Homework#7

Peter Burbery

Abstract

Section

XXXX

XXXX:

In[ ]:= **XXXX**

Out[ ]=

XXXX

- XXXX
- XXXX

Exercise 1

part a

7a

I will explain how the propositions “For all integers a and b, if a×b≡0 (mod 3) then a≡0 (mod 3) or b≡0 (mod 3).” and “For all integers a and b, if 3|a×b then 3|a or 3|b.” are equivalent. By definition, the hypothesis of question #6, a×b≡0 (mod 3) means that 3|(a×b-0), which means 3|a×b, the hypothesis of question #7. The definition for the first part of the conclusion of #6, a≡0 (mod 3) is 3|(a-0). This is equal to 3|a, which is the same as the first part of the conclusion for #7. The definition for the next part of the conclusion of #6, b≡0 (mod 3) is 3|(b-0). This is equal to 3|b, which is the same as the next part of the conclusion for #7.

part b

7b. Prove that for each integer a, if 3 divides a^2, then 3 divides a.

Proof

If $3 \mid a^2$ then $3 \mid a$.

If $3 \mid a^2$ then $a^2 \equiv \mod 3$ and $\exists_{m_1 \in \mathbb{Z}}\, 3\, m_1 = a^2$. We need to show 3|a by demonstrating a≡0 mod 3 and/or $\exists_{m_2 \in \mathbb{Z}}\, 3\, m_2 = a$. We make a constraint for m_1 as $m_1 = a \times m_2$. We have $3\, a \times m_2 = a^2$. We cancel the a and

end up $3\,m_2 = a$. We have now proved that 3|a.

Exercise 2

Page 154, #12 part a).

12. (a) Use the result in Proposition 3.33 to help prove that for each integer a,
if 5 divides a^2, then 5 divides a.

We will use proof by contradiction by demonstrating that if we assume $5 \mid a^2$ and 5 doesn't divide a, we end up with nonsense.

We know that 5 doesn't divide a means that $a \not\equiv 0 \pmod 5$.

We use Proposition 3.33 to conclude that since $a \not\equiv 0 \pmod 5$, then $a^2 \equiv 1 \pmod 5$ or $a^2 \equiv 4 \pmod 5$.

We have two cases.

Case 1 ($a^2 \equiv 1 \pmod 5$):

We know that $5 \mid a^2$ means $\exists_{m_1, m_1 \in \mathbb{Z}}\ a^2 = 5\,m_1$.

We know $a^2 \equiv 1 \pmod 5$ means that $\exists_{m_2, m_2 \in \mathbb{Z}}\ a^2 = 5\,m_2 + 1$.

We can use these two equations by equating them because they both equal a^2:

$5\,m_1 = 5\,m_2 + 1$

After some algebraic manipulations, we obtain the following:

$m_1 = m_2 + \frac{1}{5}$

We assumed m_2 is an integer, but if we add the rational number $\frac{1}{5}$ to the integer m_2, we don't get an integer for m_1, which must be a rational number. The fact that m_1 is a rational number that's not an integer contradicts our assumption that m_1 was an integer. We conclude the assumption is false. We have proved $5 \mid a^2$ and $a^2 \not\equiv 1 \bmod 5$ by negating the contradictory assumption that $a^2 \equiv 1 \bmod 5$.

Case 2 ($a^2 \equiv 4 \pmod 5$):

We know that $5 \mid a^2$ means $\exists_{m_1, m_1 \in \mathbb{Z}}\ a^2 = 5\,m_1$.

We know $a^2 \equiv 4 \pmod 5$ means that $\exists_{m_3, m_3 \in \mathbb{Z}}\ a^2 = 5\,m_3 + 4$.

We can use these two equations by equating them because they both equal a^2:

$5\,m_1 = 5\,m_3 + 4$

After some algebraic manipulations, we obtain the following:

$m_1 = m_2 + \frac{4}{5}$

We assumed m_3 is an integer, but if we add the rational number $\frac{4}{5}$ to the integer m_3, we don't get an integer for m_1, which must be a rational number. The fact that m_1 is a rational number that's not an

integer contradicts our assumption that m_1 was an integer. We conclude the assumption is false. We have proved $5 \mid a^2$ and $a^2 \not\equiv 4 \bmod 5$ by negating the contradictory assumption that $a^2 \equiv 4 \bmod 5$.

Finishing the Proof

We can conclude from Proposition 3.33 that since $a^2 \not\equiv 1 \bmod 5$ and $a^2 \not\equiv 4 \bmod 5$, the statement $a \not\equiv 0 \pmod 5$ is false. If $a \not\equiv 0 \pmod 5$ is false, then $a \equiv 0 \pmod 5$. We know that $a \equiv 0 \pmod 5$ means that 5|a. We have finished our proof by contradiction that $5 \mid a^2$ implies 5|a.

Exercise 3

Page 154, #12 part b).

12b) Prove that the real number $\sqrt{5}$ is an irrational number.

