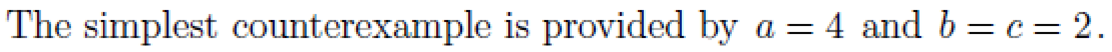
CSE 15 Homework 8

Solution (20pt total)

Type your answers in a text file and submit it in CatCourses.
You can also write your answers on papers and scan them into image files for submission.

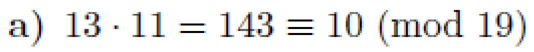
Section 4.1

8. (1pt)

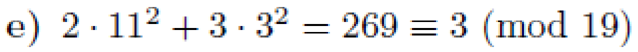


The simplest counterexample is provided by $a = 4$ and $b = c = 2$.

14. (1pt each, 2pt total)

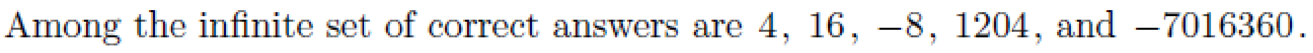


a) $13 \cdot 11 = 143 \equiv 10 \pmod{19}$



e) $2 \cdot 11^2 + 3 \cdot 3^2 = 269 \equiv 3 \pmod{19}$

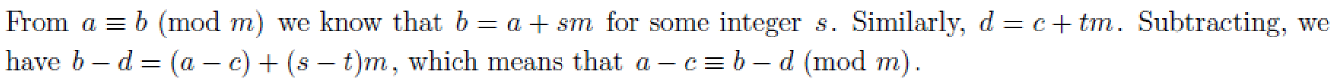
26. (1pt)



Among the infinite set of correct answers are 4, 16, -8, 1204, and -7016360.

(There can be other solutions)

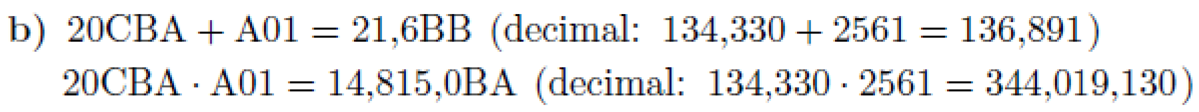
34. (1pt)



From $a \equiv b \pmod{m}$ we know that $b = a + sm$ for some integer s. Similarly, $d = c + tm$. Subtracting, we have $b - d = (a - c) + (s - t)m$, which means that $a - c \equiv b - d \pmod{m}$.

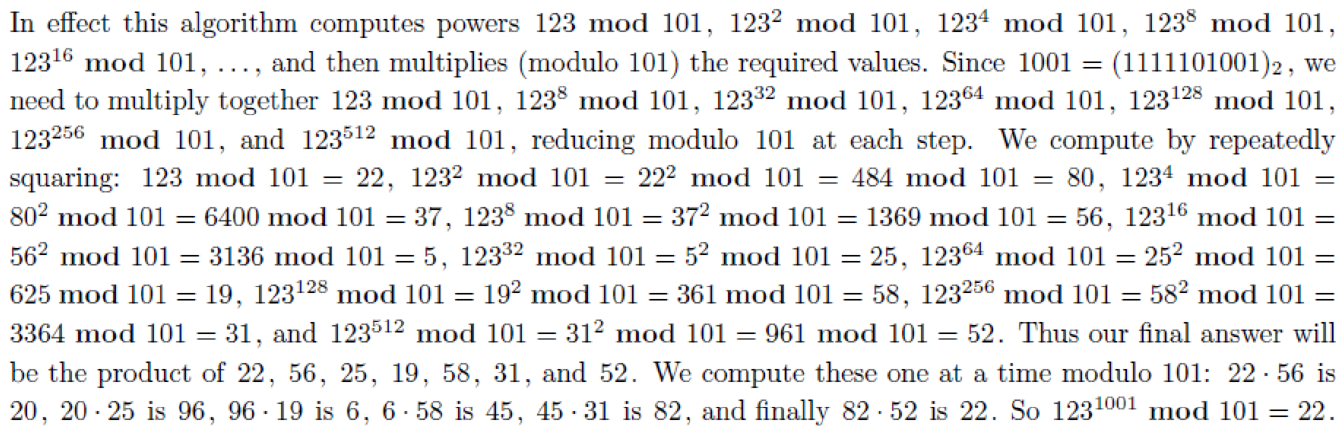
Section 4.2

24. (1pt)



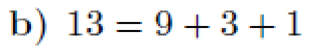
b) 20CBA + A01 = 21,6BB (decimal: 134,330 + 2561 = 136,891)
20CBA $\cdot$ A01 = 14,815,0BA (decimal: 134,330 $\cdot$ 2561 = 344,019,130)

28. (1pt)



