CSE 311 Section 4

Number Theory

Administrivia

Announcements & Reminders

- HW2
  - If you think something was graded incorrectly, submit a regrade request!
- HW3 was due yesterday
  - Use late days if you need them!
- HW4
  - Due next week on July 23rd at 11:59PM on Gradescope

Greatest Common Divisor

Some Definitions

- Greatest Common Divisor (GCD):
  - The Greatest Common Divisor of a and b ($\gcd(a, b)$) is the largest integer c such that $c|a$ and $c|b$
- Multiplicative Inverse:
  - The multiplicative inverse of $a \pmod{n}$ is an integer b such that $ab \equiv 1 \pmod{n}$

Definitions Continued

If a is a positive integer, $\gcd(a,0) = a$

If a and b are positive integers, then $\gcd(a,b) = \gcd(b, a \% b)$

Conceptual Review

Review

What’s the definition of “a divides b”?

Review

What's the definition of "a divides b"?

There exists an integer z such that $az = b$.

Review

What’s the definition of "a is congruent to b modulo m"?

Review

What's the definition of "a is congruent to b modulo m"?

We say a is congruent to b mod m if and only if $m|(a-b)$.

Intuitively, $a \equiv b \pmod{m}$ means that $a\%m = b\%m$.

Review

What’s the division theorem?

Review

What's the division theorem?

The division theorem states that for any integer a and positive integer d, there exist unique integers q, r with $0 \leq r < d$ such that $a = qd + r$.

Warm Up

Problem 1 - GCD

(b) Calculate gcd(17, 31).

(d) Calculate gcd(18,14)

(e) Calculate gcd(80,44)

(h) Does 49 have an multiplicative inverse $\pmod 7$?

(g) Find the multiplicative inverse of 6 $\pmod 7$.

Work on parts (b), (d), (e), (h), and (g) with the people around you!

Problem 1 - GCD

(b) Calculate gcd(17, 31).

Problem 1 - GCD

(b) Calculate gcd(17, 31).

In this case, both numbers are prime.

By definition, this means their GCD is 1.

Problem 1 - GCD

(d) Calculate gcd(18,14)

Problem 1 - GCD

(d) Calculate gcd(18,14)

$$\gcd(18, 14) = \gcd(14, 4)$$

Problem 1 - GCD

(d) Calculate gcd(18,14)

$$\begin{aligned}\gcd(18, 14) &= \gcd(14, 4) \\ &= \gcd(4, 2)\end{aligned}$$

Problem 1 - GCD

(d) Calculate gcd(18,14)

$$\begin{aligned}\gcd(18,14) &= \gcd(14,4)\\ &= \gcd(4,2)\\ &= \gcd(2,0)\end{aligned}$$

Problem 1 - GCD

(d) Calculate gcd(18,14)

$$\begin{aligned}\gcd(18,14) &= \gcd(14,4)\\ &= \gcd(4,2)\\ &= \gcd(2,0)\\ &= 2\end{aligned}$$

Problem 1 - GCD

(e) Calculate gcd(80,44)

Problem 1 - GCD

(e) Calculate gcd(80,44)

$$\gcd(80, 40) = \gcd(44, 36)$$

Problem 1 - GCD

(e) Calculate gcd(80,44)

$$\begin{aligned}\gcd(80, 40) &= \gcd(44, 36) \\ &= \gcd(36, 8)\end{aligned}$$

Problem 1 - GCD

(e) Calculate gcd(80,44)

$$\begin{aligned}\gcd(80, 40) &= \gcd(44, 36) \\ &= \gcd(36, 8) \\ &= \gcd(8, 4)\end{aligned}$$

Problem 1 - GCD

(e) Calculate gcd(80,44)

$$\begin{aligned}\gcd(80, 40) &= \gcd(44, 36) \\ &= \gcd(36, 8) \\ &= \gcd(8, 4) \\ &= \gcd(4, 0\end{aligned}$$

Problem 1 - GCD

(e) Calculate gcd(80,44)

$$\begin{aligned}\gcd(80, 40) &= \gcd(44, 36) \\ &= \gcd(36, 8) \\ &= \gcd(8, 4) \\ &= \gcd(4, 0 \\ &= 4\end{aligned}$$

Problem 1 - GCD

(g) Find the multiplicative inverse of 6 (mod 7).