Proof: Let us assume the negation, which is that $\sqrt{5}$ is rational. Then there exist coprime positive integers b and c such that

$$\sqrt{5} = \frac{b}{c}$$

We cross multiply to obtain

$b = c\sqrt{5}$

Squaring on both sides, we get:

$b^2 = 5\,b^2$

Therefore b^2 is divisible by 5. Since $5 \mid b^2$, 5|b based on homework exercise #2. We can write b=5p for some integer p. Substituting we have $25\,p^2 = 5\,c^2$, which simplifies to $c^2 = 5\,b^2$.

This means c^2 is also divisible by 5. Since $5 \mid c^2$, 5|c.

We know see that b and c have at least one common factor, that is, 5.

But this contradicts our statement that b and c are coprime.

We made a false assumption.

Therefore $\sqrt{5}$ is irrational.

Exercise 4

1. Page 154, #13 parts a) and b).

part a

Proposition 13a is “Prove that for each integer a, if a≢0 (mod 7) then $a^2 \not\equiv 0 \pmod 7$.

Proof: We will prove this proposition using cases for a based on congruence modulo 7. In doing so, we will use the results in Theorem 3.28 and Theorem 3.30. Because the hypothesis is a≢0 (mod 7), we can

use four cases, which are: (1) a≡1 (mod 7), (2) a≡2 (mod 7), (3) a≡3 (mod 7), (4) a≡4 (mod 7), (5) a≡5 (mod 7), (6) a≡6 (mod 7).

Case 1 (a≡1 (mod 7))

In this case, we use Theorem 3.28 to conclude that

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

This proves that if $a \equiv 1 \pmod 7$, then $a^2 \equiv 1 \pmod 7$.

Case 2 (a≡2 (mod 7))

In this case, we use Theorem 3.28 to conclude that

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

This proves that if $a \equiv 2 \pmod 7$, then $a^2 \equiv 4 \pmod 7$.

Case 3 (a≡3 (mod 7))

In this case, we use Theorem 3.28 to conclude that

$a^2 \equiv 3^2 \pmod 7$ or $a^2 \equiv 9 \pmod 7$

We also know that $9 \equiv 2 \pmod 7$. So we have $a^2 \equiv 9 \pmod 7$ and $9 \equiv 2 \pmod 7$, and we can now use the transitive property of congruence (Theorem 3.30) to conclude that $a^2 \equiv 2 \pmod 7$. This proves that if $a \equiv 3 \pmod 7$, then $a^2 \equiv 2 \pmod 7$.

Case 4 (a≡4 (mod 7))

In this case, we use Theorem 3.28 to conclude that

$a^2 \equiv 4^2 \pmod 7$ or $a^2 \equiv 16 \pmod 7$

We also know that $16 \equiv 2 \pmod 7$. So we have $a^2 \equiv 16 \pmod 7$ and $16 \equiv 2 \pmod 7$, and we can now use the transitive property of congruence (Theorem 3.30) to conclude that $a^2 \equiv 2 \pmod 7$. This proves that if $a \equiv 4 \pmod 7$, then $a^2 \equiv 2 \pmod 7$.

Case 5 (a≡5 (mod 7))

In this case, we use Theorem 3.28 to conclude that

$a^2 \equiv 5^2 \pmod 7$ or $a^2 \equiv 25 \pmod 7$

We also know that $25 \equiv 4 \pmod 7$. So we have $a^2 \equiv 25 \pmod 7$ and $25 \equiv 4 \pmod 7$, and we can now use the transitive property of congruence (Theorem 3.30) to conclude that $a^2 \equiv 4 \pmod 7$. This proves that if $a \equiv 5 \pmod 7$, then $a^2 \equiv 4 \pmod 7$.

Case 6 (a≡6 (mod 7))

In this case, we use Theorem 3.28 to conclude that

$a^2 \equiv 6^2 \pmod 7$ or $a^2 \equiv 36 \pmod 7$

We also know that $36 \equiv 1 \pmod 7$. So we have $a^2 \equiv 36 \pmod 7$ and $36 \equiv 1 \pmod 7$, and we can now use the transitive property of congruence (Theorem 3.30) to conclude that $a^2 \equiv 1 \pmod 7$. This proves that if $a \equiv 6 \pmod 7$, then $a^2 \equiv 1 \pmod 7$.

We know that $a \not\equiv 0 \pmod 7$ means one of the following cases holds true:(1) $a \equiv 1 \pmod 7$, (2) $a \equiv 2 \pmod 7$, (3) $a \equiv 3 \pmod 7$, (4) $a \equiv 4 \pmod 7$, (5) $a \equiv 5 \pmod 7$, (6) $a \equiv 6 \pmod 7$.

We have the following table:

Case ⌗	Hypothesis	Conclusion
1	$a \equiv 1 \pmod 7$	$a^2 \equiv 1 \pmod 7$
2	$a \equiv 2 \pmod 7$	$a^2 \equiv 4 \pmod 7$
3	$a \equiv 3 \pmod 7$	$a^2 \equiv 2 \pmod 7$
4	$a \equiv 4 \pmod 7$	$a^2 \equiv 2 \pmod 7$
5	$a \equiv 5 \pmod 7$	$a^2 \equiv 4 \pmod 7$
6	$a \equiv 6 \pmod 7$	$a^2 \equiv 1 \pmod 7$

We see $a \not\equiv 0 \pmod 7$ means $a^2 \equiv 1 \pmod 7$, or $a^2 \equiv 2 \pmod 7$, or $a^2 \equiv 4 \pmod 7$. This proves that $a \not\equiv 0 \pmod 7$ implies $a^2 \not\equiv 0 \pmod 7$.

part b

13 b. Prove that for each integer a, if 7 divides a^2, then 7 divides a.

