **Caesar shift**. Essentially, I shifted every character in my original message by three letters.

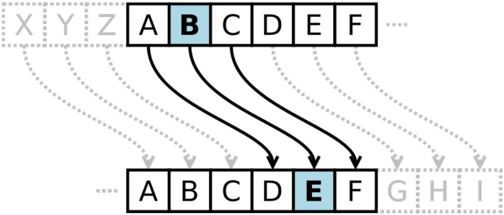

Figure 1: Caesar Shift Cryptography for $k = 3$.

Using this, can you figure out my original message?

Caesar Shift Examples

Example 2. Encode the message 'PYTHON IS FUN' using a Caesar shift with $k = 2$.

Example 3. Decode the message 'YHUB ZHOO GRQH' given it was encoded using a Caesar shift with $k = 3$.

General Formulas

Theorem. If we represent the letter A as 0 and Z as 25, we can think of the alphabet as a mod 26 system.

- To encode a letter x, we use the encoding $E_n(x) \equiv x + n \pmod{26}$.
- To decode a letter x, we use the decoding $D_n(x) \equiv x - n \pmod{26}$.

Modulo Multiplication I

We now multiplying the congruence $10 \equiv 3 \pmod 7$ by constants.

- Blue represents a multiplication by 2.
- Orange represents a multiplication by 3.

Sun	Mon	Tue	Wed	Thu	Fri	Sat
	1	2	**3**	4	5	6
7	8	9	**10**	11	12	13
14	15	16	17	18	19	20
21	22	23	24	25	26	27
28	29	30	31	32	33	34

Multiplying by 2 gives $20 \equiv 6 \pmod 7$ and by 3 gives $30 \equiv 9 \pmod 7$.

Theorem. If $n_1 \equiv n_2 \pmod d$, then for integer c, $n_1 c \equiv n_2 c \pmod d$.

Modulo Multiplication II

Theorem. If $n_1 \equiv n_2 \pmod{d}$, then for integer c, $n_1 c \equiv n_2 c \pmod{d}$.

Proof. Since $n_1 \equiv n_2 \pmod{d}$, we have $d \mid n_1 - n_2$.

By our theorem yesterday, we can multiply a divisibility by a constant:

$$d \mid n_1 - n_2 \implies d \mid c\,(n_1 - n_2)\,.$$

Expanding, we see that $c\,(n_1 - n_2) = n_1 c - n_2 c$. Therefore,

$$d \mid n_1 c - n_2 c \implies n_1 c \equiv n_2 c \pmod{d}.$$

Example. Find the units digit of $34 \cdot 62$. What do you notice?

Units Digit Multiplication

Example. Find the units digit of $34 \cdot 62$. What do you notice?

Solution. Through multiplying, $34 \cdot 62 = 2108$, which has a units digit of **8**. We see that 8 is the product of the units digit of $3\underline{4}$ and $6\underline{2}$.

In general, let the two numbers be $n = 10q_n + r_n$ and $m = 10q_m + r_m$:

$$\begin{aligned} nm &= (10q_n + r_n)(10q_m + r_m) \\ &= 100q_nq_m + 10q_nr_m + 10q_mr_n + r_nr_m \\ &\equiv r_nr_m \pmod{10}. \end{aligned}$$

The units digit of nm equals the product of the units digit of n and m.

Modulo Multiplication IV

Theorem. If m_1, m_2, n_1, n_2 are integers such that

$$m_1 \equiv m_2 \pmod{d}$$
$$n_1 \equiv n_2 \pmod{d},$$

then $m_1 n_1 \equiv m_2 n_2 \pmod{d}$.

Modulo Multiplication Puzzles

Example 4. The remainders when two natural numbers are divided by 12 are 7 and 9 respectively.

- Find the remainder when their product is divided by 12.
- Find the remainder when their product is divided by 4.

Product Mod 12 and 4

Example. The remainders when two natural numbers are divided by 12 are 7 and 9 respectively.

- Find the remainder when their product is divided by 12.
- Find the remainder when their product is divided by 4.

Solution. Let a and b be such that $a \equiv 7 \pmod{12}$ and $b \equiv 9 \pmod{12}$.