Problem 1 - GCD

(g) Find the multiplicative inverse of 6 (mod 7).

Let's use guess-and check for some small values.
We need to find a value for x such that $6x \equiv 1 \pmod 7$.

Problem 1 - GCD

(g) Find the multiplicative inverse of 6 (mod 7).

Let's use guess-and check for some small values.
We need to find a value for x such that $6x \equiv 1 \pmod 7$.
6 * 2 = 12, 12 %7 = 5
6 * 3 = 18, 18 %7 = 4
6 * 4 = 24, 24 %7 = 3
6 * 5 = 30, 30 %7 = 2
6 * 6 = 36, 36 %7 = 1

Problem 1 - GCD

(g) Find the multiplicative inverse of 6 (mod 7).

Let's use guess-and check for some small values.
We need to find a value for x such that $6x \equiv 1 \pmod 7$.
6 * 2 = 12, 12 %7 = 5
6 * 3 = 18, 18 %7 = 4
6 * 4 = 24, 24 %7 = 3
6 * 5 = 30, 30 %7 = 2
6 * 6 = 36, 36 %7 = 1
So, for the assignment x = 6, $6x \equiv 1 \pmod 7$.
Thus, the multiplicative inverse of 6 (mod 7) is 6.

Problem 1 - GCD

(h) Does 49 have an multiplicative inverse $\pmod 7$?

Problem 1 - GCD

(h) Does 49 have an multiplicative inverse $\pmod 7$?

It does not. Intuitively, this is because $49x$ for any x is going to be $0 \bmod 7$, which means it can never be 1.

Number Theory

Bonus! :D

Some Definitions

- Divides:
  - For $a, b \in \mathbb{Z}$: $a \mid b$ iff $\exists (k \in \mathbb{Z})\ b = ka$
  - For integers a and b, we say a divides b if and only if there exists an integer k such that $b = ka$
- Congruence Modulo:
  - For $a, b \in \mathbb{Z}, m \in \mathbb{Z}^+$: $a \equiv b \pmod{m}$ iff $m \mid (b - a)$
  - For integers a and b and positive integer m, we say a is congruent to b modulo m if and only if m divides $b - a$

Some Definitions

- Divides:
  - For $a, b \in \mathbb{Z}$: $a \mid b$ iff $\exists (k \in \mathbb{Z})\ b = ka$
  - For integers a and b, we say a divides b if and only if there exists an integer k such that $b = ka$
- Congruence Modulo:
  - For $a, b \in \mathbb{Z}, m \in \mathbb{Z}^+$: $a \equiv b \pmod{m}$ iff $m \mid (b - a)$
  - For integers a and b and positive integer m, we say a is congruent to b modulo m if and only if m divides $b - a$

Problem 3 – Divisibility Proof

Prove that if $a \mid b$ and $b \mid a$, where a and b are integers, then $a = b$ or $a = -b$.

Problem 3 – Divisibility Proof

Prove that if $a \mid b$ and $b \mid a$, where a and b are integers, then $a = b$ or $a = -b$.

Suppose that $a \mid b$ and $b \mid a$, where a, b are integers.

…

Therefore, it follows that $a = -b$ or $a = b$.

Start with your proof skeleton!

Problem 3 – Divisibility Proof

Prove that if $a \mid b$ and $b \mid a$, where a and b are integers, then $a = b$ or $a = -b$.

Suppose that $a \mid b$ and $b \mid a$, where a, b are integers.

By the definition of divides, we have $a \neq 0, b \neq 0$ and $b = ka, a = jb$ for some integers k, j.

…

Therefore, it follows that $a = -b$ or $a = b$.

