COMP 761: Lecture 7 – Number Theory

David Rolnick

September 18, 2020

Problem

Prove that $n^7 - n$ is divisible by 42 for every integer n.

(Please don't post your ideas in the chat just yet, we'll discuss the problem soon in class.)

Course Announcements

Course Announcements

- Problem Set 1 is due **today** at 11:59 pm Montreal time

Course Announcements

- Problem Set 1 is due **today** at 11:59 pm Montreal time
- Clarification on Problem 2 - please don't cite the fact that $\sqrt{3}$ is irrational (unless you prove it, in which case it's fine)

Finishing up from last class

Finishing up from last class

- The so-called *Trivial Inequality*:

$$x^2 \geq 0, \text{ for any real } x.$$

Finishing up from last class

- The so-called *Trivial Inequality*:

$$x^2 \geq 0, \text{ for any real } x.$$

- Surprisingly useful.

Finishing up from last class

- The so-called *Trivial Inequality*:

$$x^2 \geq 0, \text{ for any real } x.$$

- Surprisingly useful.
- Why does $x^2 - 2x + 2 = 0$ have no real solutions?

$$x^2 - 2x + 2 = (x^2 - 2x + 1) + 1 = (x - 1)^2 + 1 \geq 1.$$

AM-GM Inequality

The *AM-GM Inequality* (stands for “Arithmetic Mean-Geometric Mean”)

AM-GM Inequality

The *AM-GM Inequality* (stands for "Arithmetic Mean-Geometric Mean")

- 2-variable case:

$$\frac{a+b}{2} \geq \sqrt{ab}, \qquad \text{for } a, b \geq 0$$

AM-GM Inequality

The *AM-GM Inequality* (stands for "Arithmetic Mean-Geometric Mean")

- 2-variable case:

$$\frac{a+b}{2} \geq \sqrt{ab}, \qquad \text{for } a, b \geq 0$$

- General case:

$$\frac{a_1 + a_2 + \cdots + a_n}{n} \geq (a_1 a_2 \cdots a_n)^{1/n}, \qquad \text{for } a_1, a_2, \ldots, a_n \geq 0$$

AM-GM Inequality

The *AM-GM Inequality* (stands for "Arithmetic Mean-Geometric Mean")

- 2-variable case:

$$\frac{a+b}{2} \geq \sqrt{ab}, \qquad \text{for } a, b \geq 0$$

- General case:

$$\frac{a_1 + a_2 + \cdots + a_n}{n} \geq (a_1 a_2 \cdots a_n)^{1/n}, \qquad \text{for } a_1, a_2, \ldots, a_n \geq 0$$

Proof of 2-variable case:

AM-GM Inequality

The *AM-GM Inequality* (stands for "Arithmetic Mean-Geometric Mean")

- 2-variable case:

$$\frac{a+b}{2} \geq \sqrt{ab}, \qquad \text{for } a, b \geq 0$$

- General case:

$$\frac{a_1 + a_2 + \cdots + a_n}{n} \geq (a_1 a_2 \cdots a_n)^{1/n}, \qquad \text{for } a_1, a_2, \ldots, a_n \geq 0$$

Proof of 2-variable case:

- Squaring it, it's equivalent to:

$$\frac{a^2 + 2ab + b^2}{4} \geq ab.$$

AM-GM Inequality

The *AM-GM Inequality* (stands for "Arithmetic Mean-Geometric Mean")

- 2-variable case:

$$\frac{a+b}{2} \geq \sqrt{ab}, \quad \text{for } a, b \geq 0$$

- General case:

$$\frac{a_1 + a_2 + \cdots + a_n}{n} \geq (a_1 a_2 \cdots a_n)^{1/n}, \quad \text{for } a_1, a_2, \ldots, a_n \geq 0$$

Proof of 2-variable case:

- Squaring it, it's equivalent to:

$$\frac{a^2 + 2ab + b^2}{4} \geq ab.$$

- Multiplying out and rearranging, that is $a^2 - 2ab + b^2 \geq 0$.

AM-GM Inequality

The *AM-GM Inequality* (stands for "Arithmetic Mean-Geometric Mean")

- 2-variable case:

$$\frac{a+b}{2} \geq \sqrt{ab}, \quad \text{for } a, b \geq 0$$

- General case:

$$\frac{a_1 + a_2 + \cdots + a_n}{n} \geq (a_1 a_2 \cdots a_n)^{1/n}, \quad \text{for } a_1, a_2, \ldots, a_n \geq 0$$

Proof of 2-variable case:

- Squaring it, it's equivalent to:

$$\frac{a^2 + 2ab + b^2}{4} \geq ab.$$

- Multiplying out and rearranging, that is $a^2 - 2ab + b^2 \geq 0$.
- That is just the Trivial Inequality!

$$a^2 - 2ab + b^2 = (a-b)^2 \geq 0$$

Problem

What is the minimum possible value of $x^{100} + \frac{3}{x^{100}}$?

Problem

What is the minimum possible value of $x^{100} + \frac{3}{x^{100}}$?

- We could use calculus, but what is a faster way?

Problem

What is the minimum possible value of $x^{100} + \frac{3}{x^{100}}$?

- We could use calculus, but what is a faster way?
- By AM-GM, we know that the average of two numbers is at least their geometric mean:

$$\frac{x^{100} + \frac{3}{x^{100}}}{2} \geq \sqrt{x^{100} \cdot \frac{3}{x^{100}}} = \sqrt{3}.$$

Problem

What is the minimum possible value of $x^{100} + \frac{3}{x^{100}}$?

- We could use calculus, but what is a faster way?
- By AM-GM, we know that the average of two numbers is at least their geometric mean:

$$\frac{x^{100} + \frac{3}{x^{100}}}{2} \geq \sqrt{x^{100} \cdot \frac{3}{x^{100}}} = \sqrt{3}.$$

- Therefore, the answer is $2\sqrt{3}$.