- Multiplying the congruences gives

$$ab \equiv 7 \cdot 9 \equiv 63 \equiv 3 \pmod{12}.$$

- We wish to find the modulo 4 residues of a and b:

$$\begin{aligned} a &= 12q_1 + 7 = 4(3q_1 + 1) + 3 \\ b &= 12q_2 + 9 = 4(3q_2 + 2) + 1. \end{aligned}$$

Therefore, $a \equiv 3 \pmod 4$ and $b \equiv 1 \pmod 4$. Multiplying gives:

$$ab \equiv 3 \cdot 1 \equiv 3 \pmod 4.$$

Outline

Exponential Divisibility Puzzles

Example 5. Show that 3 always divides $4^n - 1^n$ for all integers n.

Example 6. Show that 5 always divides $7^n - 2^n$ for all integers n.

$4^n - 1$ Divisible by 3 Part I

Example. Show that 3 always divides $4^n - 1^n$ for all integers n.

Solution.

$$\begin{aligned}
4^2 - 1^2 &= 16 - 1 = 15 &&= \mathbf{3} \cdot 5 \\
4^3 - 1^3 &= 64 - 1 = 63 &&= \mathbf{3} \cdot 21 \\
4^4 - 1^4 &= 256 - 1 = 255 &&= \mathbf{3} \cdot 85 \\
4^5 - 1^5 &= 1024 - 1 = 1023 &&= \mathbf{3} \cdot 341.
\end{aligned}$$

Do you notice anything interesting about the numbers on the right?

$$\begin{aligned}
5 &= 4 + 1 \\
21 &= 16 + 4 + 1 \\
85 &= 64 + 16 + 4 + 1 \\
341 &= 256 + 64 + 16 + 4 + 1.
\end{aligned}$$

These are all powers of 4. Why does this hold true?

$4^n - 1$ Divisible by 3 Part II

Example. Show that 3 always divides $4^n - 1$ for all integers n.

Using the fact that $4 - 1 = 3$, we can rewrite the original equations as:

$$\begin{aligned}
4^2 - 1^2 &= (4-1)(4+1) \\
4^3 - 1^3 &= (4-1)(4^2+4+1) \\
4^4 - 1^4 &= (4-1)(4^3+4^2+4+1) \\
4^5 - 1^5 &= (4-1)(4^4+4^3+4^2+4+1).
\end{aligned}$$

In general, I claim that

$$4^n - 1 = (4-1)\left(4^{n-1} + 4^{n-2} + \cdots + 4 + 1\right).$$

How do we prove this?

$4^n - 1$ Divisible by 3 Part III

Example. Show that $4^n - 1 = (4-1)\left(4^{n-1} + 4^{n-2} + \cdots + 4 + 1\right)$.

Solution. Let $S = 4^{n-1} + 4^{n-2} + \cdots + 4 + 1$. Then

$$\begin{aligned} 4S &= 4^n + 4^{n-1} + 4^{n-2} + \cdots + 4^2 + 4 \\ S &= 4^{n-1} + 4^{n-2} + \cdots + 4^2 + 4 + 1 \end{aligned}$$

Subtracting these equations yields $3S = 4^n - 1$. Substituting for S proves

$$(4-1)\left(4^{n-1} + 4^{n-2} + \cdots + 4 + 1\right) = 4^n - 1.$$

Therefore, for all integers n, $3 \mid 4^n - 1$. Can we generalize this result?

$$x^n - 1 = (x-1)\left(x^{n-1} + x^{n-2} + \cdots + x + 1\right).$$

This is equivalent to the geometric series formula you see in algebra.

General Factorization

Theorem. For all positive integers n,

$$x^n - y^n = (x-y)\left(x^{n-1} + x^{n-2}y^1 + x^{n-3}y^2 + \cdots + y^{n-1}\right).$$

Therefore, $x - y \mid x^n - y^n$.

Mod Exponents

The previous are identical to $4^n \equiv 1 \pmod{3}$ and $7^n \equiv 2^n \pmod{5}$.

Theorem. For integers x and y, if $x \equiv y \pmod{d}$ then $x^n \equiv y^n \pmod{d}$.

Proof. $x \equiv y \pmod{d} \implies d \mid x - y$ and $x - y \mid x^n - y^n$. Hence,

$$d \mid x - y \mid x^n - y^n \implies d \mid x^n - y^n.$$

The conclusion is that $x^n \equiv y^n \pmod{d}$.

An alternative way is observing the congruences

$$\begin{aligned} x &\equiv y \pmod{d} \\ x &\equiv y \pmod{d}. \end{aligned}$$

Multiplying them gives $x^2 \equiv y^2 \pmod{d}$. Multiplying again gives $x^3 \equiv y^3 \pmod{d}$. We can always increase the exponent by 1, hence, in general, $x^n \equiv y^n \pmod{d}$. This proof method is known as **induction**.