Problem 3 – Divisibility Proof

Prove that if $a \mid b$ and $b \mid a$, where a and b are integers, then $a = b$ or $a = -b$.

Suppose that $a \mid b$ and $b \mid a$, where a, b are integers.

By the definition of divides, we have $a \neq 0, b \neq 0$ and $b = ka, a = jb$ for some integers k, j.
Combining these equations, we see that $a = j(ka)$.
…

Therefore, it follows that $a = -b$ or $a = b$.

Problem 3 – Divisibility Proof

Prove that if $a \mid b$ and $b \mid a$, where a and b are integers, then $a = b$ or $a = -b$.

Suppose that $a \mid b$ and $b \mid a$, where a, b are integers.

By the definition of divides, we have $a \neq 0, b \neq 0$ and $b = ka, a = jb$ for some integers k, j.
Combining these equations, we see that $a = j(ka)$.
Then, dividing both sides by a, we get $1 = jk$. So, $\frac{1}{j} = k$.

…

Therefore, it follows that $a = -b$ or $a = b$.

Problem 3 – Divisibility Proof

Prove that if $a \mid b$ and $b \mid a$, where a and b are integers, then $a = b$ or $a = -b$.

Suppose that $a \mid b$ and $b \mid a$, where a, b are integers.

By the definition of divides, we have $a \neq 0$, $b \neq 0$ and $b = ka$, $a = jb$ for some integers k, j.
Combining these equations, we see that $a = j(ka)$.
Then, dividing both sides by a, we get $1 = jk$. So, $\frac{1}{j} = k$.
Note that j and k are integers, which is only possible if $j, k \in \{1, -1\}$.

Therefore, it follows that $a = -b$ or $a = b$.

Problem 4 – Another Divisibility Proof

Prove that if $n \mid m$, where n and m are integers greater than 1, and if $a \equiv b \pmod{m}$, where a and b are integers, then $a \equiv b \pmod{n}$.

Problem 4 – Another Divisibility Proof

Prove that if $n \mid m$, where n and m are integers greater than 1, and if $a \equiv b \pmod{m}$, where a and b are integers, then $a \equiv b \pmod{n}$.

Let n, m, a, b be integers. Suppose $n \mid m$ with $n, m > 1$, and $a \equiv b \pmod{m}$.

…

Therefore, we have $a \equiv b \pmod{n}$.

Problem 4 – Another Divisibility Proof

Prove that if $n \mid m$, where n and m are integers greater than 1, and if $a \equiv b \pmod{m}$, where a and b are integers, then $a \equiv b \pmod{n}$.

Let n, m, a, b be integers. Suppose $n \mid m$ with $n, m > 1$, and $a \equiv b \pmod{m}$.

…

… we have $n \mid (b - a)$.

Therefore, by definition of congruence, we have $a \equiv b \pmod{n}$.

Problem 4 – Another Divisibility Proof

Prove that if $n \mid m$, where n and m are integers greater than 1, and if $a \equiv b \pmod{m}$, where a and b are integers, then $a \equiv b \pmod{n}$.

Let n, m, a, b be integers. Suppose $n \mid m$ with $n, m > 1$, and $a \equiv b \pmod{m}$.

NOTE: we don't know what C will look like yet, just that there is SOME integer here!

…

… we have $b - a = nC$.

Because C is an integer, by definition of divides, we have $n \mid (b - a)$.

Therefore, by definition of congruence, we have $a \equiv b \pmod{n}$.

Problem 4 – Another Divisibility Proof

Prove that if $n \mid m$, where n and m are integers greater than 1, and if $a \equiv b \pmod{m}$, where a and b are integers, then $a \equiv b \pmod{n}$.

Let n, m, a, b be integers. Suppose $n \mid m$ with $n, m > 1$, and $a \equiv b \pmod{m}$.

By definition of divides, we have $m = kn$ for some $k \in \mathbb{Z}$.

…

… we have $b - a = nC$.

Because C is an integer, by definition of divides, we have $n \mid (b - a)$.

Therefore, by definition of congruence, we have $a \equiv b \pmod{n}$.

