

Week 3 Homework Solutions

Chapter 2:

Section 4:

$$\begin{array}{lll} 12.39 = 3(13) & 81 = 3^4 & 101 \text{ is prime} \quad 143 = 11(13) \\ 289 = 17^2 & 899 = 29(31) & \end{array}$$

14. A number is divisible by 10^n iff it ends with n zeroes. Hence we wish to find the greatest power of 10 which divides $100!$. Clearly 2 divides $100!$ more than 5 does, so we wish to find the greatest power of 5 which divides $100!$. We observe that 25, 50, 75, and 100 each provide two factors of five and 5, 10, 15, 20, 30, 35, 40, 45, 55, 60, 65, 70, 80, 85, 90, and 95 each provide one factor of five. Hence $100!$ contains 24 factors of five so the number $100!$ ends with 24 zeroes.

16.1, 5, 7, 11

20.A. $1 + 2 + 3 = 6$ $1 + 2 + 4 + 7 + 14 = 28$

B. When $2^p - 1$ is prime the factors of $2^{p-1}(2^p - 1)$ are $1, 2, 4, \dots, 2^{p-1}$ and $1(2^p - 1), 2(2^p - 1), 4(2^p - 1), \dots, 2^{p-1}(2^p - 1)$. The sum of the first row is $2^p - 1$ and the sum of the second row is $2^p - 1$ times that of the first. Hence the sum of all the factors is $2^{p-1}(2^p - 1 + 1) = 2^p(2^p - 1)$. Subtracting the number $2^{p-1}(2^p - 1)$ itself gives us $2^{p-1}(2^p - 1)$ again. Hence $2^{p-1}(2^p - 1)$ is a perfect number when $2^p - 1$ is prime.

22. By definition.

$$\begin{array}{ll} 36 \cdot -17 \pmod{2} = 1 & 144 \pmod{7} = 4 \\ -101 \pmod{13} = 3 & 199 \pmod{19} = 9 \end{array}$$

$$40. \text{lcm}(a, b) = (2^7 3^8 5^2 7^{11}) / (2^3 3^4 5) = 2^4 3^4 5 (7^{11})$$

Section 5:

2. $321 = 101000001$ $1023 = 1111111111$
 $100632 = 11000100100011000$

24. $55 = 34(1) + 11$ $34 = 11(3) + 1$ $11 = 1(11) + 0$
 $\text{gcd}(55, 34) = \text{gcd}(34, 11) = \text{gcd}(11, 1) = 11$
Three divisions are needed.

26. $5 = 1(-1)(-1)$ $13 = 111$ $37 = 1101$ $79 = 100(-1)1$

32. m and $-m$ are complements when the integers are represented in One's complement form.

34. To find $m-n$, it suffices to consider the case where m and n are both positive and $m > n$ since other cases can be solved or reduced to this case by using basic integer facts and ordinary binary addition. We then put $-m$ and n into one's complement form and add them by regular binary addition. The complement of the sum is then $m-n$.

1	1- m_i	...	1- m_1	1- m_0	- m in one's complement
0	n_i	...	n_1	n_0	n in one's complement
1	1- m_i+n_i	...	1- m_1+n_1	1- m_0+n_0	Sum
0	m_i-n_i	...	m_1-n_1	m_0-n_0	Complement of Sum = $m-n$

Section 6:

4. $937(13) = 12181 = 2436(5) + 1$. So $937(13) \equiv 1 \pmod{2436}$ so 937 is the inverse of 13 mod 2436.

6. $2(9) \equiv 1 \pmod{17}$ so 9 is an inverse of 2 mod 17.

14.A. 2 and 6 3 and 4 7 and 8 5 and 9

B. $10! = 1(2)(3)(4)(5)(6)(7)(8)(9)(10) = 1(2)(6)(3)(4)(7)(8)(5)(9)(10) \equiv 10 \equiv -1 \pmod{11}$

22. By the Chinese Remainder Theorem there is a unique solution to the system of equations. Hence there is a unique representation in that form.

