Running Head: ELEMENTARY NUMBER THEORY

Week 3 Application: Elementary Number Theory

Jered McClure

Walden University

Week 3 Application: Elementary Number Theory

Questions: 3.1-1, 3.2-15, 3.4-2, 3.5-4, 3.6-1

|  |
| --- |
| 3.1-1Let m and n be arbitrary integers.Consider the product of an even m and an odd n is always even. Let m=2k and n=2l+1 That is, 2k(2l+1)= 2(2kl+k)=mn. Note that 2(2kl+k) is even.Therefore, the product of an even integer and an odd integer is always even. |
| 3.2-15“Compute 73 div 10 and 73 mod 10” (Ferland, 2009, p. 124).Let 73, 10 ∈ Z. Observe:   That is, 73=10(7)+3 Such that, n = 73, d = 10, q = 7, r = 3Therefore, 73÷10. |
| 3.4-2Prove:  Observe that . 23 div 3 = 7 3 mod 3 = 2 Note that 3 is a prime element of Z and is not divisible by 2 or 5.Therefore,  |

|  |
| --- |
| 3.5-4Show: .Contradiction: Observe  That is,  **Specifically, gcd(a,b) = 1**. Thus,  So, a2 =pb2. That is, a mod 2 = 0. Thus a = pk where k ∈ Z. It follows pb2=a2=p2k2. So, b2=pk2. Since b2 mod 2 = 0, then b mod 2 =0. **Note, gcd(a,b)=2.** This is a contradiction.Therefore  |
| 3.6-1True or False: 55 ≡ 15(mod 10) Observe that 15|(55-10) 15(3)=45 45+10=55Therefore, 55 ≡ 15(mod 10) is a true assertion. |

Section 3.1: Odd exercises 1-13 (Note that question 1 is at the top of this paper.

|  |
| --- |
| 3.1-3Consider if n2 is even then n is even. Let n ∈ Z and n=2k. That is n2=n(n)=2k(2k)=4k2 Note that 4k2 is even.Therefore, if n2 is even then n is even. |
| 3.1-5Consider for every even integer, n, (-1)n=1. Let n ∈ Z and n = 2k. Such that, (-1)2k=1. Observe that, . Note.Therefore, for every even integer, n, (-1)n=1. |
| 3.1-7What is the status of a Television after the power button on its remote is pressed 50 times, starting from on? Let on=1 and off = -1. Specifically, on = (-1)2 .(Which is the same formula 3.1-5, for every even integer, n, (-1)n=1 .) Thus, the status is (-1)50=1.Therefore, the Television will be on after the power button is pressed 50 times. |

|  |
| --- |
| 3.1-9Consider a|0. Let a ∈ Z. Note that 0=ak. That is, 0 ∈ a or 0 ∈ k. In either case ak=0.Thus, a|0. |
| 3.1-11Consider if a|1, then a = ± 1. That is 1=ak. Note that when a=1, k=1. Also, when a=-1, k=-1. -1(-1)=-12=1, and 1(1)=12=1.Therefore, if a|1, then a = ± 1. |

|  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- |
| 3.1-13(Part A): Consider, (a-1)|(a2-1) where a ∈ Z. Observe (a-1)|(a2-1) =  (a-1)|(a+1)(a-1) = (a+1)(Part B):

|  |  |  |  |
| --- | --- | --- | --- |
|   | (a-1)(a-1) |   |   |
| a2 |   |   |   |   |   |
|   |   |   |   |
|   |   |   |   |
|   |   |   |   |   |
|   | (a-1) |   |   |

 |

Section 3.2: Odd exercises 11-19 (Note that question 15 is at the top of this paper).

|  |  |  |
| --- | --- | --- |
| 3.2-11“Find the quotient and remainder resulting from the integer division problems” (Ferland, 2009, p. 124).

|  |  |
| --- | --- |
| A: 127÷12Let n, d, q, r ∈ Z.If n = 127 and d=12, then q = 10 and r = 7 That is, 127=12(10)+7Such that, 127 div 12 = 10 and 127 mod 12 = 7 | B: 216÷15Let n, d, q, r ∈ Z.If n = 216 and d = 15, then q = 14 and r = 6 That is, 216=15(14)+6Such that, 216 div 15 = 14 and 216 mod 15 = 6 |

 |
| 3.2-13“Verify the conclusions of the Division Algorithm for each of the following” (Ferland, 2009, p. 124).