Problem 4 – Another Divisibility Proof

Prove that if $n \mid m$, where n and m are integers greater than 1, and if $a \equiv b \pmod{m}$, where a and b are integers, then $a \equiv b \pmod{n}$.

Let n, m, a, b be integers. Suppose $n \mid m$ with $n, m > 1$, and $a \equiv b \pmod{m}$.

By definition of divides, we have $m = kn$ for some $k \in \mathbb{Z}$.
By definition of congruence, we have $m \mid a - b$, which means that $a - b = mj$ for some $j \in \mathbb{Z}$.
…
… we have $b - a = nC$.
Because C is an integer, by definition of divides, we have $n \mid (b - a)$.

Therefore, by definition of congruence, we have $a \equiv b \pmod{n}$.

Problem 4 – Another Divisibility Proof

Prove that if $n \mid m$, where n and m are integers greater than 1, and if $a \equiv b \pmod{m}$, where a and b are integers, then $a \equiv b \pmod{n}$.

Let n, m, a, b be integers. Suppose $n \mid m$ with $n, m > 1$, and $a \equiv b \pmod{m}$.

By definition of divides, we have $m = kn$ for some $k \in \mathbb{Z}$.
By definition of congruence, we have $m \mid a - b$, which means that $a - b = mj$ for some $j \in \mathbb{Z}$.
Combining the two equations, we see that $a - b = (knj) = n(kj)$.
… we have $b - a = nC$.
Because C is an integer, by definition of divides, we have $n \mid (b - a)$.

Therefore, by definition of congruence, we have $a \equiv b \pmod{n}$.

Problem 4 – Another Divisibility Proof

Prove that if $n \mid m$, where n and m are integers greater than 1, and if $a \equiv b \pmod{m}$, where a and b are integers, then $a \equiv b \pmod{n}$.

Let n, m, a, b be integers. Suppose $n \mid m$ with $n, m > 1$, and $a \equiv b \pmod{m}$.

By definition of divides, we have $m = kn$ for some $k \in \mathbb{Z}$.
By definition of congruence, we have $m \mid a - b$, which means that $a - b = mj$ for some $j \in \mathbb{Z}$.
Combining the two equations, we see that $a - b = (knj) = n(kj)$.
Equivalently, we have $b - a = n(-kj)$.
Because C is an integer, by definition of divides, we have $n \mid (b - a)$.

Therefore, by definition of congruence, we have $a \equiv b \pmod{n}$.

Problem 4 – Another Divisibility Proof

Prove that if $n \mid m$, where n and m are integers greater than 1, and if $a \equiv b \pmod{m}$, where a and b are integers, then $a \equiv b \pmod{n}$.

Let n, m, a, b be integers. Suppose $n \mid m$ with $n, m > 1$, and $a \equiv b \pmod{m}$.

By definition of divides, we have $m = kn$ for some $k \in \mathbb{Z}$.
By definition of congruence, we have $m \mid a - b$, which means that $a - b = mj$ for some $j \in \mathbb{Z}$.
Combining the two equations, we see that $a - b = (knj) = n(kj)$.
Equivalently, we have $b - a = n(-kj)$.
Because $-kj$ is an integer, by definition of divides, we have $n \mid (b - a)$.

Therefore, by definition of congruence, we have $a \equiv b \pmod{n}$.

Problem 6 - A Prime Example

Let p be an integer such that $p > 3$. Prove that if p is prime, either $p \equiv 1 \pmod 6$ or $p \equiv 5 \pmod 6$.
Hint: Prove by contrapositive. Within your contrapositive proof, you may wish to include cases.

Problem 6 - A Prime Example

Let p be an integer such that $p > 3$. Prove that if p is prime, either $p \equiv 1 \pmod 6$ or $p \equiv 5 \pmod 6$.
Hint: Prove by contrapositive. Within your contrapositive proof, you may wish to include cases.

We prove by contrapositive. Let $p > 3$ be an arbitrary integer. Suppose that $p \not\equiv 1 \pmod 6$ and $p \not\equiv 5 \pmod 6$. We show that p is not prime.

