

**8.A From Textbook 2.3 8ef**

**8ef** 107 and 113 are primes. You only need to test the prime numbers up to  $\lfloor \sqrt{n} \rfloor$ . Since one can see that those numbers are not divisible by 2, 3, 5 nor 11, and that  $70+35 = 15 \times 7 = 105$ , those numbers are prime (and you don't need a calculator to find it out).

**8.B From Textbook 2.3 10ef**

**10ef**  $289 = 17^2$  and  $899 = 29 \cdot 31$  One can easily see that 2, 3, 5 and 11 do not divide those numbers. For 7: 280 is 7·40, and 910 is 700 + 210 and 7 does not divide 9 nor -11. You just need to try 13 and above.

**8.C From Textbook 2.3 28ab**

**28a**  $-17 \pmod 2 = 1$                       **28b**  $144 \pmod 7 = 140 + 4 \pmod 7 = 4$

**8.D From Textbook 2.3 46c**

**46c** EAT DIM SUM

**9.A From Textbook 2.4 2e**

$$\begin{aligned}
 \mathbf{2e} \quad & \gcd(1529, 14038) &= \gcd(277, 1529 \pmod{277}) &= \gcd(133, 11) \\
 & = \gcd(1529, 14038 \pmod{1529}) &= \gcd(277, 144) &= \gcd(11, 1) \\
 & = \gcd(1529, 277) &= \gcd(144, 133) &= 1
 \end{aligned}$$

**9.B From Textbook 2.4 8ac**

**8a**  $11011_2 = 1 \cdot 2^0 + 1 \cdot 2^1 + 0 \cdot 2^2 + 1 \cdot 2^3 + 1 \cdot 2^4 = 27$   
**8c**  $1110111110_2 = 0 \cdot 2^0 + 1 \cdot 2^1 + 1 \cdot 2^2 + 1 \cdot 2^3 + 1 \cdot 2^4 + 1 \cdot 2^5 + 0 \cdot 2^6 + 1 \cdot 2^7 + 1 \cdot 2^8 + 1 \cdot 9^4$   
 or (lazy way)  $= 100\,0000\,0000_2 - 1_2 - 100\,0000_2 - 1_2$   
 $= 2^{10} - 2^0 - 2^6 - 1$   
 $= 1024 - 1 - 64 - 1 = 958$

**9.C From Textbook 2.4 36**

**36**

$a :$	1	1	1	0	
$b :$	1	0	1	0	
		0	0	0	0
$c_1 :$		0	0	0	0
$c_2 :$	1	1	1	0	
$c_3 :$	0	0	0	0	
$c_4 :$	1	1	1	0	
$carry :$	1	1	1		
$a \cdot b :$	1	0	0	0	1
	1	0	0	0	1
					1
					0
					0

## 10.A From Textbook 2.5 2f

**2f** Note:  $124 = 4 \cdot 31$ ,  $323 = 17 \cdot 19$  and  $\gcd(124, 323) = 1$

$$323 = 2 \cdot 124 + 75 \quad 124 = 1 \cdot 75 + 49$$

$$75 = 1 \cdot 49 + 26 \quad 49 = 1 \cdot 26 + 23$$

$$26 = 1 \cdot 23 + 3 \quad 23 = 7 \cdot 3 + 2$$

$$3 = 1 \cdot 2 + 1$$

$$\begin{aligned} 1 &= 3 - 2 = 3 - (23 - 7 \cdot 3) \\ &= (1 + 7) \cdot (26 - 1 \cdot 23) - 23 \\ &= (1 + 7) \cdot 26 + [(1 + 7) \cdot -1 - 1] \cdot 23 \\ &= (1 + 7) \cdot 26 - (1 + 7 + 1)(49 - 1 \cdot 26) \\ &= (1 + 7 + (1 + 7 + 1)) \cdot (75 - 1 \cdot 49) - (1 + 7 + 1) \cdot 49 \\ &= 17 \cdot 75 - (17 + 9) \cdot (124 - 1 \cdot 75) \\ &= (17 + 26) \cdot (323 - 2 \cdot 124) - 26 \cdot 124 \\ &= 43 \cdot 323 - (2 \cdot 43 + 26) \cdot 124 \end{aligned}$$