Proof:

We will use proof by contradiction by demonstrating that if we assume $7 \mid a^2$ and 7 doesn't divide a, we end up with nonsense.

We know that 7 doesn't divide a means that $a \not\equiv 0 \pmod 7$.

We will use the theorem proved in exercise #13a that if $a \not\equiv 0 \pmod 7$ then $a^2 \not\equiv 0 \pmod 7$.

Since $a \not\equiv 0 \pmod 7$, $a^2 \not\equiv 0 \pmod 7$.

Since $a^2 \not\equiv 0 \pmod 7$, 7 does not divide a^2.

But we assumed $7 \mid a^2$, which contradicts our conclusion that 7 does not divide a^2.

Therefore the premise that $7 \mid a^2$ and 7 does not divide a is false. Therefore $7 \mid a^2$ implies 7 divides a. The proof by contradiction for $7 \mid a^2$ implies 7|a is complete.

Exercise 5

1. Page 156, #22 part b).

For this problem, read the instructions carefully. You are assessing the proof that is presented. No need to write up the presented proof. The instructions tell you how to go about it. (Look at the instructions for Exercise 19 on page 100.) Follow this process.

(b) Proposition. For each integer m, 5 divides $(m^5 - m)$.

Proof. Let $m \in \mathbb{Z}$. We will prove that 5 divides $(m^5 - m)$ by proving that $(m^5 - m) \equiv 0 \pmod 5$. We will use cases.

For the first case, if $m \equiv 0 \pmod 5$, then $m^5 \equiv 0 \pmod 5$ and, hence, $(m^5 - m) \equiv 0 \pmod 5$.

For the second case, if $m \equiv 1 \pmod 5$, then $m^5 \equiv 1 \pmod 5$ and, hence, $(m^5 - m) \equiv (1 - 1) \pmod 5$, which means that $(m^5 - m) \equiv 0 \pmod 5$.

For the third case, if $m \equiv 2 \pmod 5$, then $m^5 \equiv 32 \pmod 5$ and, hence, $(m^5 - m) \equiv (32 - 2) \pmod 5$, which means that $(m^5 - m) \equiv 0 \pmod 5$. ■

This proof is incomplete. The cases for m≡3 (mod 5) and m≡4 (mod 5) are missing.

first case

For the first case, if m≡0 (mod 5) we can use the third property of congruence modulo n that $a^m \equiv b^m \pmod n$ if $a \equiv b \pmod n$ based on Theorem 3.28. We have $m^5 \equiv 0^5 \pmod 5$, which means $m^5 \equiv 0 \pmod 5$. Then we can use the second congruence property to know that (-1) m≡ (-1)(0)(mod 5) Then we can use the second property of congruence from Theorem 3.28 to subtract the two congruence equations m≡0(mod 5) and $m^5 \equiv 0 \pmod 5$ to get $m^5 - m \equiv 0 - 0 \pmod 5$, or $m^5 - m \equiv 0 \pmod 5$.

third case

For the third case, if m≡2 (mod 5), then $m^5 \equiv 32 \pmod 5$ and, hence, $m^5 - m \equiv (32 - 2) \pmod 5$. This means $m^5 - m \equiv 30 \pmod 5$. This means that $m^5 - m \equiv 0 \pmod 5$ because 30≡0(mod 5). This means $m^5 - m \equiv 0 \pmod 5$.

fourth case

For the fourth case, if m≡3 (mod 5), then $m^5 \equiv 3^5$ (mod) (or $m^5 \equiv 243 \pmod 5$). This means that $m^5 \equiv 3 \pmod 5$ because 243≡3 (mod 5). This means that $m^5 \equiv 3 \pmod 5$ because of the transitive property of the modulo relation. We subtract m≡3 (mod 5) to get $m^5 - m \equiv 3 - 3 \pmod 5$ to get $m^5 - m \equiv 0 \pmod 5$.

fifth case

For the fifth case, if m≡4 (mod 5), then $m^5 \equiv 4^5$ (mod) (or $m^5 \equiv 1024 \pmod 5$). This means that $m^5 \equiv 4 \pmod 5$ because 1024≡4 (mod 5). This means that $m^5 \equiv 4 \pmod 5$ because of the transitive property of the modulo relation. We subtract m≡4 (mod 5) to get $m^5 - m \equiv 4 - 4 \pmod 5$ to get $m^5 - m \equiv 0 \pmod 5$.

all cases

We have shown that all cases imply that $m^5 - m \equiv 0 \pmod 5$. This means that $5 \mid m^5 - m$, and the proof is complete. QED.