...

Conclusion: We have shown that in all cases, p is not prime. Since p was arbitrary, for all integers p, if $p > 3$ and $p \not\equiv 1 \pmod 6$ and $p \not\equiv 5 \pmod 6$, then p is not prime.

Since the contrapositive of our original statement is true, it follows that the original statement holds as well.

Start with the proof skeleton! Then, recognize what cases you need to prove.

Problem 6 - A Prime Example

Let p be an integer such that $p > 3$. Prove that if p is prime, either $p \equiv 1 \pmod 6$ or $p \equiv 5 \pmod 6$.
Hint: Prove by contrapositive. Within your contrapositive proof, you may wish to include cases.

Case $p \equiv 0 \pmod 6$:

Problem 6 - A Prime Example

Let p be an integer such that $p > 3$. Prove that if p is prime, either $p \equiv 1 \pmod 6$ or $p \equiv 5 \pmod 6$.
Hint: Prove by contrapositive. Within your contrapositive proof, you may wish to include cases.

Case $p \equiv 0 \pmod 6$: By definition of congruence, $6|p$. So $p = 6k$ for some integer k.

Problem 6 - A Prime Example

Let p be an integer such that $p > 3$. Prove that if p is prime, either $p \equiv 1 \pmod 6$ or $p \equiv 5 \pmod 6$.
Hint: Prove by contrapositive. Within your contrapositive proof, you may wish to include cases.

Case $p \equiv 0 \pmod 6$: By definition of congruence, $6|p$. Then by definition of divides, $p = 6k$ for some integer k. Then either $p = 6$, which is not prime, or $p \neq 6$ but has 6 as a factor and therefore is not prime.

Problem 6 - A Prime Example

Let p be an integer such that $p > 3$. Prove that if p is prime, either $p \equiv 1 \pmod 6$ or $p \equiv 5 \pmod 6$.
Hint: Prove by contrapositive. Within your contrapositive proof, you may wish to include cases.

Case $p \equiv 0 \pmod 6$: By definition of congruence, $6|p$. Then by definition of divides, $p = 6k$ for some integer k. Then either $p = 6$, which is not prime, or $p \neq 6$ but has 6 as a factor and therefore is not prime.

Case $p \equiv 2 \pmod 6$:

Problem 6 - A Prime Example

Let p be an integer such that $p > 3$. Prove that if p is prime, either $p \equiv 1 \pmod 6$ or $p \equiv 5 \pmod 6$.
Hint: Prove by contrapositive. Within your contrapositive proof, you may wish to include cases.

Case $p \equiv 0 \pmod 6$: By definition of congruence, $6|p$. Then by definition of divides, $p = 6k$ for some integer k. Then either $p = 6$, which is not prime, or $p \neq 6$ but has 6 as a factor and therefore is not prime.

Case $p \equiv 2 \pmod 6$: By definition of congruence, $6|(p-2)$. Then by definition of divides, $p - 2 = 6k$ for some integer k.

Problem 6 - A Prime Example

Let p be an integer such that $p > 3$. Prove that if p is prime, either $p \equiv 1 \pmod 6$ or $p \equiv 5 \pmod 6$.
Hint: Prove by contrapositive. Within your contrapositive proof, you may wish to include cases.

Case $p \equiv 0 \pmod 6$: By definition of congruence, $6|p$. Then by definition of divides, $p = 6k$ for some integer k. Then either $p = 6$, which is not prime, or $p \neq 6$ but has 6 as a factor and therefore is not prime.

Case $p \equiv 2 \pmod 6$: By definition of congruence, $6|(p-2)$. Then by definition of divides, $p - 2 = 6k$ for some integer k. Rearranging, we have $p = 6k + 2 = 2(3k + 1)$. So, p is divisible by 2.

Problem 6 - A Prime Example

Let p be an integer such that $p > 3$. Prove that if p is prime, either $p \equiv 1 \pmod 6$ or $p \equiv 5 \pmod 6$.
Hint: Prove by contrapositive. Within your contrapositive proof, you may wish to include cases.

