4.1

2.a) $a = a.1 \rightarrow 1 | a$

2.b) $0 = a.0 \rightarrow a | 0$

4) $a|b \rightarrow \exists\, k \in \mathbb{Z} \quad b = ka$

$b|c \rightarrow \exists\, k' \in \mathbb{Z} \quad c = k'b$

$c = k'b \rightarrow c = k'(ka) \rightarrow c = (k'k)a \rightarrow a|c$

14)

$a \equiv 11 \pmod{19}$ $\quad 0 \leq c \leq 18$

$b \equiv 3 \pmod{19}$

a) $a \overset{19}{\equiv} 11 \rightarrow 13a \overset{19}{\equiv} 13 \times 11 \rightarrow 13a \overset{19}{\equiv} 143$

$\rightarrow 13a \overset{19}{\equiv} (143 \bmod 19) \rightarrow 13a \overset{19}{\equiv} 10 \leftrightarrow \boxed{c = 10}$

$143 \bmod 19 = 10 \quad : \quad 143 \div 19 = 7$ (remainder $= 10$)

b) $b \overset{19}{\equiv} 3 \rightarrow 8b \overset{19}{\equiv} 24 \rightarrow 8b \overset{19}{\equiv} (24 \bmod 19)$

$\rightarrow 8b \overset{19}{\equiv} 5 \rightarrow \boxed{c = 5}$

c) $a \overset{19}{\equiv} 11 \wedge b \overset{19}{\equiv} 3 \rightarrow a + b \overset{19}{\equiv} 11 + 3 \rightarrow \boxed{c = 14}$

14 - Continued

d) $a \overset{19}{\equiv} 11 \rightarrow 7a \overset{19}{\equiv} 77$ ①

$b \overset{19}{\equiv} 3 \rightarrow 3b \overset{19}{\equiv} 9$ ②

$1,2 \rightarrow 7a + 3b \overset{19}{\equiv} 77 + 9 \rightarrow 7a + 3b \overset{19}{\equiv} (83 \bmod 19)$

$\rightarrow 7a + 3b \overset{19}{\equiv} 7 \rightarrow \boxed{c = 7}$

e) $a \overset{19}{\equiv} 11 \rightarrow a^2 \overset{19}{\equiv} 121 \rightarrow 2a^2 \overset{19}{\equiv} 242$ ①

$b \overset{19}{\equiv} 3 \rightarrow b^2 \overset{19}{\equiv} 9 \rightarrow 3b^2 \overset{19}{\equiv} 27$ ②

$① \wedge ② \rightarrow 2a^2 + 3b^2 \overset{19}{\equiv} 242 + 27$

$\rightarrow 2a^2 + 3b^2 \overset{19}{\equiv} (469 \bmod 19)$

$\rightarrow 2a^2 + 3b^2 \overset{19}{\equiv} 13 \longrightarrow \boxed{c = 13}$

f) $a \overset{19}{\equiv} 11 \longrightarrow a^3 \overset{19}{\equiv} (11)^3 = 1331$ ①

$b \overset{19}{\equiv} 3 \rightarrow b^3 \overset{19}{\equiv} 27 \rightarrow 4b^3 \overset{19}{\equiv} 108$ ②

$① \wedge ② \rightarrow a^3 + 4b^3 \overset{19}{\equiv} 1439 \rightarrow a^3 + 4b^3 \overset{19}{\equiv} (1439 \bmod 19)$

$\rightarrow a^3 + 4b^3 \overset{19}{\equiv} 14 \rightarrow \boxed{c = 14}$

6) $a|c \wedge b|d \wedge a \neq 0 \rightarrow ab|cd$

$$\left.\begin{array}{l}\exists k_1 \quad c = ak_1 \\ \exists k_2 \quad d = bk_2\end{array}\right\} \rightarrow cd = ab\, k_1 k_2$$

$K_0 = k_1 k_2$ having $k = k_0$ we can say

$\exists K \quad cd = ab\,K \Rightarrow ab|cd$

10) $44 = 8 \times 5 + 4 \rightarrow r = 4 \quad q = 5$

$777 = 21 \times 37 + 0 \rightarrow r = 0 \quad q = 37$

$-123 = 19 \times (-7) + 10 \rightarrow r = 10 \quad q = -7$

$-1 = 23 \times (-1) + 22 \rightarrow r = 22 \quad q = -1$

$-2002 = 87 \times (-24) + 86 \rightarrow r = 86 \quad q = -24$

$0 = 17 \times 0 + 0 \rightarrow r = 0 \quad q = 0$

$1234567 = 1001 \times 1233 + 334 \rightarrow r = 334 \quad q = 1233$

$-100 = 101 \times (-1) + 1 \rightarrow r = 1 \quad q = -1$

12) $100 \bmod 24 = 4$

time now $= 2 \rightarrow$ time after 100 h is $2 + 4 = 6$

12 - Continued

b) 45 mod 24 = 21

time now = 12 $\rightarrow$ before : 12 − 21 = −9

−9 mod 24 = 15

another way : time now − 45 = 12 − 45 = −33

−33 mod 24 = 15

c) 19 + 168 mod 24 = 19

---

18) If $a \in \mathbb{Z} \wedge b \in \mathbb{Z} \wedge b > 1 \wedge a = qb + r$
$0 \leq r < b \wedge q \in \mathbb{Z}$