Problem

What is the minimum possible value of $x^{100} + \frac{3}{x^{100}}$?

- We could use calculus, but what is a faster way?
- By AM-GM, we know that the average of two numbers is at least their geometric mean:

$$\frac{x^{100} + \frac{3}{x^{100}}}{2} \geq \sqrt{x^{100} \cdot \frac{3}{x^{100}}} = \sqrt{3}.$$

- Therefore, the answer is $2\sqrt{3}$.
- Important detail: We do need to check that this value is actually attained at some x.

Problem

What is the minimum possible value of $x^{100} + \frac{3}{x^{100}}$?

- We could use calculus, but what is a faster way?
- By AM-GM, we know that the average of two numbers is at least their geometric mean:

$$\frac{x^{100} + \frac{3}{x^{100}}}{2} \geq \sqrt{x^{100} \cdot \frac{3}{x^{100}}} = \sqrt{3}.$$

- Therefore, the answer is $2\sqrt{3}$.
- Important detail: We do need to check that this value is actually attained at some x.
- But equality in AM-GM happens when $x^{100} = \frac{3}{x^{100}}$, which is possible when $x = 3^{1/200}$.

Prime numbers

Prime numbers

A *prime number* is a positive integer that is divisible by no positive integers other than itself and 1.

$$2, 3, 5, 7, 11, 13, 17, \ldots$$

Prime numbers

A *prime number* is a positive integer that is divisible by no positive integers other than itself and 1.

$$2, 3, 5, 7, 11, 13, 17, \ldots$$

Some cool things about primes:

Prime numbers

A *prime number* is a positive integer that is divisible by no positive integers other than itself and 1.

$$2, 3, 5, 7, 11, 13, 17, \ldots$$

Some cool things about primes:

- Infinitely many (we've already proven this!)

Prime numbers

A *prime number* is a positive integer that is divisible by no positive integers other than itself and 1.

$$2, 3, 5, 7, 11, 13, 17, \ldots$$

Some cool things about primes:

- Infinitely many (we've already proven this!)
- Bertrand's Postulate: for every positive integer n, there is a prime p such that

$$n < p < 2n.$$

Prime numbers

A *prime number* is a positive integer that is divisible by no positive integers other than itself and 1.

$$2, 3, 5, 7, 11, 13, 17, \ldots$$

Some cool things about primes:

- Infinitely many (we've already proven this!)
- Bertrand's Postulate: for every positive integer n, there is a prime p such that
$$n < p < 2n.$$
- Prime Number Theorem: the number of primes less than n is approximately $n/\log n$ (exact in the limit as $n \to \infty$).

Prime numbers

A *prime number* is a positive integer that is divisible by no positive integers other than itself and 1.

$$2, 3, 5, 7, 11, 13, 17, \ldots$$

Some cool things about primes:

- Infinitely many (we've already proven this!)
- Bertrand's Postulate: for every positive integer n, there is a prime p such that
$$n < p < 2n.$$
- Prime Number Theorem: the number of primes less than n is approximately $n/\log n$ (exact in the limit as $n \to \infty$).
- No really easy way to find primes exactly.

Prime factorization

Theorem (Fundamental Theorem of Arithmetic)

Every positive integer n greater than 1 can be written uniquely as the product of primes:

$$n = p_1^{r_1} p_2^{r_2} \cdots p_k^{r_k}.$$

Prime factorization

Theorem (Fundamental Theorem of Arithmetic)

Every positive integer n greater than 1 can be written uniquely as the product of primes:

$$n = p_1^{r_1} p_2^{r_2} \cdots p_k^{r_k}.$$

- Example: $36 = 2^2 3^2$.

Prime factorization

Theorem (Fundamental Theorem of Arithmetic)

Every positive integer n greater than 1 can be written uniquely as the product of primes:

$$n = p_1^{r_1} p_2^{r_2} \cdots p_k^{r_k}.$$

- Example: $36 = 2^2 3^2$.
- What happens if n is a square?

Prime factorization

Theorem (Fundamental Theorem of Arithmetic)

Every positive integer n greater than 1 can be written uniquely as the product of primes:

$$n = p_1^{r_1} p_2^{r_2} \cdots p_k^{r_k}.$$

- Example: $36 = 2^2 3^2$.
- What happens if n is a square?
- The exponents $r_1, r_2, \ldots, r_k$ are all even.

Problem

Suppose that

$$n = p_1^{r_1} p_2^{r_2} \cdots p_k^{r_k}.$$

How many (positive integer) divisors does n have?

Problem

Suppose that

$$n = p_1^{r_1} p_2^{r_2} \cdots p_k^{r_k}.$$

How many (positive integer) divisors does n have?

- Let's try an example:

$$18 = 2^1 3^2.$$

Problem

Suppose that

$$n = p_1^{r_1} p_2^{r_2} \cdots p_k^{r_k}.$$

How many (positive integer) divisors does n have?

- Let's try an example:

$$18 = 2^1 3^2.$$

- Divisors:

$$1 = 1$$
$$2 = 2^1$$
$$3 = 3^1$$
$$6 = 2^1 3^1$$
$$9 = 3^2$$
$$18 = 2^1 3^2$$

Problem

Suppose that

$$n = p_1^{r_1} p_2^{r_2} \cdots p_k^{r_k}.$$

How many (positive integer) divisors n have?

Problem

Suppose that

$$n = p_1^{r_1} p_2^{r_2} \cdots p_k^{r_k}.$$

How many (positive integer) divisors n have?

- Suppose that m is a divisor of n.

Problem

Suppose that

$$n = p_1^{r_1} p_2^{r_2} \cdots p_k^{r_k}.$$

How many (positive integer) divisors n have?

- Suppose that m is a divisor of n.
- What primes can divide m?