Case $p \equiv 0 \pmod 6$: By definition of congruence, $6|p$. Then by definition of divides, $p = 6k$ for some integer k. Then either $p = 6$, which is not prime, or $p \neq 6$ but has 6 as a factor and therefore is not prime.

Case $p \equiv 2 \pmod 6$: By definition of congruence, $6|(p-2)$. Then by definition of divides, $p - 2 = 6k$ for some integer k. Rearranging, we have $p = 6k + 2 = 2(3k + 1)$. So, p is divisible by 2. Since $p > 3$, it follows that 2 is a factor between 1 and p that is not 1 or p. So, p is not prime.

Problem 6 - A Prime Example

Let p be an integer such that $p > 3$. Prove that if p is prime, either $p \equiv 1 \pmod 6$ or $p \equiv 5 \pmod 6$.
Hint: Prove by contrapositive. Within your contrapositive proof, you may wish to include cases.

Case $p \equiv 0 \pmod 6$: By definition of congruence, $6|p$. Then by definition of divides, $p = 6k$ for some integer k. Then either $p = 6$, which is not prime, or $p \neq 6$ but has 6 as a factor and therefore is not prime.

Case $p \equiv 2 \pmod 6$: By definition of congruence, $6|(p-2)$. Then by definition of divides, $p - 2 = 6k$ for some integer k. Rearranging, we have $p = 6k + 2 = 2(3k + 1)$. So, p is divisible by 2. Since $p > 3$, it follows that 2 is a factor between 1 and p that is not 1 or p. So, p is not prime.

Case $p \equiv 3 \pmod 6$:

Problem 6 - A Prime Example

Let p be an integer such that $p > 3$. Prove that if p is prime, either $p \equiv 1 \pmod 6$ or $p \equiv 5 \pmod 6$.
Hint: Prove by contrapositive. Within your contrapositive proof, you may wish to include cases.

Case $p \equiv 0 \pmod 6$: By definition of congruence, $6|p$. Then by definition of divides, $p = 6k$ for some integer k. Then either $p = 6$, which is not prime, or $p \neq 6$ but has 6 as a factor and therefore is not prime.

Case $p \equiv 2 \pmod 6$: By definition of congruence, $6|(p-2)$. Then by definition of divides, $p - 2 = 6k$ for some integer k. Rearranging, we have $p = 6k + 2 = 2(3k + 1)$. So, p is divisible by 2. Since $p > 3$, it follows that 2 is a factor between 1 and p that is not 1 or p. So, p is not prime.

Case $p \equiv 3 \pmod 6$: By definition of congruence, $6|(p-3)$. Then by definition of divides, $p - 3 = 6k$ for some integer k.

Problem 6 - A Prime Example

Let p be an integer such that $p > 3$. Prove that if p is prime, either $p \equiv 1 \pmod 6$ or $p \equiv 5 \pmod 6$.
Hint: Prove by contrapositive. Within your contrapositive proof, you may wish to include cases.

Case $p \equiv 0 \pmod 6$: By definition of congruence, $6|p$. Then by definition of divides, $p = 6k$ for some integer k. Then either $p = 6$, which is not prime, or $p \neq 6$ but has 6 as a factor and therefore is not prime.

Case $p \equiv 2 \pmod 6$: By definition of congruence, $6|(p-2)$. Then by definition of divides, $p - 2 = 6k$ for some integer k. Rearranging, we have $p = 6k + 2 = 2(3k + 1)$. So, p is divisible by 2. Since $p > 3$, it follows that 2 is a factor between 1 and p that is not 1 or p. So, p is not prime.

Case $p \equiv 3 \pmod 6$: By definition of congruence, $6|(p-3)$. Then by definition of divides, $p - 3 = 6k$ for some integer k. Rearranging, we have $p = 6k + 3 = 3(2k + 1)$. So, p is divisible by 3.