Then $q = \lfloor a/b \rfloor \wedge r = a - b \lfloor a/b \rfloor$

Solution:

$a = qb + r \rightarrow r = a - qb$

$0 \leq r < b \rightarrow 0 \leq a - qb < b \rightarrow 0 \leq \frac{a - qb}{b} < 1$

$\rightarrow \lfloor \frac{a-qb}{b} \rfloor = 0 \rightarrow \lfloor \frac{a}{b} - q \rfloor = 0$ (1)

Sinse $q \in \mathbb{Z}$ $\lfloor \frac{a}{b} - q \rfloor = \lfloor \frac{a}{b} \rfloor - q$ (2)

(1), (2) $\rightarrow \lfloor \frac{a}{b} \rfloor - q = 0 \rightarrow q = \lfloor \frac{a}{b} \rfloor$ is Continued

18-continued

$r = a - qb \wedge q = \lfloor \frac{a}{b} \rfloor \rightarrow r = a - \lfloor \frac{a}{b} \rfloor b$

Note: in this question the premise $b>1$ is not used and is not necessary and the question must be corrected. However it is required for b to be positive to be able to use the "division theorem". So, $b=1$ can be included.

30-a) $(177+270) \bmod 31 = 13$

30-b) $(177 \cdot 270) \bmod 31 = 19$

---

38) There are 2 cases for n. whether n is odd or even. Case 1: $n = 2k$ for some $k \in \mathbb{Z}$:

Then $n^2 = 4k^2$ which $4 \mid 4k^2 - 0$ Thus

$4k^2 \equiv 0 \pmod 4 \Rightarrow n^2 \equiv 0 \pmod 4$

Case 2. n is odd so $n = 2k-1$ for some $k \in \mathbb{Z}$:

$n^2 = 4k^2 - \cancel{4}k + 1 \Rightarrow n^2 = 4(k^2-k)+1 \Rightarrow 4 \mid \underbrace{4(k^2-k)+1}_{n^2} - 1$

$\Rightarrow 4 \mid n^2 - 1 \Rightarrow n^2 \equiv 1 \pmod 4$

40) n is odd so $n = 2k+1$ for some $k \in \mathbb{Z}$

$n^2 = 4k^2 + 4k + 1 = 4k(k+1) + 1$

between two concequense numbers k and $k+1$

one of them is even. ~~and~~ WLG we can assume

k is even and $k = 2l$ for some $l \in \mathbb{Z}$ Thus

$n^2 = 4k(k+1) + 1 = 4(2l)(k+1) + 1$

$= 8l(k+1) + 1$

$8 \mid \underbrace{8l(k+1)+1}_{=n^2} - 1 \rightarrow 8 \mid n^2 - 1$

$\rightarrow 1 \equiv n^2 \pmod{8}$

44) $m \geq 2 \rightarrow a \cdot_m (b +_m c) = a \cdot_m b +_m a \cdot_m c$

$\forall a, b, c \in \mathbb{Z}_m$

Proof in the next page

we prove That both sides are equal to

" $ab + ac \mod m$ "

right side /

$a \cdot_m b +_m a \cdot_m c$

let's say $a \cdot_m b = K_1$ and $a \cdot_m c = K_2$. This means

$a \cdot b \mod m = K_1$ Then $a \cdot b = q_1 m + K_1 \quad \exists q_1 \in \mathbb{Z}$

Thus $K_1 = a \cdot b - q_1 m$

The same way we have $K_2 = a \cdot c - q_2 m \quad \exists q_2 \in \mathbb{Z}$

right side $= K_1 +_m K_2$ which means $K_1 + K_2 \mod m$

$K_1 + K_2 = ab - q_1 m + a \cdot c - q_2 m = ab + ac - (q_1 + q_2) m$

and $K_1 + K_2 \mod m = ab + ac - (q_1 + q_2) m \mod m$

$= ab + ac \mod m$ so

right side $= ab + ac \mod m$ Continued

4.4 - Continued

left side / $a \cdot_m (b +_m c)$

let's say $b +_m c = k$. This means $b+c \bmod m = k$

which means $b + c = qm + k$ for some $q \in \mathbb{Z}$

so $k = b + c - qm$

$a \cdot_m (b +_m c) = a \cdot_m k = a \cdot_m (b + c - qm)$

$= a \cdot (b + c - qm) \bmod m$

$= (a \cdot b + a \cdot c - aqm) \bmod m$

$= a \cdot b + a \cdot c \bmod m$

so the left side also is equal to

$a \cdot b + a \cdot c \bmod m$ so left side = right side

$\rightarrow a \cdot_m (b +_m c) = (a \cdot_m b) +_m (a \cdot_m c)$

Note: assumption $m \geq 2$ is not needed!