Problem

Suppose that

$$n = p_1^{r_1} p_2^{r_2} \cdots p_k^{r_k}.$$

How many (positive integer) divisors n have?

- Suppose that m is a divisor of n.
- What primes can divide m?
- Only $p_1, p_2, \ldots, p_k$. If another prime p divided m, then it would also have to divide n.

Problem

Suppose that

$$n = p_1^{r_1} p_2^{r_2} \cdots p_k^{r_k}.$$

How many (positive integer) divisors n have?

- Suppose that m is a divisor of n.
- What primes can divide m?
- Only $p_1, p_2, \ldots, p_k$. If another prime p divided m, then it would also have to divide n.

Problem

Suppose that

$$n = p_1^{r_1} p_2^{r_2} \cdots p_k^{r_k}.$$

How many (positive integer) divisors n have?

- Suppose that m is a divisor of n.
- What primes can divide m?
- Only $p_1, p_2, \ldots, p_k$. If another prime p divided m, then it would also have to divide n.
- So

$$m = p_1^{s_1} p_2^{s_2} \cdots p_k^{s_k}.$$

Problem

Suppose that

$$n = p_1^{r_1} p_2^{r_2} \cdots p_k^{r_k}.$$

How many (positive integer) divisors n have?

- Suppose that m is a divisor of n.
- What primes can divide m?
- Only $p_1, p_2, \ldots, p_k$. If another prime p divided m, then it would also have to divide n.
- So

$$m = p_1^{s_1} p_2^{s_2} \cdots p_k^{s_k}.$$

- What can we say about $s_1, s_2, \ldots, s_k$?

Problem

Suppose that

$$n = p_1^{r_1} p_2^{r_2} \cdots p_k^{r_k}.$$

How many (positive integer) divisors n have?

- Suppose that m is a divisor of n.
- What primes can divide m?
- Only $p_1, p_2, \ldots, p_k$. If another prime p divided m, then it would also have to divide n.
- So

$$m = p_1^{s_1} p_2^{s_2} \cdots p_k^{s_k}.$$

- What can we say about $s_1, s_2, \ldots, s_k$?
- Each s_i is between 0 and r_i inclusive.

Problem

Suppose that

$$n = p_1^{r_1} p_2^{r_2} \cdots p_k^{r_k}.$$

How many (positive integer) divisors n have?

- Suppose that m is a divisor of n.
- What primes can divide m?
- Only $p_1, p_2, \ldots, p_k$. If another prime p divided m, then it would also have to divide n.
- So

$$m = p_1^{s_1} p_2^{s_2} \cdots p_k^{s_k}.$$

- What can we say about $s_1, s_2, \ldots, s_k$?
- Each s_i is between 0 and r_i inclusive.
- So $r_i + 1$ possibilities for each s_i, for a total of

$$(r_1 + 1)(r_2 + 1) \cdots (r_k + 1)$$

different divisors (including 1, where every $s_i = 0$)

Problem

- Back to our example:

$$18 = 2^1 3^2.$$

- Divisors:

$$1 = 1$$
$$2 = 2^1$$
$$3 = 3^1$$
$$6 = 2^1 3^1$$
$$9 = 3^2$$
$$18 = 2^1 3^2$$

Problem

- Back to our example:

$$18 = 2^1 3^2.$$

- Divisors:

$$1 = 1$$
$$2 = 2^1$$
$$3 = 3^1$$
$$6 = 2^1 3^1$$
$$9 = 3^2$$
$$18 = 2^1 3^2$$

- Number of divisors is $(1+1)(2+1) = 6$.

lcm and gcd

lcm and gcd

- The Least Common Multiple (lcm) of two numbers is the smallest integer that is a multiple of them both.

lcm and gcd

- The Least Common Multiple (lcm) of two numbers is the smallest integer that is a multiple of them both.
- Example: $\text{lcm}(10, 12) = 60$.

lcm and gcd

- The Least Common Multiple (lcm) of two numbers is the smallest integer that is a multiple of them both.
- Example: $\text{lcm}(10, 12) = 60$.
- The Greatest Common Divisor (gcd) of two numbers is the largest integer that divides them both.

lcm and gcd

- The Least Common Multiple (lcm) of two numbers is the smallest integer that is a multiple of them both.
- Example: $\text{lcm}(10, 12) = 60$.
- The Greatest Common Divisor (gcd) of two numbers is the largest integer that divides them both.
- Example: $\gcd(10, 12) = 2$.

lcm and gcd

- The Least Common Multiple (lcm) of two numbers is the smallest integer that is a multiple of them both.
- Example: $\text{lcm}(10, 12) = 60$.
- The Greatest Common Divisor (gcd) of two numbers is the largest integer that divides them both.
- Example: $\gcd(10, 12) = 2$.
- How do lcm and gcd relate to the prime factorization?

$$10 = 2^1 5^1$$

$$12 = 2^2 3^1$$

lcm and gcd

- The Least Common Multiple (lcm) of two numbers is the smallest integer that is a multiple of them both.
- Example: $\text{lcm}(10, 12) = 60$.
- The Greatest Common Divisor (gcd) of two numbers is the largest integer that divides them both.
- Example: $\gcd(10, 12) = 2$.
- How do lcm and gcd relate to the prime factorization?

$$10 = 2^1 5^1$$

$$12 = 2^2 3^1$$

- Let's expand those factorizations so they include the same primes:

lcm and gcd

- The Least Common Multiple (lcm) of two numbers is the smallest integer that is a multiple of them both.
- Example: $\text{lcm}(10, 12) = 60$.
- The Greatest Common Divisor (gcd) of two numbers is the largest integer that divides them both.
- Example: $\gcd(10, 12) = 2$.
- How do lcm and gcd relate to the prime factorization?