|  |  |
| --- | --- |
| A: n = 45 and d = 7Let n, d ∈ Z.Note that 45 div 7 = 6 and 45 mod 7 = 3 That is, 45=7(6)+3 Such that, n = 45, d = 7, q = 6, and r = 3 Where q, r ∈ Z. Therefore, 45÷7. | B: n=-37 and d = 4Let n, d ∈ Z.Note that -37 div 4 = -9 and -37 mod 4 = -1 That is, -37 = 4(-9)-1 Such that, n = -37, d = 4, q = -9, and r = -1 Where q, r ∈ Z.Therefore, -37÷4 |

 |
| 3.2-17Compute the following:

|  |  |
| --- | --- |
| A: 67 div 13 and 67 mod 13Let 67, 13 ∈ Z. Observe:   That is, 67=13(5)+2 Such that, n = 67, d = 13, q = 5, r = 2Therefore, 67÷13. | B: -67 div 13 and -67 mod 13Let -67, 13 ∈ Z. Observe:   That is, -67=13(-5)-2 Such that, n = -67, d = 13, q = -5, r = -2Therefore, -67÷13. |

 |

|  |
| --- |
| 3.2-19Given 165 people who need to sit, and rows of 18 seats. How many rows are required?Let 165, 18 ∈ Z.Calculate: 165÷18= ⎡n⎤ 165 div 18 = 9 165 mod 18 = 3 Note that there are still 3 people left standing. ⎡n⎤ = ⎡9⎤ = 10Therefore, 10 rows of seating are required. |

Section 3.4: Odd exercises 1-27

|  |
| --- |
| 3.4-1Prove: . Observe that  That is, 11 div 2 = 5. 11 mod 2 = 1. Note that 2 is a divisor of itself.Therefore, . |
| 3.4-3Prove:  Observe that  That is, -67 div 5 = -13 -67 mod 5 = -2. Note that 5 is a divisor of itself.Therefore,  |
| 3.4-5Prove: 5.821 ∈ Q. Observe that 5.821 =  That is, 5821 div 1000 = 5 5821 mod 1000 = 821 5821 = 1000(5)+821 Note: 1000 mod 2 = 0 and 1000 mod 5 = 0Therefore, 5.821 ∈ Q. |

|  |
| --- |
| 3.4-7Prove:  Observe that  That is, 311 div 99 = 3 311 mod 99 = 14 Such that, 311=99(3)+14 Note that 99 ∈ Z, 99 ≠ 0, and is repeating.Therefore,  |
| 3.4-9Prove:  Observe that  That is, -713 div 165 = -4 -713 mod 165 = -53 Such that, -713 = 165(-4)-53 Note that 165 mod 5 = 0.Therefore,  |
| 3.4-11Let r ∈ Q and n ∈ Z.Prove: nr ∈ Q. If .Therefore, nr ∈ Q. |

|  |  |  |
| --- | --- | --- |
| 3.4-13Let s, r ∈ Q.

|  |  |
| --- | --- |
| A: Prove –s ∈ Q. If .Therefore, –s ∈ Q. | B: Prove r – s ∈ Q. Since  Then Therefore, r – s ∈ Q. |

 |
| 3.4-15Let r ∈ Q and n ∈ Z.Prove: If n ≥ 0, then rn ∈ Q. Note that rn = r(rm+n). Observe that r(rm+1) ∈ Q.Therefore, If n ≥ 0, then rn ∈ Q. |
| 3.4-17Express in lowest term: .Let 65, 39 ∈ Z. gcd(65,39)=13 65 div 13 = 5 39 div 13 = 3Therefore, . |

|  |
| --- |
| 3.4-19Express in lowest term: .Let -513, 72 ∈ Z. gcd(-513,72)= 9 -513 div 9 = -57 72 div 9 = 8Therefore, . |
| 3.4-21Express in lowest term: 3.14 Note that 3.14 =  That is, 314 = 3(100)+14. So gcd(314,100) = 2 314 div 2 = 157 100 div 2 = 50Therefore, . |
| 3.4-23Express in decimal: . 12 \* 10 = 120 **.** 25 \* 4 = 100 **4** 20 \* 10 = 200  25 \* 8 = 200 **8**Therefore, .48 |

|  |
| --- |
| 3.4-25Express in decimal. 3 \*10 = 30 . 7 \* 4 = 28 4 2 \* 10 = 20 7 \* 2 = 14 2 6 \* 10 = 60 7 \* 8 = 56 8 4 \* 10 = 40 7 \* 5 = 35 5 5 \* 10 = 50 7 \* 7 = 49 7 1 \* 10 = 10 7 \* 1 = 7 1 3 \* 10 = 30, Note this is the first repeat.Therefore,.  |
| 3.4-27Express in decimal:  8 \* 10 = 80 **.** 15 \* 5 = 75 **5** 5 \* 10 = 50 15 \* 3 = 45 **3** 5 \* 10 = 50, Note this is the first repeat, and will continue to repeat.Therefore, |