$$\gcd(124, 323) = 43 \cdot 323 - 112 \cdot 124 = 1$$

## 10.B From Textbook 2.5 24ab

**24a**  $3^4 \equiv 1 \pmod{5}$ ,  $3^6 \equiv 1 \pmod{7}$ ,  $3^{10} \equiv 1 \pmod{11}$

$$3^{302} \pmod{5} = 3^{300} \cdot 3^2 \pmod{5} = (3^4)^{75} \cdot 9 \pmod{5} = 9 \pmod{5} = 4$$

$$3^{302} \pmod{7} = 3^{300} \cdot 3^2 \pmod{7} = (3^6)^{50} \cdot 9 \pmod{7} = 9 \pmod{7} = 2$$

$$3^{302} \pmod{11} = 3^{300} \cdot 3^2 \pmod{11} = (3^{10})^{30} \cdot 9 \pmod{11} = 9 \pmod{11} = 9$$

**24b** One can see that 9 is solution:  $9 \equiv 3^{302} \pmod{5}$ ,  $9 \equiv 3^{302} \pmod{7}$  and  $9 \equiv 3^{302} \pmod{11}$ .  $x \equiv 3^{302} \pmod{5 \cdot 7 \cdot 11}$  has a unique solution modulus 385, which has to verify the three previous relations. Those three have a unique solution modulus 385, (which is 9) due to the Chinese Remainder Theorem. Therefore, 9 is solution of  $x \equiv 3^{302} \pmod{5 \cdot 7 \cdot 11}$ .

If one is not convinced, there exists integers  $\lambda_1, \lambda_2, \lambda_3$  such that  $3^{302} - 9 = 5 \cdot \lambda_1 = 7 \cdot \lambda_2 = 11 \cdot \lambda_3 = \lambda$ . Because 5, 7 and 11 are relatively primes,  $385 = 5 \cdot 7 \cdot 11 \mid \lambda$  and  $3^{302} \pmod{385} = 9 + \lambda \pmod{385} = 9$ .

If not, one can construct  $x = a_1 M_1 y_1 + a_2 M_2 y_2 + a_3 M_3 y_3$  with  $a_1 = 4$ ,  $a_2 = 2$ ,  $a_3 = 9$ ,  $M_1 = 7 \cdot 11 = 77$ ,  $M_2 = 5 \cdot 11 = 55$ ,  $M_3 = 5 \cdot 7 = 35$ , and  $y_k$  such that  $M_k y_k \equiv 1 \pmod{m_k}$ . Be careful not to consider another formula for  $y_k$ . The only simplification you can do is the following:  $(M_k \pmod{m_k}) y_k \equiv 1 \pmod{m_k}$

For  $y_1$ :  $77 \pmod{5} = 2$ ,  $2 \cdot 3 = 6 \equiv 1 \pmod{5}$  and  $y_1 = 3$

For  $y_2$ :  $55 \pmod{7} = 6$ ,  $6 \cdot 6 = 36 \equiv 1 \pmod{7}$  and  $y_2 = 6$

For  $y_3$ :  $35 \pmod{11} = 2$ ,  $2 \cdot 6 = 12 \equiv 1 \pmod{11}$  and  $y_3 = 6$

$$x = 4 \cdot 77 \cdot 3 + 2 \cdot 55 \cdot 6 + 9 \cdot 35 \cdot 6 = 924 + 660 + 1890 = 3474 \equiv 9 \pmod{385}$$

## 10.C From Textbook 2.5 26di

**26d**  $a \pmod{4} = 2$ ,  $a \pmod{7} = 1$

$$a = 4k + 2 = 7l + 1 = 22$$

(take  $k = 5$  and  $l = 3$ )

**26i**  $a \pmod{4} = 3$ ,  $a \pmod{7} = 6$

$$a = 4k - 1 = 7l - 1 = 27$$

(take  $k = 7$  and  $l = 4$ )