Problem 6 - A Prime Example

Let p be an integer such that $p > 3$. Prove that if p is prime, either $p \equiv 1 \pmod 6$ or $p \equiv 5 \pmod 6$.
Hint: Prove by contrapositive. Within your contrapositive proof, you may wish to include cases.

Case $p \equiv 0 \pmod 6$: By definition of congruence, $6|p$. Then by definition of divides, $p = 6k$ for some integer k. Then either $p = 6$, which is not prime, or $p \neq 6$ but has 6 as a factor and therefore is not prime.

Case $p \equiv 2 \pmod 6$: By definition of congruence, $6|(p-2)$. Then by definition of divides, $p - 2 = 6k$ for some integer k. Rearranging, we have $p = 6k + 2 = 2(3k + 1)$. So, p is divisible by 2. Since $p > 3$, it follows that 2 is a factor between 1 and p that is not 1 or p. So, p is not prime.

Case $p \equiv 3 \pmod 6$: By definition of congruence, $6|(p-3)$. Then by definition of divides, $p - 3 = 6k$ for some integer k. Rearranging, we have $p = 6k + 3 = 3(2k + 1)$. So, p is divisible by 3. Since $p > 3$, it follows that 3 is a factor between 1 and p that is not 1 or p. So, p is not prime.

Problem 6 - A Prime Example

Let p be an integer such that $p > 3$. Prove that if p is prime, either $p \equiv 1 \pmod 6$ or $p \equiv 5 \pmod 6$.
Hint: Prove by contrapositive. Within your contrapositive proof, you may wish to include cases.

Case $p \equiv 0 \pmod 6$: By definition of congruence, $6|p$. Then by definition of divides, $p = 6k$ for some integer k. Then either $p = 6$, which is not prime, or $p \neq 6$ but has 6 as a factor and therefore is not prime.

Case $p \equiv 2 \pmod 6$: By definition of congruence, $6|(p-2)$. Then by definition of divides, $p - 2 = 6k$ for some integer k. Rearranging, we have $p = 6k + 2 = 2(3k + 1)$. So, p is divisible by 2. Since $p > 3$, it follows that 2 is a factor between 1 and p that is not 1 or p. So, p is not prime.

Case $p \equiv 3 \pmod 6$: By definition of congruence, $6|(p-3)$. Then by definition of divides, $p - 3 = 6k$ for some integer k. Rearranging, we have $p = 6k + 3 = 3(2k + 1)$. So, p is divisible by 3. Since $p > 3$, it follows that 3 is a factor between 1 and p that is not 1 or p. So, p is not prime.

Case $p \equiv 4 \pmod 6$:

Problem 6 - A Prime Example

Let p be an integer such that $p > 3$. Prove that if p is prime, either $p \equiv 1 \pmod 6$ or $p \equiv 5 \pmod 6$.
Hint: Prove by contrapositive. Within your contrapositive proof, you may wish to include cases.

Case $p \equiv 0 \pmod 6$: By definition of congruence, $6|p$. Then by definition of divides, $p = 6k$ for some integer k. Then either $p = 6$, which is not prime, or $p \neq 6$ but has 6 as a factor and therefore is not prime.

Case $p \equiv 2 \pmod 6$: By definition of congruence, $6|(p-2)$. Then by definition of divides, $p - 2 = 6k$ for some integer k. Rearranging, we have $p = 6k + 2 = 2(3k + 1)$. So, p is divisible by 2. Since $p > 3$, it follows that 2 is a factor between 1 and p that is not 1 or p. So, p is not prime.

Case $p \equiv 3 \pmod 6$: By definition of congruence, $6|(p-3)$. Then by definition of divides, $p - 3 = 6k$ for some integer k. Rearranging, we have $p = 6k + 3 = 3(2k + 1)$. So, p is divisible by 3. Since $p > 3$, it follows that 3 is a factor between 1 and p that is not 1 or p. So, p is not prime.

Case $p \equiv 4 \pmod 6$: By definition of congruence, $6|(p-4)$. Then by definition of divides, $p - 4 = 6k$ for some integer k.