Section 3.5: Exercises 1-7.

|  |
| --- |
| 3.5-1Show: Contradiction: Observe  That is,  **Specifically, gcd(a,b) = 1**. Thus, So, a2 =3b2. That is, a mod 2 = 0. Thus a = 3k where k ∈ Z. It follows 3b2=a2=9k2. So, b2=3k2. Since b2 mod 2 = 0, then b mod 2 =0. **Note, gcd(a,b)=2.** This is a contradiction.Therefore  |
| 3.5-3Show: Contradiction: Observe  That is,  **Specifically, gcd(a,b) = 1**. Thus,  So, a2 =13b2. That is, a mod 2 = 0. Thus a = 13k where k ∈ Z. It follows 13b2=a2=169k2. So, b2=13k2. Since b2 mod 2 = 0, then b mod 2 =0. **Note, gcd(a,b)=2.** This is a contradiction.Therefore  |
| 3.5-7Show: Contradiction: Observe  That is,  **Specifically, gcd(a,b) = 1**. Thus,  So, a3 =7b3. Since 7|a3, 7|a. That is, a = 7c  Thus a = 7c where c ∈ Z. It follows 7b3=a3=343k3. So, b3=7k3. Since 7|b3, then 7|b. **Note, gcd(a,b)=7.** This is a contradiction.Therefore  |

Section 3.6: Odd exercises 1-7, 39, 41, and 47 (Note that question 1 is located at the top of this paper).

|  |
| --- |
| 3.6-3True or False: -7 ≡ 21 (mod 6). Observe: -7|(21-6) is a false statement gcd(15,-7)=1Therefore, -7 ≡ 21 (mod 6) is a false assertion. |
| 3.6-5What day was it on Jan 8, 1987 if it was Monday Oct 19, 1987? There are 283 days between Jan 8, 1987 and Oct 19, 1987 (assuming this is not a leap year). There are 7 days in a week. 283 mod 7 = 3. Given: 0 1 2  **3** 4 5 6 M T W **Th** F S SuTherefore, it was a Thursday on Jan 8, 1987. |
| 3.6-7What time is it 279 hours from 6 A.M.? 279 hours + 6 hours = 285 hours 285 mod 24 = 21 21 mod 12 = 9 285 div 24 = 11Therefore, it is 9 P.M. 11 days later. |

|  |
| --- |
| 3.6 – 39Given the linear cipher function f=(2x+8) encrypt the message “DISCRETE MATH” using a modulus of 27 and the English alphabet with a space character for 0.D 2(4)+8 mod 27=16 P 2(0)+8 mod 27= 8 HI 2(9)+8 mod 27= 26 Z M 2(13)+8 mod 27= 7 GS 2(19)+8 mod 27= 19 S A 2(1)+8 mod 27= 10 JC 2(3)+8 mod 27= 14 N T 2(x)+8 mod 27= 21 UR 2(18)+8 mod 27=17 Q H 2(8)+8 mod 27= 24 XE 2(5)+8 mod 27= 18 RT 2(20)+8 mod 27= 21 UE 2(5)+8 mod 27= 18 REncrypted: “PZSNQRURHGJUX” |
| 3.6-41Decrypt “QPVOZ” using x = 14 (y – 13) mod 27.Q 14 (17 – 13) mod 27 = 2 BP 14 (16 – 13) mod 27 = 15 OV 14 (22 – 13) mod 27 = 18 RO 14 (15 – 13) mod 27 = 1 AZ 14 (y – 13) mod 27 = 20 TDecrypted: “BORAT” |
| 3.6-47Use: x7(mod 55) = y to encrypt. Use: y3(mod 55)=x to decrypt.

|  |  |
| --- | --- |
| A.American Express, 87(mod 55) = 2 Encrypted | B.Visa, 497(mod 55) = 14 Encrypted |
| C.Encrypted 12, 123(mod 55)= 23 Discover | D.Encrypted 35, 353(mod 55)=30 MasterCard |

 |

Reference

Ferland, K. (2009). *Discrete Mathematics.* Boston: Houghton Mifflin Company.