$$10 = 2^1 3^0 5^1$$

$$12 = 2^2 3^1 5^0$$

- Let's expand those factorizations so they include the same primes:

lcm and gcd

- The Least Common Multiple (lcm) of two numbers is the smallest integer that is a multiple of them both.
- Example: $\text{lcm}(10, 12) = 60$.
- The Greatest Common Divisor (gcd) of two numbers is the largest integer that divides them both.
- Example: $\gcd(10, 12) = 2$.
- How do lcm and gcd relate to the prime factorization?

$$10 = 2^1 3^0 5^1$$

$$12 = 2^2 3^1 5^0$$

- Let's expand those factorizations so they include the same primes:

$$\text{lcm}(10, 12) = 60 = 2^2 3^1 5^1 = 2^{\max(1,2)} 3^{\max(0,1)} 5^{\max(1,0)}$$

lcm and gcd

- The Least Common Multiple (lcm) of two numbers is the smallest integer that is a multiple of them both.
- Example: $\text{lcm}(10, 12) = 60$.
- The Greatest Common Divisor (gcd) of two numbers is the largest integer that divides them both.
- Example: $\gcd(10, 12) = 2$.
- How do lcm and gcd relate to the prime factorization?

$$10 = 2^1 3^0 5^1$$
$$12 = 2^2 3^1 5^0$$

- Let's expand those factorizations so they include the same primes:

$$\text{lcm}(10, 12) = 60 = 2^2 3^1 5^1 = 2^{\max(1,2)} 3^{\max(0,1)} 5^{\max(1,0)}$$
$$\gcd(10, 12) = 2 = 2^1 = 2^{\min(1,2)} 3^{\min(0,1)} 5^{\min(1,0)}.$$

Euclidean algorithm

Claim: If $m > n$, then $\gcd(m, n) = \gcd(n, m - n)$.

Euclidean algorithm

Claim: If $m > n$, then $\gcd(m, n) = \gcd(n, m - n)$.

- Anything that divides both m and n must divide their difference $m - n$.

Euclidean algorithm

Claim: If $m > n$, then $\gcd(m, n) = \gcd(n, m - n)$.

- Anything that divides both m and n must divide their difference $m - n$.
- Conversely, anything that divides both n and $m - n$ must divide their sum m.

Euclidean algorithm

Claim: If $m > n$, then $\gcd(m, n) = \gcd(n, m - n)$.

- Anything that divides both m and n must divide their difference $m - n$.
- Conversely, anything that divides both n and $m - n$ must divide their sum m.
- Therefore, the biggest common divisor of m, n is also the biggest common divisor of n and $m - n$.

Euclidean algorithm

Claim: If $m > n$, then $\gcd(m, n) = \gcd(n, m - n)$.

- Anything that divides both m and n must divide their difference $m - n$.
- Conversely, anything that divides both n and $m - n$ must divide their sum m.
- Therefore, the biggest common divisor of m, n is also the biggest common divisor of n and $m - n$.

Let's use this to find $\gcd(182, 224)$.

Euclidean algorithm

Claim: If $m > n$, then $\gcd(m, n) = \gcd(n, m - n)$.

- Anything that divides both m and n must divide their difference $m - n$.
- Conversely, anything that divides both n and $m - n$ must divide their sum m.
- Therefore, the biggest common divisor of m, n is also the biggest common divisor of n and $m - n$.

Let's use this to find $\gcd(182, 224)$.

- By the Claim, it's the same as the $\gcd(42, 182)$, since $42 = 224 - 182$.

Euclidean algorithm

Claim: If $m > n$, then $\gcd(m, n) = \gcd(n, m - n)$.

- Anything that divides both m and n must divide their difference $m - n$.
- Conversely, anything that divides both n and $m - n$ must divide their sum m.
- Therefore, the biggest common divisor of m, n is also the biggest common divisor of n and $m - n$.

Let's use this to find $\gcd(182, 224)$.

- By the Claim, it's the same as the $\gcd(42, 182)$, since $42 = 224 - 182$.
- Doing this again, it's the same as $\gcd(42, 140)$.

Euclidean algorithm

Claim: If $m > n$, then $\gcd(m, n) = \gcd(n, m - n)$.

- Anything that divides both m and n must divide their difference $m - n$.
- Conversely, anything that divides both n and $m - n$ must divide their sum m.
- Therefore, the biggest common divisor of m, n is also the biggest common divisor of n and $m - n$.

Let's use this to find $\gcd(182, 224)$.

- By the Claim, it's the same as the $\gcd(42, 182)$, since $42 = 224 - 182$.
- Doing this again, it's the same as $\gcd(42, 140)$.
- $= \gcd(42, 98) = \gcd(42, 56) = \gcd(14, 42) = \gcd(14, 28) = \gcd(14, 14)$.

Euclidean algorithm

Claim: If $m > n$, then $\gcd(m, n) = \gcd(n, m - n)$.

- Anything that divides both m and n must divide their difference $m - n$.
- Conversely, anything that divides both n and $m - n$ must divide their sum m.
- Therefore, the biggest common divisor of m, n is also the biggest common divisor of n and $m - n$.

Let's use this to find $\gcd(182, 224)$.

- By the Claim, it's the same as the $\gcd(42, 182)$, since $42 = 224 - 182$.
- Doing this again, it's the same as $\gcd(42, 140)$.
- $= \gcd(42, 98) = \gcd(42, 56) = \gcd(14, 42) = \gcd(14, 28) = \gcd(14, 14)$.
- So it's 14.

Euclidean algorithm

Claim: If $m > n$, then $\gcd(m, n) = \gcd(n, m - n)$.

- Anything that divides both m and n must divide their difference $m - n$.
- Conversely, anything that divides both n and $m - n$ must divide their sum m.
- Therefore, the biggest common divisor of m, n is also the biggest common divisor of n and $m - n$.

Let's use this to find $\gcd(182, 224)$.