Factorizing $x^n + y^n$

Theorem. For all **odd** positive integers n,

$$x^n + y^n = (x + y)\left(x^{n-1} - x^{n-2}y + x^{n-3}y^2 + \cdots + y^{n-1}\right).$$

Therefore, for odd n, $x + y \mid x^n + y^n$.

Exploration

Example 7. Compute $5^{70} \pmod{31}$.

Example 8. Compute the units digit of $3^{7^{11}}$.

Powers of 5 Mod 31

Example. Compute $5^{70} \pmod{31}$.

Solution. Notice that $5^3 \equiv 1 \pmod{31}$, therefore

$$5^{70} = 5^1 \cdot \left(5^3\right)^{23} \equiv 5^1 \cdot 1^{23} \equiv \mathbf{5} \pmod{31}.$$

Units Digit of Power of 7

Example. Compute the units digit of $3^{7^{11}}$.

Solution. Observe the following relations for nonnegative integer n:

$$\begin{aligned} n \equiv 0 \pmod 4 &\implies 3^n \equiv 1 \pmod{10} \\ n \equiv 1 \pmod 4 &\implies 3^n \equiv 3 \pmod{10} \\ n \equiv 2 \pmod 4 &\implies 3^n \equiv 9 \pmod{10} \\ n \equiv 3 \pmod 4 &\implies 3^n \equiv 7 \pmod{10}. \end{aligned}$$

We therefore wish to compute $7^{11} \bmod 4$. Observe

$$7^{11} \equiv (-1)^{11} \equiv -1 \equiv 3 \pmod 4.$$

Therefore,

$$3^{7^{11}} \equiv 3^3 \equiv \mathbf{7} \pmod{10}.$$

Binomial Theorem

Theorem. For every positive integer n,

$$(x+y)^n = \sum_{k=0}^{n} \binom{n}{k} x^k y^{n-k}.$$

Example 9. Show that 100 divides $11^{10} - 1$.

Power of 11

Example. Show that 100 divides $11^{10} - 1$.

Since $11 = 1 + 10$, we use the binomial theorem:

$$\begin{aligned} 11^{10} &= (10+1)^{10} \\ &= \sum_{k=0}^{10} \binom{10}{k} 10^k 1^{10-k} \\ &= 1 + \binom{10}{1} 10^1 + \binom{10}{2} 10^2 + \binom{10}{3} 10^3 + \cdots \\ &\equiv 1 \pmod{100}. \end{aligned}$$

The conclusion hence follows that $100 \mid 11^{10} - 1$.

Outline

Decimal

The system we conventionally use for writing numbers is known as **decimal**.

In the decimal system, we write a number such as 1337 in terms of powers of 10. For instance, $1337 = 10^3 + 3 \cdot 10^2 + 3 \cdot 10^1 + 7 \cdot 10^0$. In general,

$$\begin{aligned} n &= a_k a_{k-1} \cdots a_2 a_1 a_0 \\ &= 10^k a_k + 10^{k-1} a_{k-1} + \cdots + 10^2 a_2 + 10^1 a_1 + a_0 \\ &= \sum_{j=0}^{k} \left(10^j \cdot a_j\right). \end{aligned}$$

Using decimal, we can prove the divisibility rules for 9 and 11.

Divisibility Rule for 9

Example. Show that a number is divisible by 9 if and only if the sum of its digits is divisible by 9.

Solution. Let the number be n. We express n in decimal form:

$$n = 10^k a_k + 10^{k-1} a_{k-1} + \cdots + 10^2 a_2 + 10^1 a_1 + a_0.$$

Notice that $10 \equiv 1 \pmod{9}$. Therefore, using modulo exponentiation:

$$\begin{aligned} n &= 10^k a_k + 10^{k-1} a_{k-1} + \cdots + 10^2 a_2 + 10^1 a_1 + a_0 \\ &\equiv 1^k a_k + 1^{k-1} a_{k-1} + \cdots + 1^2 a_2 + 1^1 a_1 + a_0 \\ &\equiv a_k + a_{k-1} + \cdots + a_2 + a_1 + a_0 \pmod{9}. \end{aligned}$$

Therefore, n is divisible by 9 if and only if the sum of its digits is.

Divisibility Rule for 11

Example. Show that a number is divisible by 11 if and only if the alternating sum of its digits is divisible by 11.