4.3

8) First we need to have the Primes less Than $\sqrt{n}$, using a sieve algorithm. Then we utilize it in our Trial Divison algorithm:

```
Precedure Trial_division (n : integer)
  if n = 1  return [1]
Primelist = Sieve(√n)
  Prime_factors = [ ]
  For i ∈ Primelist
      break,
      while n mod i = 0
          add i to Prime_factors,
          n ← n/i
  if n>1  add n to Prime_factors,
  return Prime_factors.
```

10) Proof by Contradiction. let's say $m \neq 2^n$ for some $n \in \mathbb{Z}^+$. This means

(either m is odd strictly bigger Than 1 $\oplus$ m is even $\vee$ m is 1)

Note: $\oplus$ is exclusive or

Case 1 : m is odd, $m > 1$

for any such m we have

$x^m + 1 = (x+1)(x^{m-1} - x^{m-2} + \cdots + 1)$ evaluating $x = 2$ we have $2^m + 1 = 3(\cdots)$ which means $3 \mid 2^m + 1$ and This contradicts The fact That $2^m + 1$ is prime.

Case2 : m is even or m is 1

if $m \neq 1$ Then $\exists k_1 \in \mathbb{Z}$ $m = 2k_1$ Then $2^m + 1 = 2^{2k_1} + 1 = 4^{k_1} + 1$ with The same argument as Case 1, k_1 could not be odd strictly bigger Than 1 otherwise $5 \mid 2^m + 1$ which Contradicts The fact That $2^m + 1$ is Prime

(Continued)

10 - Continued

so K_1 is either even or 1. Continuing This argument we have $m = 2K_1$, $K = 2K_2$, $K_2 = 2K_3$ ... until we ~~rea~~ reach 1 which means There exist an n for which $K_n = 1$ This shows $m = 2^n$.

14) 5, 7, 11

16 - a) yes b) yes

c) yes d) yes

18) a) $6 = 3 + 2 + 1$

$28 = 14 + 7 + 4 + 2 + 1$

b) if $2^p - 1$ is prime all factors of $2^{p-1}(2^p - 1)$ are as follow: 2^i $i = 0, 1, \ldots p-1$ and $(2^p - 1)2^i$ $i = 0, 1, \ldots p-2$

sum of all factors other Than The number itself:

$$\sum_{i=0}^{p-1} 2^i + (2^p - 1)\sum_{i=0}^{p-2} 2^i = 2^p - 1 + (2^p - 1)(2^{p-1} - 1) = (2^p - 1)(2^{p-1})$$ ✓

28) $\gcd(1000, 625) = 125$

$lcm(1000, 625) = 5000$

$5000 \times 125 = 625 \times 1000 = 625000$ ✓

---

32) a-1 b-1 c-1 d-139

e-1 f-1

sample (d)

$14039 \bmod 1529 = 278$

$1529 \bmod 278 = 139$

$278 \bmod 139 = 0$

$\rightarrow 139 = \gcd$

---

50) $a \overset{m}{\equiv} b \rightarrow m \mid a-b \rightarrow \exists k \in \mathbb{Z} \quad a-b = mk$

$\gcd(a,m) \mid m$

$\gcd(a,m) \mid a$

$\rightarrow \gcd(a,m) \mid a-mk$

$\rightarrow \gcd(a,m) \mid b$ ~~The same way ge~~

$\gcd(a,m) \mid b \wedge \gcd(a,m) \mid m \rightarrow \gcd(a,m) \mid \gcd(b,m)$ ①

The same way $\gcd(b,m) \mid \gcd(a,m)$ ② ①,② $\rightarrow \gcd(a,m) = \gcd(b,m)$

54) let's assume we have finite primes in the form of $3k+2$ namely $p_1 p_2 \cdots p_n$ and 2

$A = 3 p_1 p_2 \cdots p_n + 2$ is a new number in the form $3k+2$. It is either prime or has a prime factor. If it is prime we have found a new prime in the form $3k+2$ which contradicts the assumption. ~~and~~ If it has prime factor we show that at least one of these factors is a new prime p other than $p_1, p_2, \dots, p_n$ and in the form of $3k+2$

whatever form this factor has it could not be one of $p_1, p_2 \cdots p_n$ because if it is then $(p \mid 3p_1 p_2 \cdots p_n \wedge p \mid A) \rightarrow p \mid A - 3p_1 p_2 \cdots p_n \rightarrow p \mid 2 \rightarrow p = 2$ so p is new.

Now we need to show that p has a form $3k+2$:

$3 \nmid A$ because if $3 \mid A$ since $3 \mid 3p_1 p_2 \cdots p_n$ then $3 \mid 2$ $\times$.

let's say ~~[illegible]~~ all factors of A are in the form $3k+1$ this means A is in the form $3k+1$ while is not so it is in the form $3k+2$