26. $x \equiv 0 \pmod{5}$ and $x \equiv 1 \pmod{3}$. By inspection, this solves to $x \equiv 10 \pmod{15}$.

28. $3^{302} \pmod{5} = 3^{302 \pmod{4}} \pmod{5} = 3^2 \pmod{5} = 9 \pmod{5} = 4$

$3^{302} \pmod{7} = 3^{302 \pmod{6}} \pmod{7} = 3^2 \pmod{7} = 9 \pmod{7} = 2$

$3^{302} \pmod{11} = 3^{302 \pmod{10}} \pmod{11} = 3^2 \pmod{11} = 9 \pmod{11} = 9$

Let $x = 3^{302} \pmod{385}$. Then we have the system of equations:

$x \equiv 4 \pmod{5}$ $x \equiv 2 \pmod{7}$ $x \equiv 9 \pmod{11}$ so

$x \equiv 77(y_1)(4) + 55(y_2)(2) + 35(y_3)(9) \pmod{385}$ we compute

$77y_1 \equiv 1 \pmod{5}$ $55y_2 \equiv 1 \pmod{7}$ $35y_3 \equiv 1 \pmod{11}$ so

$2y_1 \equiv 1 \pmod{5}$ $6y_2 \equiv 1 \pmod{7}$ $2y_3 \equiv 1 \pmod{11}$ so

$y_1 = 3$ $y_2 = 6$ $y_3 = 6$ so

$x \equiv 77(3)(4) + 55(6)(2) + 35(6)(9) \equiv 77(12) + 55(12) + 35(54) \equiv$

$924 + 660 + 1890 \equiv 3474 \equiv 9 \pmod{385}$

Hence $3^{302} \pmod{385} = 9$.

36. $a \equiv x \pmod{4}$ and $a \equiv y \pmod{7}$ so $a \equiv 7(z_1)(a) + 4(z_2)(b) \pmod{28}$. We compute

$7z_1 \equiv 1 \pmod{4}$ so $3z_1 \equiv 1 \pmod{4}$ so $z_1 = 3$ and $4z_2 \equiv 1 \pmod{7}$ so $z_2 = 2$. Hence

$x \equiv 21a + 8b \pmod{28}$. We use this to solve for x in the pairs (a,b) below.

$$\begin{array}{llllll} (0,0) = 0 & (1,0) = 21 & (1,1) = 1 & (2,1) = 22 & (2,2) = 2 & (0,3) = 24 \\ (2,0) = 14 & (3,5) = 19 & (3,6) = 27 & & & \end{array}$$

46. ATTACK is represented by the numbers 19, 1900, 210.

$$\begin{aligned} M=19: C &= 19^{13} \pmod{2537} = [(19^8)(19^4)(19)] \pmod{2537} = (2165)(934)(19) \pmod{2537} \\ &= 38420090 \pmod{2537} = 2299 \end{aligned}$$

$$\begin{aligned} M=1900: C &= 1900^{13} \pmod{2537} = (19^{13})(4^{13})(25^{13}) \pmod{2537} = \\ &(2299)(4^8)(4^4)(4)(25^8)(25^4)(25) \pmod{2537} = \\ &(2299)(2111)(256)(4)(255)(2464)(25) \pmod{2537} = \\ &(1478)(2346)(712) \pmod{2537} = 2468780256 \pmod{2537} = 186 \end{aligned}$$

$$\begin{aligned} M = 210: C &= 210^{13} \pmod{2537} = (2^{13})(3^{13})(5^{13})(7^{13}) \pmod{2537} = \\ &(256)(16)(2)(3^8)(81)(3)(5^8)(625)(5)(7^8)(7^4)(7) \pmod{2537} = \\ &(581)(1487)(243)(2464)(588)(737)(2401)(7) \pmod{2537} = \\ &(2371)(1435)(1248) \pmod{2537} = 4246176480 \pmod{2537} = 2117 \end{aligned}$$

The encrypted sequence is 2299, 186, 2117