Solution. The alternating sum of digits of n is $a_0 - a_1 + a_2 - a_3 + \cdots + (-1)^k a_k$. Notice that $10 \equiv -1 \pmod{11}$. Therefore, using modulo exponentiation:

$$\begin{aligned} n &= 10^k a_k + 10^{k-1} a_{k-1} + \cdots + 10^2 a_2 + 10^1 a_1 + a_0 \\ &\equiv (-1)^k a_k + (-1)^{k-1} a_{k-1} + \cdots + (-1)^2 a_2 + (-1)^1 a_1 + a_0 \\ &\equiv a_0 - a_1 + a_2 - a_3 + \cdots + (-1)^k a_k \pmod{11}. \end{aligned}$$

Therefore, n is divisible by 11 if and only if the alternating sum of its digits is.

Divisible by 91 Problem

Example. (HMMT) For what single digit N does 91 divide the 9-digit number $12345N789$.

Solution. Since $1001 = 91 \cdot 11$, $10^3 = 1000 \equiv -1 \pmod{91}$. Now,

$$\begin{aligned} 123450789 &= 123 \cdot 10^6 + 450 \cdot 10^3 + 789 \\ &\equiv 123 \cdot 1 + 450 \cdot -1 + 789 \cdot 1 \\ &\equiv 32 + (-5) \cdot (-1) + 61 \\ &\equiv 98 \equiv 7 \pmod{91}. \end{aligned}$$

Therefore, in order to find N:

$$12345N789 = 7 + 1000N \equiv 7 - N \equiv 0 \pmod{91} \implies N = \boxed{7}.$$

Outline

Natural Numbers Divided by 12

Example. The remainders when two natural numbers are divided by 12 are 7 and 8 respectively.

- Find the remainder when their sum is divided by 12.
- Find the remainder when their sum is divided by 6.

Solution. Let a and b be such that $a \equiv 7 \pmod{12}$ and $b \equiv 8 \pmod{12}$.

- Adding the congruences gives

$$a + b \equiv 7 + 8 \equiv 15 \equiv 3 \pmod{12}.$$

- We wish to find the modulo 6 residues of a and b:

$$\begin{aligned} a &= 12q_1 + 7 = 6\left(2q_1 + 1\right) + 1 \\ b &= 12q_2 + 8 = 6\left(2q_2 + 1\right) + 2. \end{aligned}$$

Therefore, $a \equiv 1 \pmod{6}$ and $b \equiv 2 \pmod{6}$. Adding gives:

$$a + b \equiv 1 + 2 \equiv 3 \pmod{6}.$$

$7^n - 2^n$ Divisible by 5 Part I

Example. Show that 5 always divides $7^n - 2^n$ for all integers n.

Solution. As we did before, we begin by exploring this for small values of n:

$$\begin{aligned}
7^2 - 2^2 &= 49 - 4 = 45 &&= \mathbf{5} \cdot 9 \\
7^3 - 2^3 &= 343 - 8 = 335 &&= \mathbf{5} \cdot 67 \\
7^4 - 2^4 &= 2401 - 16 = 2385 &&= \mathbf{5} \cdot 477
\end{aligned}$$

Do you see anything interesting about the coefficients on the right?

$$\begin{aligned}
9 &= 7^1 + 2^1 \\
67 &= 7^2 + 7^1 \cdot 2^1 + 2^2 \\
477 &= 7^3 + 7^2 \cdot 2^1 + 7^1 \cdot 2^2 + 2^3
\end{aligned}$$

$7^n - 2^n$ Divisible by 5 Part II

Example. Show that 5 always divides $7^n - 2^n$ for all integers n.

Using the fact that $7 - 2 = 5$, we can rewrite the original equations as:

$$
\begin{aligned}
7^2 - 2^2 &= (7-2)(7+2) \\
7^3 - 2^3 &= (7-2)(7^2 + 7^1 \cdot 2^1 + 2^2) \\
7^4 - 2^4 &= (7-2)(7^3 + 7^2 \cdot 2^1 + 7^1 \cdot 2^2 + 2^3).
\end{aligned}
$$

In general, I claim that

$$7^n - 2^n = (7-2)\left(7^{n-1} + 7^{n-2} \cdot 2^1 + 7^{n-3} \cdot 2^2 + \cdots + 2^{n-1}\right).$$

Therefore, $5 \mid 7^n - 2^n$.