- By the Claim, it's the same as the $\gcd(42, 182)$, since $42 = 224 - 182$.
- Doing this again, it's the same as $\gcd(42, 140)$.
- $= \gcd(42, 98) = \gcd(42, 56) = \gcd(14, 42) = \gcd(14, 28) = \gcd(14, 14)$.
- So it's 14.
- This is called the *Euclidean algorithm*.

Relatively prime numbers

Relatively prime numbers

- Two positive integers are said to be *relatively prime* if they have no common divisors except for 1.

Relatively prime numbers

- Two positive integers are said to be *relatively prime* if they have no common divisors except for 1.
- Example: 6 and 25 are relatively prime, even though neither is itself a prime

Relatively prime numbers

- Two positive integers are said to be *relatively prime* if they have no common divisors except for 1.
- Example: 6 and 25 are relatively prime, even though neither is itself a prime
- What can we say about the prime factorizations of two relatively prime integers?

$$m = p_1^{r_1} p_2^{r_2} \cdots p_k^{r_k}$$
$$n = q_1^{s_1} q_2^{s_2} \cdots q_\ell^{s_\ell}.$$

Relatively prime numbers

- Two positive integers are said to be *relatively prime* if they have no common divisors except for 1.
- Example: 6 and 25 are relatively prime, even though neither is itself a prime
- What can we say about the prime factorizations of two relatively prime integers?

$$m = p_1^{r_1} p_2^{r_2} \cdots p_k^{r_k}$$
$$n = q_1^{s_1} q_2^{s_2} \cdots q_\ell^{s_\ell}.$$

- None of $p_1, \ldots, p_k$ can equal any of $q_1, \ldots, q_\ell$.

Intro to modular arithmetic

Intro to modular arithmetic

- For integers x, y and a positive integer m, we write

$$x \equiv y \pmod{m}$$

if $x - y$ is a multiple of m.

Intro to modular arithmetic

- For integers x, y and a positive integer m, we write

$$x \equiv y \pmod{m}$$

  if $x - y$ is a multiple of m.
- We say *x is equal (or congruent) to y modulo m*.

Intro to modular arithmetic

- For integers x, y and a positive integer m, we write

$$x \equiv y \pmod{m}$$

  if $x - y$ is a multiple of m.
- We say x *is equal (or congruent) to* y *modulo* m.
- Example: $12 \equiv 62 \pmod{10}$.

Intro to modular arithmetic

- For integers x, y and a positive integer m, we write

$$x \equiv y \pmod{m}$$

  if $x - y$ is a multiple of m.
- We say *x is equal (or congruent) to y modulo m*.
- Example: $12 \equiv 62 \pmod{10}$.
- Example: $12 \equiv -8 \pmod{10}$.

Intro to modular arithmetic

- For integers x, y and a positive integer m, we write

$$x \equiv y \pmod{m}$$

  if $x - y$ is a multiple of m.
- We say *x is equal (or congruent) to y modulo m*.
- Example: $12 \equiv 62 \pmod{10}$.
- Example: $12 \equiv -8 \pmod{10}$.
- Every integer x is equal to one of $\{0, 1, 2, \ldots, m-1\}$ modulo m.

Intro to modular arithmetic

- For integers x, y and a positive integer m, we write

$$x \equiv y \pmod{m}$$

  if $x - y$ is a multiple of m.
- We say *x is equal (or congruent) to y modulo m*.
- Example: $12 \equiv 62 \pmod{10}$.
- Example: $12 \equiv -8 \pmod{10}$.
- Every integer x is equal to one of $\{0, 1, 2, \ldots, m-1\}$ modulo m.
- Example: $17 \equiv 2 \pmod{5}$.

Intro to modular arithmetic

- For integers x, y and a positive integer m, we write

$$x \equiv y \pmod{m}$$

  if $x - y$ is a multiple of m.
- We say *x is equal (or congruent) to y modulo m*.
- Example: $12 \equiv 62 \pmod{10}$.
- Example: $12 \equiv -8 \pmod{10}$.
- Every integer x is equal to one of $\{0, 1, 2, \ldots, m-1\}$ modulo m.
- Example: $17 \equiv 2 \pmod{5}$.
- Example: $-3 \equiv 2 \pmod{5}$.

Intro to modular arithmetic

- For integers x, y and a positive integer m, we write

$$x \equiv y \pmod{m}$$

  if $x - y$ is a multiple of m.
- We say *x is equal (or congruent) to y modulo m*.
- Example: $12 \equiv 62 \pmod{10}$.
- Example: $12 \equiv -8 \pmod{10}$.
- Every integer x is equal to one of $\{0, 1, 2, \ldots, m-1\}$ modulo m.
- Example: $17 \equiv 2 \pmod{5}$.
- Example: $-3 \equiv 2 \pmod{5}$.
- We say that 2 is the *residue of x modulo m* (same as the remainder when dividing by m).

Intro to modular arithmetic

- For integers x, y and a positive integer m, we write

$$x \equiv y \pmod{m}$$

  if $x - y$ is a multiple of m.
- We say *x is equal (or congruent) to y modulo m*.
- Example: $12 \equiv 62 \pmod{10}$.
- Example: $12 \equiv -8 \pmod{10}$.
- Every integer x is equal to one of $\{0, 1, 2, \ldots, m-1\}$ modulo m.
- Example: $17 \equiv 2 \pmod{5}$.
- Example: $-3 \equiv 2 \pmod{5}$.
- We say that 2 is the *residue of x modulo m* (same as the remainder when dividing by m).
- Anything divisible by m has residue 0 modulo m.

Addition and subtraction

If $x \equiv a \pmod{m}$ and $y \equiv b \pmod{m}$, then $x + y \equiv a + b \pmod{m}$ and $x - y \equiv a - b \pmod{m}$

Addition and subtraction

If $x \equiv a \pmod{m}$ and $y \equiv b \pmod{m}$, then $x + y \equiv a + b \pmod{m}$ and $x - y \equiv a - b \pmod{m}$

- Why is this true?