In effect this algorithm computes powers $123 \textbf{ mod } 101$, $123^2 \textbf{ mod } 101$, $123^4 \textbf{ mod } 101$, $123^8 \textbf{ mod } 101$, $123^{16} \textbf{ mod } 101, \ldots,$ and then multiplies (modulo 101) the required values. Since $1001 = (1111101001)_2$, we need to multiply together $123 \textbf{ mod } 101$, $123^8 \textbf{ mod } 101$, $123^{32} \textbf{ mod } 101$, $123^{64} \textbf{ mod } 101$, $123^{128} \textbf{ mod } 101$, $123^{256} \textbf{ mod } 101$, and $123^{512} \textbf{ mod } 101$, reducing modulo 101 at each step. We compute by repeatedly squaring: $123 \textbf{ mod } 101 = 22$, $123^2 \textbf{ mod } 101 = 22^2 \textbf{ mod } 101 = 484 \textbf{ mod } 101 = 80$, $123^4 \textbf{ mod } 101 = 80^2 \textbf{ mod } 101 = 6400 \textbf{ mod } 101 = 37$, $123^8 \textbf{ mod } 101 = 37^2 \textbf{ mod } 101 = 1369 \textbf{ mod } 101 = 56$, $123^{16} \textbf{ mod } 101 = 56^2 \textbf{ mod } 101 = 3136 \textbf{ mod } 101 = 5$, $123^{32} \textbf{ mod } 101 = 5^2 \textbf{ mod } 101 = 25$, $123^{64} \textbf{ mod } 101 = 25^2 \textbf{ mod } 101 = 625 \textbf{ mod } 101 = 19$, $123^{128} \textbf{ mod } 101 = 19^2 \textbf{ mod } 101 = 361 \textbf{ mod } 101 = 58$, $123^{256} \textbf{ mod } 101 = 58^2 \textbf{ mod } 101 = 3364 \textbf{ mod } 101 = 31$, and $123^{512} \textbf{ mod } 101 = 31^2 \textbf{ mod } 101 = 961 \textbf{ mod } 101 = 52$. Thus our final answer will be the product of 22, 56, 25, 19, 58, 31, and 52. We compute these one at a time modulo 101: $22 \cdot 56$ is 20, $20 \cdot 25$ is 96, $96 \cdot 19$ is 6, $6 \cdot 58$ is 45, $45 \cdot 31$ is 82, and finally $82 \cdot 52$ is 22. So $123^{1001} \textbf{ mod } 101 = 22$.

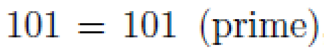
30. (1pt)



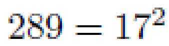
b) $13 = 9 + 3 + 1$

Section 4.3

4. (1pt each, 2pt total)

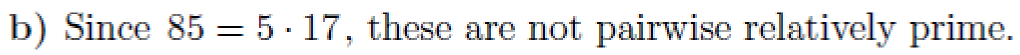
c) 

$101 = 101$ (prime)

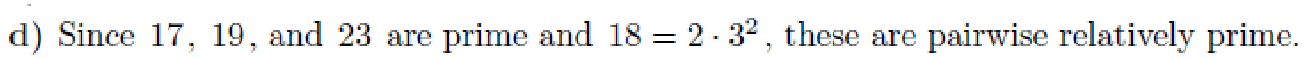
e) 

$289 = 17^2$

16. (1pt each, 2pt total)



b) Since $85 = 5 \cdot 17$, these are not pairwise relatively prime.



d) Since 17, 19, and 23 are prime and $18 = 2 \cdot 3^2$, these are pairwise relatively prime.

24. (0.5pt each, 2pt total)

c) 17 d) 1 e) 5 f) $2 \cdot 3 \cdot 5 \cdot 7$

26. (0.5pt each, 2pt total)

c) 17^{17} d) $2^2 \cdot 5^3 \cdot 7 \cdot 13$

e) undefined (0 is not a positive integer) f) $2 \cdot 3 \cdot 5 \cdot 7$

30. (1pt)

By Exercise 31 we know that the product of the greatest common divisor and the least common multiple of two numbers is the product of the two numbers. Therefore the answer is $(2^7 \cdot 3^8 \cdot 5^2 \cdot 7^{11})/(2^3 \cdot 3^4 \cdot 5) = 2^4 \cdot 3^4 \cdot 5 \cdot 7^{11}$.

32. (0.5pt each, 2pt total)

a) $\gcd(1,5) = \gcd(1,0) = 1$

b) $\gcd(100,101) = \gcd(100,1) = \gcd(1,0) = 1$

e) $\gcd(1529,14038) = \gcd(1529,277) = \gcd(277,144) = \gcd(144,133) = \gcd(133,11) = \gcd(11,1) = \gcd(1,0) = 1$

f) $\gcd(11111,111111) = \gcd(11111,1) = \gcd(1,0) = 1$

54. (1pt)

Suppose by way of contradiction that q_1, q_2, ..., q_n are the only primes of the form $3k+2$. Notice that this list necessarily includes 2. Let $Q = 3q_1q_2 \cdots q_n - 1$. Notice that neither 3 nor any prime of the form $3k+2$ is a factor of Q. But $Q \geq 3 \cdot 2 - 1 = 5 > 1$, so it must have prime factors. Therefore all of its prime factors are of the form $3k+1$. However, the product of numbers of the form $3k+1$ is again of that form, because $(3k+1)(3l+1) = 3(3kl+k+l)+1$. Patently Q is not of that form, and we have a contradiction, which completes the proof.