Homework 7 4.1

4\. if $a|b$ and $b|c$, then $a|c$

Proof: let $\exists k, l \in \mathbb{Z}$ because $a, b \in \mathbb{Z}$

So $a \cdot k = b$ and $b \cdot l = c$ because rules of divisibility.

$c = b \cdot l = a \cdot k \cdot l = a(kl)$. by rules of divisibility, $a|c$. proved!

14a) 44 div 8 = 5 r4

14.b) 777 div 21 = 37 r0

14.c) −123 div 19 = −7 r10

14.d) −1 div 23 = −1 r22

16a) 100 mod 24 = 4 So $\boxed{6:00}$

16b) 48 mod 24 = 0 48−45 = 3 12:00 + 3 = $\boxed{15:00}$

16.c 168 mod 24 = 0 $\boxed{19:00}$

18b) $C \equiv 8b \pmod{19} \equiv 8 \cdot 3 \pmod{19} \equiv 24 \bmod 19 = 5$ $\boxed{C=5}$

18.c) $C \equiv a - b \pmod{19} \equiv 11 - 3 \pmod{19} \equiv 8 \pmod{19} = 8$ $\boxed{C=8}$

18.e) $C \equiv 2a^2 + 3b^2 \pmod{19} \equiv 2 \cdot 11^2 + 3 \cdot 3^2 \pmod{19} \equiv 242 + 27 \pmod{19}$

$\equiv 269 \bmod 19 = 3$ $\boxed{C=3}$

26.a) −17 mod 2 = 1 26.b) 144 mod 7 = 4 26.c) −101 mod 13 = 3

26.d) 199 mod 19 = 9

30.b) $17-29=-12$ $\quad -12 \bmod 29 = \boxed{-12}$

34.a) $37 = 7\cdot 5+2$. Not congruent to $3 \bmod 7$

34.b) $66 = 7\cdot 9+3$ Congruent to $3 \bmod 7$

34.c) $-17 = 7\cdot -3+4$ Not congruent to $3 \bmod 7$

34.d) $-67 = 7\cdot -10+3$ Congruent to $3 \bmod 7$

38.b) $(32^3 \bmod 13)^2 \bmod 11 \equiv ((32 \bmod 13)^3 \bmod 13)^2 \bmod 11$

$\equiv (6^3 \bmod 13)^2 \bmod 11 \equiv (216 \bmod 13)^2 \bmod 11$

$\equiv 8^2 \bmod 11 \equiv 64 \bmod 11 = \boxed{9}$

38.d) $(21^2 \bmod 15)^3 \bmod 22 \equiv ((21 \bmod 15)^2 \bmod 15)^3 \bmod 22$

$\equiv (6^2 \bmod 15)^3 \bmod 22 \equiv (36 \bmod 15)^3 \bmod 22 \equiv 6^3 \bmod 22 \equiv 216 \bmod 22$

$\equiv \boxed{18}$

4.2

2.a) $321 = 2\cdot 160+1$ $\quad 160 = 2\cdot 80+0$ $\quad 80 = 2\cdot 40+0$

$40 = 2\cdot 20+0$ $\quad 20 = 2\cdot 10+0$ $\quad 10 = 2\cdot 5+0$ $\quad 5 = 2\cdot 2+1$

$2 = 2\cdot 1+0$ $\quad 1 = 1\cdot 0+1 = (101000001)_2$

2.b) $1023 = 2\cdot 511+1$ $\quad 511 = 255\cdot 2+1$ $\quad 255 = 2\cdot 127+1$ $\quad 127 = 2\cdot 63+1$

$63 = 2\cdot 31+1$ $\quad 31 = 2\cdot 15+1$ $\quad 15 = 2\cdot 7+1$ $\quad 7 = 2\cdot 3+1$ $\quad 3 = 2\cdot 1+1$

$1 = 1\cdot 0+1$

$(1111111111)_2$

2.c) $100632 = 2\cdot 50316$ $\quad 50316 = 2\cdot 25158$ $\quad 25158 = 2\cdot 12579$

$12579 = 2\cdot 6289+1$ $\quad 6289 = 2\cdot 3144+1$ $\quad 3144 = 2\cdot 1572$ $\quad 1572 = 2\cdot 786$

$786 = 2\cdot 393$ $\quad 393 = 2\cdot 196+1$ $\quad 196 = 2\cdot 98$ $\quad 98 = 2\cdot 49$ $\quad 49 = 2\cdot 24+1$

$24 = 2\cdot 12$ $\quad 12 = 2\cdot 6$ $\quad 6 = 2\cdot 3$ $\quad 3 = 2\cdot 1+1$ $\quad 1 = 1\cdot 0+1$

$= (11000100100011000)_2$

4.b) $(10\,1011\,0101)_2 = 1\cdot2^9+1\cdot2^7+1\cdot2^5+1\cdot2^4+1\cdot2^2+1\cdot2^0 = \boxed{693}$