Addition and subtraction

If $x \equiv a \pmod{m}$ and $y \equiv b \pmod{m}$, then $x + y \equiv a + b \pmod{m}$ and $x - y \equiv a - b \pmod{m}$

- Why is this true?
- Let's suppose $x \equiv a \pmod{m}$ and $y \equiv b \pmod{m}$.

Addition and subtraction

If $x \equiv a \pmod{m}$ and $y \equiv b \pmod{m}$, then $x + y \equiv a + b \pmod{m}$ and $x - y \equiv a - b \pmod{m}$

- Why is this true?
- Let's suppose $x \equiv a \pmod{m}$ and $y \equiv b \pmod{m}$.
- Then, we can write $x = a + cm$ and $y = b + dm$ for integers c, d.

Addition and subtraction

If $x \equiv a \pmod{m}$ and $y \equiv b \pmod{m}$, then $x + y \equiv a + b \pmod{m}$ and $x - y \equiv a - b \pmod{m}$

- Why is this true?
- Let's suppose $x \equiv a \pmod{m}$ and $y \equiv b \pmod{m}$.
- Then, we can write $x = a + cm$ and $y = b + dm$ for integers c, d.
- Therefore:

$$\begin{aligned} x + y &= a + b + cm + dm = (a + b) + (c + d)m \\ &\equiv a + b \pmod{m} \end{aligned}$$

Addition and subtraction

If $x \equiv a \pmod{m}$ and $y \equiv b \pmod{m}$, then $x + y \equiv a + b \pmod{m}$ and $x - y \equiv a - b \pmod{m}$

- Why is this true?
- Let's suppose $x \equiv a \pmod{m}$ and $y \equiv b \pmod{m}$.
- Then, we can write $x = a + cm$ and $y = b + dm$ for integers c, d.
- Therefore:

$$\begin{aligned} x + y &= a + b + cm + dm = (a + b) + (c + d)m \\ &\equiv a + b \pmod{m} \end{aligned}$$

- Likewise:

$$\begin{aligned} x - y &= a - b + cm - dm = (a - b) + (c - d)m \\ &\equiv a - b \pmod{m} \end{aligned}$$

Addition and subtraction

Addition and subtraction

- Examples:

Addition and subtraction

- Examples:

$$\begin{aligned} 61 + 16 &\equiv 1 + 0 \pmod 2 \\ &\equiv 1 \pmod 2 \end{aligned}$$

Addition and subtraction

- Examples:

$$\begin{aligned} 61 + 16 &\equiv 1 + 0 \pmod 2 \\ &\equiv 1 \pmod 2 \end{aligned}$$

and

$$\begin{aligned} 14 - 5 &\equiv 2 - 2 \pmod 3 \\ &\equiv 0 \pmod 3 \end{aligned}$$

Multiplication

Multiplication

- If $x \equiv y \pmod{m}$, then $ax \equiv ay \pmod{m}$ for any integer a.

Multiplication

- If $x \equiv y \pmod{m}$, then $ax \equiv ay \pmod{m}$ for any integer a.
- Why is this true?

Multiplication

- If $x \equiv y \pmod{m}$, then $ax \equiv ay \pmod{m}$ for any integer a.
- Why is this true?
- If $x \equiv y \pmod{m}$, then $x - y = cm$.

Multiplication

- If $x \equiv y \pmod{m}$, then $ax \equiv ay \pmod{m}$ for any integer a.
- Why is this true?
- If $x \equiv y \pmod{m}$, then $x - y = cm$.
- So $ax - ay = acm$, which is also a multiple of m.

Multiplication

- If $x \equiv y \pmod{m}$, then $ax \equiv ay \pmod{m}$ for any integer a.
- Why is this true?
- If $x \equiv y \pmod{m}$, then $x - y = cm$.
- So $ax - ay = acm$, which is also a multiple of m.
- Example: $12 \equiv 2 \pmod{10}$, so $36 \equiv 6 \pmod{10}$.

Multiplication

- If $x \equiv y \pmod{m}$, then $ax \equiv ay \pmod{m}$ for any integer a.
- Why is this true?
- If $x \equiv y \pmod{m}$, then $x - y = cm$.
- So $ax - ay = acm$, which is also a multiple of m.
- Example: $12 \equiv 2 \pmod{10}$, so $36 \equiv 6 \pmod{10}$.
- Example: $4 \equiv -1 \pmod{5}$ so $4^n \equiv (-1)^n \pmod{5}$, e.g.

$$4, 16, 64, 256, \ldots \equiv -1, 1, -1, 1, \ldots \pmod{5}$$

Problem

Prove that a positive integer is divisible by 9 if and only if the sum of its digits is divisible by 9.

Problem

Prove that a positive integer is divisible by 9 if and only if the sum of its digits is divisible by 9.

- Let's write the integer x in terms of its digits $x_n x_{n-1} \ldots x_1 x_0$:

$$x = 10^n x_n + 10^{n-1} x_{n-1} + \cdots + 10 x_1 + x_0.$$

Problem

Prove that a positive integer is divisible by 9 if and only if the sum of its digits is divisible by 9.

- Let's write the integer x in terms of its digits $x_n x_{n-1} \ldots x_1 x_0$:

$$x = 10^n x_n + 10^{n-1} x_{n-1} + \cdots + 10 x_1 + x_0.$$

- How can we simplify this?

Problem

Prove that a positive integer is divisible by 9 if and only if the sum of its digits is divisible by 9.

- Let's write the integer x in terms of its digits $x_n x_{n-1} \ldots x_1 x_0$:

$$x = 10^n x_n + 10^{n-1} x_{n-1} + \cdots + 10 x_1 + x_0.$$

- How can we simplify this?
- 10 has residue 1 modulo 9.