Problem 6 - A Prime Example

Let p be an integer such that $p > 3$. Prove that if p is prime, either $p \equiv 1 \pmod 6$ or $p \equiv 5 \pmod 6$.
Hint: Prove by contrapositive. Within your contrapositive proof, you may wish to include cases.

Case $p \equiv 0 \pmod 6$: By definition of congruence, $6|p$. Then by definition of divides, $p = 6k$ for some integer k. Then either $p = 6$, which is not prime, or $p \neq 6$ but has 6 as a factor and therefore is not prime.

Case $p \equiv 2 \pmod 6$: By definition of congruence, $6|(p-2)$. Then by definition of divides, $p - 2 = 6k$ for some integer k. Rearranging, we have $p = 6k + 2 = 2(3k + 1)$. So, p is divisible by 2. Since $p > 3$, it follows that 2 is a factor between 1 and p that is not 1 or p. So, p is not prime.

Case $p \equiv 3 \pmod 6$: By definition of congruence, $6|(p-3)$. Then by definition of divides, $p - 3 = 6k$ for some integer k. Rearranging, we have $p = 6k + 3 = 3(2k + 1)$. So, p is divisible by 3. Since $p > 3$, it follows that 3 is a factor between 1 and p that is not 1 or p. So, p is not prime.

Case $p \equiv 4 \pmod 6$: By definition of congruence, $6|(p-4)$. Then by definition of divides, $p - 4 = 6k$ for some integer k. Then rearranging, we have $p = 6k + 4 = 2(3k + 2)$. So, p is divisible by 2.

Problem 6 - A Prime Example

Let p be an integer such that $p > 3$. Prove that if p is prime, either $p \equiv 1 \pmod 6$ or $p \equiv 5 \pmod 6$.
Hint: Prove by contrapositive. Within your contrapositive proof, you may wish to include cases.

Case $p \equiv 0 \pmod 6$: By definition of congruence, $6|p$. Then by definition of divides, $p = 6k$ for some integer k. Then either $p = 6$, which is not prime, or $p \neq 6$ but has 6 as a factor and therefore is not prime.

Case $p \equiv 2 \pmod 6$: By definition of congruence, $6|(p-2)$. Then by definition of divides, $p - 2 = 6k$ for some integer k. Rearranging, we have $p = 6k + 2 = 2(3k + 1)$. So, p is divisible by 2. Since $p > 3$, it follows that 2 is a factor between 1 and p that is not 1 or p. So, p is not prime.

Case $p \equiv 3 \pmod 6$: By definition of congruence, $6|(p-3)$. Then by definition of divides, $p - 3 = 6k$ for some integer k. Rearranging, we have $p = 6k + 3 = 3(2k + 1)$. So, p is divisible by 3. Since $p > 3$, it follows that 3 is a factor between 1 and p that is not 1 or p. So, p is not prime.

Case $p \equiv 4 \pmod 6$: By definition of congruence, $6|(p-4)$. Then by definition of divides, $p - 4 = 6k$ for some integer k. Then rearranging, we have $p = 6k + 4 = 2(3k + 2)$. So, p is divisible by 2. Since $p > 3$, it follows that 2 is a factor between 1 and p that is not 1 or p. So, p is not prime.

Problem 6 - A Prime Example

Let p be an integer such that $p > 3$. Prove that if p is prime, either $p \equiv 1 \pmod 6$ or $p \equiv 5 \pmod 6$.
Hint: Prove by contrapositive. Within your contrapositive proof, you may wish to include cases.

Conclusion: We have shown that in all cases, p is not prime. Since p was arbitrary, for all integers p, if $p > 3$ and $p \not\equiv 1 \pmod 6$ and $p \not\equiv 5 \pmod 6$, then p is not prime.

Since the contrapositive of our original statement is true, it follows that the original statement holds as well.

Since we covered every case for p, we can conclude the proof!

That's All, Folks!

Thanks for coming to section this week!
Any questions?