4.d) $(111\,1100\,0001\,1111)_2 = 2^{14}+2^{13}+2^{12}+2^{11}+2^{10}+2^4+2^3+2^2+2^1+2^0$

$= \boxed{31775}$

6.b) 101 010 101 010

5 2 5 2 $=(5252)_8$

6.d) 101 010 101 010 101

5 2 5 2 5 $=(52525)_8$

8.) B A D F A C E D $= (1011\,1010\,1101\,1111\,1010\,1100\,1110\,1101)_2$

1011 1010 1101 1111 1010 1100 1110 1101

12.) 1 1000 0110 0011 $= (1863)_{16}$

1 8 6 3

23.c)

$$\begin{array}{r} 1111 \\ +\;\;777 \\ \hline 2110 \end{array} \qquad \begin{array}{r} 777 \\ \cdot\;1111 \\ \hline 777 \\ 7770 \\ 77700 \\ 777000 \\ \hline 1107667 \end{array}$$

24.a)

$$\begin{array}{r} 1AE \\ +\;BBC \\ \hline D6A \end{array} \qquad \begin{array}{r} 1AE \\ \cdot\;BBC \\ \hline 1428 \\ 127A0 \\ 127A00 \\ \hline 13B5C8 \end{array}$$

24.c)

$$\begin{array}{r} ABCDE \\ +\;1111 \\ \hline ACDEF \end{array} \qquad \begin{array}{r} ABCDE \\ \cdot\;1111 \\ \hline ABCDE \\ ABCDE0 \\ ABCDE00 \\ ABCDE000 \\ \hline B74148BE \end{array}$$

26. $11^{644} \bmod 6$ $\quad$ $664 = (1010000100)_2$

$x = 1$ $\quad$ $11 \bmod 645 = 11$

$x = 1$ $\quad$ $11^2 \bmod 645 = 121$

$x = 1$ $\quad$ $121^2 \bmod 645 = 451$

$x = 1 \cdot 451$ $\quad$ $451^2 \bmod 645 = 226$

$x = 451$ $\quad$ $226^2 \bmod 645 = 121$

$x = 451 \cdot 121 \bmod 645 = 391$ $\quad$ $121^2 \bmod 645 = 451$

$x = 391$ $\quad$ $451^2 \bmod 645 = 226$

$x = 391 \cdot 226 \bmod 645 = \boxed{1}$ $\quad$ $226^2 \bmod 645 = 226$

$\boxed{x = 1}$

---

28. $123^{1001} \bmod 101$ $\quad$ $1001 = (1111101001)_2$

$x = 1$ $\quad$ $123 \bmod 101 = 22$

$x = 22$ $\quad$ $22^2 \bmod 101 = 80$

$x = 22$ $\quad$ $80^2 \bmod 101 = 37$

$x = 22$ $\quad$ $37^2 \bmod 101 = 56$

$x = 22 \cdot 56 \bmod 101 = 20$ $\quad$ $56^2 \bmod 101 = 5$

$x = 20$ $\quad$ $25 \bmod 101 = 25$

$x = 20 \cdot 25 \bmod 101 = 96$ $\quad$ $25^2 \bmod 101 = 19$

$x = 96 \cdot 19 \bmod 101 = 6$ $\quad$ $19^2 \bmod 101 = 58$

$x = 6 \cdot 58 \bmod 101 = 45$ $\quad$ $58^2 \bmod 101 = 31$

$x = 45 \cdot 31 \bmod 101 = 82$ $\quad$ $31^2 \bmod 101 = 52$

$x = 82 \cdot 52 \bmod 101 = \boxed{22}$ $\quad$ $52^2 \bmod 101 = 78$

Section 4.3

2.d) yes 2.e) yes 2.f) yes

4.c) $101 = 101 \cdot 1$ 4.e) $289 = 17^2$ 4.f) $899 = 29 \cdot 31$

14.) 1, 5, 7, 11

16.b) $14 = 2 \cdot 7$ $17 = 17 \cdot 1$ $85 = 5 \cdot 17$

Not pairwise relativly prime

---

28 $a = 1000 = 10^3 = (2 \cdot 5)^3 = 2^3 \cdot 5^3$

$b = 625 = 5^4$ $\gcd(a,b) = 5^{\min(3,4)} = 125$

$\operatorname{lcm}(a,b) = 2^3 \cdot 5^{\max(3,4)} = 5000$

$125 \cdot 5000 = 625{,}000 = 625 \cdot 1000$

32.c) $277 = 123 \cdot 2 + 31$

$123 = 31 \cdot 3 + 30$ $\gcd(123, 277) = 1$

$31 = 30 \cdot 1 + \boxed{1}$

$30 = 30 \cdot 1 + 0$

32.d) $14039 = 1529 \cdot 9 + 278$

$1529 = 278 \cdot 5 + \boxed{139}$ $\gcd(1529, 14039) = 139$

$278 = 139 \cdot 2 + 0$