Problem

Prove that a positive integer is divisible by 9 if and only if the sum of its digits is divisible by 9.

- Let's write the integer x in terms of its digits $x_n x_{n-1} \ldots x_1 x_0$:

$$x = 10^n x_n + 10^{n-1} x_{n-1} + \cdots + 10 x_1 + x_0.$$

- How can we simplify this?
- 10 has residue 1 modulo 9.
- So $10^k \equiv 1^k \equiv 1 \pmod 9$.

Problem

Prove that a positive integer is divisible by 9 if and only if the sum of its digits is divisible by 9.

- Let's write the integer x in terms of its digits $x_n x_{n-1} \ldots x_1 x_0$:

$$x = 10^n x_n + 10^{n-1} x_{n-1} + \cdots + 10 x_1 + x_0.$$

- How can we simplify this?
- 10 has residue 1 modulo 9.
- So $10^k \equiv 1^k \equiv 1 \pmod 9$.
- We can write:

$$x \equiv 1^n x_n + 1^{n-1} x_{n-1} + \cdots + 1 x_1 + x_0 \equiv x_n + x_{n-1} + \cdots + x_1 + x_0 \pmod 9.$$

Problem

Prove that a positive integer is divisible by 9 if and only if the sum of its digits is divisible by 9.

- Let's write the integer x in terms of its digits $x_n x_{n-1} \ldots x_1 x_0$:

$$x = 10^n x_n + 10^{n-1} x_{n-1} + \cdots + 10 x_1 + x_0.$$

- How can we simplify this?
- 10 has residue 1 modulo 9.
- So $10^k \equiv 1^k \equiv 1 \pmod 9$.
- We can write:

$$x \equiv 1^n x_n + 1^{n-1} x_{n-1} + \cdots + 1 x_1 + x_0 \equiv x_n + x_{n-1} + \cdots + x_1 + x_0 \pmod 9.$$

Problem

Prove that a positive integer is divisible by 9 if and only if the sum of its digits is divisible by 9.

- Let's write the integer x in terms of its digits $x_n x_{n-1} \ldots x_1 x_0$:

$$x = 10^n x_n + 10^{n-1} x_{n-1} + \cdots + 10 x_1 + x_0.$$

- How can we simplify this?
- 10 has residue 1 modulo 9.
- So $10^k \equiv 1^k \equiv 1 \pmod 9$.
- We can write:

$$x \equiv 1^n x_n + 1^{n-1} x_{n-1} + \cdots + 1 x_1 + x_0 \equiv x_n + x_{n-1} + \cdots + x_1 + x_0 \pmod 9.$$

- The sum of the digits is equal to the integer x modulo 9.

Problem

Prove that a positive integer is divisible by 9 if and only if the sum of its digits is divisible by 9.

- Let's write the integer x in terms of its digits $x_n x_{n-1} \ldots x_1 x_0$:

$$x = 10^n x_n + 10^{n-1} x_{n-1} + \cdots + 10 x_1 + x_0.$$

- How can we simplify this?
- 10 has residue 1 modulo 9.
- So $10^k \equiv 1^k \equiv 1 \pmod 9$.
- We can write:

$$x \equiv 1^n x_n + 1^{n-1} x_{n-1} + \cdots + 1 x_1 + x_0 \equiv x_n + x_{n-1} + \cdots + x_1 + x_0 \pmod 9.$$

- The sum of the digits is equal to the integer x modulo 9.
- In particular, if x is a multiple of 9 (i.e. equals 0 modulo 9), then so is the sum of the digits, and vice versa.

Division in modular arithmetic

Division in modular arithmetic

- If $ax \equiv ay \pmod{m}$, then $x \equiv y \pmod{m}$ **if the integer a is relatively prime to m.**

Division in modular arithmetic

- If $ax \equiv ay \pmod{m}$, then $x \equiv y \pmod{m}$ **if the integer a is relatively prime to m.**
- If $ax \equiv ay \pmod{m}$, then $ax - ay = cm$.

Division in modular arithmetic

- If $ax \equiv ay \pmod{m}$, then $x \equiv y \pmod{m}$ **if the integer a is relatively prime to m.**
- If $ax \equiv ay \pmod{m}$, then $ax - ay = cm$.
- If a is relatively prime to m, then c must be divisible by a.

Division in modular arithmetic

- If $ax \equiv ay \pmod{m}$, then $x \equiv y \pmod{m}$ **if the integer a is relatively prime to m.**
- If $ax \equiv ay \pmod{m}$, then $ax - ay = cm$.
- If a is relatively prime to m, then c must be divisible by a.
- Then, $x - y = (c/a)m$, so $x \equiv y \pmod{m}$.

Division in modular arithmetic

- If $ax \equiv ay \pmod{m}$, then $x \equiv y \pmod{m}$ **if the integer a is relatively prime to m.**
- If $ax \equiv ay \pmod{m}$, then $ax - ay = cm$.
- If a is relatively prime to m, then c must be divisible by a.
- Then, $x - y = (c/a)m$, so $x \equiv y \pmod{m}$.
- Example: $24 \equiv 2 \pmod{11}$ so $12 \equiv 1 \pmod{11}$.

Division in modular arithmetic

- If $ax \equiv ay \pmod{m}$, then $x \equiv y \pmod{m}$ **if the integer a is relatively prime to m.**
- If $ax \equiv ay \pmod{m}$, then $ax - ay = cm$.
- If a is relatively prime to m, then c must be divisible by a.
- Then, $x - y = (c/a)m$, so $x \equiv y \pmod{m}$.
- Example: $24 \equiv 2 \pmod{11}$ so $12 \equiv 1 \pmod{11}$.
- Example: $12 \equiv 2 \pmod{10}$ but $6 \not\equiv 1 \pmod{10}$ (since 2 and 10 are not relatively prime)

Problem

Prove that $n^7 - n$ is divisible by 42 for every integer n.

Problem

Prove that $n^7 - n$ is divisible by 42 for every integer n.

- Note: This problem can also be solved quickly with Fermat's Little Theorem, in case you are curious.

Problem

Prove that $n^7 - n$ is divisible by 42 for every integer n.

- Note: This problem can also be solved quickly with Fermat's Little Theorem, in case you are curious.
- How can we prove something is divisible by 42?

Problem

Prove that $n^7 - n$ is divisible by 42 for every integer n.

- Note: This problem can also be solved quickly with Fermat's Little Theorem, in case you are curious.
- How can we prove something is divisible by 42?
- Since $42 = 2 \cdot 3 \cdot 7$, we can prove that it's divisible by 2, and by 3, and by 7.

Problem

Prove that $n^7 - n$ is divisible by 42 for every integer n.

- Note: This problem can also be solved quickly with Fermat's Little Theorem, in case you are curious.
- How can we prove something is divisible by 42?
- Since $42 = 2 \cdot 3 \cdot 7$, we can prove that it's divisible by 2, and by 3, and by 7.
- Why is $n^7 - n$ divisible by 2?

Problem

Prove that $n^7 - n$ is divisible by 42 for every integer n.

- Note: This problem can also be solved quickly with Fermat's Little Theorem, in case you are curious.
- How can we prove something is divisible by 42?
- Since $42 = 2 \cdot 3 \cdot 7$, we can prove that it's divisible by 2, and by 3, and by 7.
- Why is $n^7 - n$ divisible by 2?
- $n \equiv 0$ or 1 modulo 2, and both work:

$$0^7 - 0 \equiv 0 \pmod 2$$

$$1^7 - 1 \equiv 0$$

Problem

Prove that $n^7 - n$ is divisible by 42 for every integer n.

- Note: This problem can also be solved quickly with Fermat's Little Theorem, in case you are curious.
- How can we prove something is divisible by 42?
- Since $42 = 2 \cdot 3 \cdot 7$, we can prove that it's divisible by 2, and by 3, and by 7.
- Why is $n^7 - n$ divisible by 2?
- $n \equiv 0$ or 1 modulo 2, and both work:

$$0^7 - 0 \equiv 0 \pmod 2$$
$$1^7 - 1 \equiv 0$$

- For 3, we have $n \equiv 0, 1$, or 2 modulo 3, and we can check:

$$0^7 - 0 \equiv 0 \pmod 3$$
$$1^7 - 1 \equiv 0$$
$$2^7 - 2 = 126 \equiv 0$$

Problem

Prove that $n^7 - n$ is divisible by 42 for every integer n.

Problem

Prove that $n^7 - n$ is divisible by 42 for every integer n.

- For 7, we have $n \equiv 0, 1, 2, 3, 4, 5,$ or 6 modulo 7:

$$0^7 - 0 \equiv 0 \pmod 7$$
$$1^7 - 1 \equiv 0$$
$$2^7 - 2 = 126 \equiv 0$$
$$3^7 - 3 = 9^3 \cdot 3 - 3 \equiv 2^3 \cdot 3 - 3 \equiv 21 \equiv 0$$

Problem

Prove that $n^7 - n$ is divisible by 42 for every integer n.

- For 7, we have $n \equiv 0, 1, 2, 3, 4, 5,$ or 6 modulo 7:

$$\begin{aligned} 0^7 - 0 &\equiv 0 \pmod 7 \\ 1^7 - 1 &\equiv 0 \\ 2^7 - 2 &= 126 \equiv 0 \\ 3^7 - 3 &= 9^3 \cdot 3 - 3 \equiv 2^3 \cdot 3 - 3 \equiv 21 \equiv 0 \end{aligned}$$

- We could check 4, 5, 6 too, but we don't have to... For example:

$$4^7 - 4 \equiv (-3)^7 - (-3) \equiv -(3^7 - 3) \equiv 0,$$

and likewise $5 \equiv -2$ and $6 \equiv -1$.

Problem

Prove that $n^7 - n$ is divisible by 42 for every integer n.

- For 7, we have $n \equiv 0, 1, 2, 3, 4, 5,$ or 6 modulo 7:

$$\begin{aligned} 0^7 - 0 &\equiv 0 \pmod 7 \\ 1^7 - 1 &\equiv 0 \\ 2^7 - 2 &= 126 \equiv 0 \\ 3^7 - 3 &= 9^3 \cdot 3 - 3 \equiv 2^3 \cdot 3 - 3 \equiv 21 \equiv 0 \end{aligned}$$

- We could check 4, 5, 6 too, but we don't have to... For example:

$$4^7 - 4 \equiv (-3)^7 - (-3) \equiv -(3^7 - 3) \equiv 0,$$

  and likewise $5 \equiv -2$ and $6 \equiv -1$.
- We conclude that every possible residue modulo 7 works.

Problem

Prove that $n^7 - n$ is divisible by 42 for every integer n.

- For 7, we have $n \equiv 0, 1, 2, 3, 4, 5,$ or 6 modulo 7:

$$\begin{aligned} 0^7 - 0 &\equiv 0 \pmod 7 \\ 1^7 - 1 &\equiv 0 \\ 2^7 - 2 &= 126 \equiv 0 \\ 3^7 - 3 &= 9^3 \cdot 3 - 3 \equiv 2^3 \cdot 3 - 3 \equiv 21 \equiv 0 \end{aligned}$$

- We could check 4, 5, 6 too, but we don't have to... For example:

$$4^7 - 4 \equiv (-3)^7 - (-3) \equiv -(3^7 - 3) \equiv 0,$$

  and likewise $5 \equiv -2$ and $6 \equiv -1$.
- We conclude that every possible residue modulo 7 works.
- Putting it all together, $n^7 - n$ must always be divisible by 2, 3, and 7, and therefore is divisible by 42.

Next time!

Combinatorics