

CS/MA320:October 20: HW4 Solution:

Reading Assignments for the following Sections are in the Notes.

3.6 Exercises With Solutions: pg. 229: 1.a-c, 5.a-b, 23.a-c, 29

Exercises For You To Solve: pg. 229: 2.a-b, 8.a-c, 24.c-d, 29 Repeat with 9 instead of 3.

2.a Start with 321. $321 = 2 \times 160 + 1$; $160 = 2 \times 80 + 0$; $80 = 2 \times 40 + 0$; $40 = 2 \times 20 + 0$; $20 = 2 \times 10 + 0$; $10 = 2 \times 5 + 0$; $5 = 2 \times 2 + 1$; $2 = 2 \times 1 + 0$; $1 = 2 \times 0 + 1$. Reading remainders left to right we get the binary number 101000001. Check: $101000001 = 2^8 + 2^6 + 1 = 256 + 64 + 1 = 321$.

2.b We can carry out the same approach as in 2.a, or alternatively, we might notice that $1023 = 2^{10} - 1 = 1000000000 - 1 = 111111111$.

8.a $1111\ 0111 = F7$; The bits are separated in blocks of 4 and each block translates to a hex digit.

8.b $1010\ 1010\ 1010 = AAA$; **8.c** $111\ 0111\ 0111\ 0111 = 7777$; these are all blocks of 4 except the leftmost block of 3, which can be assumed to have a 0 in the leftmost bit of 4.

24.c Using the Euclidean Algorithm: $\gcd(123, 277) = \gcd(123, 31) = \gcd(31, 30) = \gcd(30, 1) = 1$.

24.d $\gcd(1529, 140390) = \gcd(1529, 278) = \gcd(278, 139) = \gcd(139, 0) = 139$.

29. Since $10 \equiv 1 \pmod{9}$, $10^k \equiv 1 \pmod{9}$, for all k , and any decimal representation for $a = a_{n-1}10^{n-1} + a_{n-2}10^{n-2} + \dots + a_110^1 + a_0$ allows us to take both sides mod 9 to get $a \pmod{9} = (a_{n-1} + a_{n-2} + \dots + a_1 + a_0) \pmod{9}$. This gives us the trick of "Casting out the 9's to check an addition".

3.7 Exercises With Solutions: pg. 244: 1.a-c, 5., 11, 27.a

Exercises For You To Solve: pg. 244: 2.a-b, 6, 12, 28.a

2.a To find the coefficients s and t such that $9s + 11t = \gcd(9, 11)$, we first carry out the steps of the Euclidean Algorithm. Dividing 11 by 9, $11 = 9 + 2$, so $\gcd(9, 11) = \gcd(2, 9)$. Now dividing 9 by 2, $9 = 4 \times 2 + 1$. Thus we end up with $\gcd(2, 1)$ which is 1. From the second (underlined) equation, we get (a) $1 = 9 - 4 \times 2$. From the first equation, we get (b) $2 = 11 - 9$. Now substitute the right-hand side of equation (b) for the 2 in equation (a), and get: $1 = 9 - 4(11 - 9) = 1 = 5 \times 9 + (-4) \times 11$, so in the terms we asked for, the coefficient $s = 5$ and the coefficient $t = -4$.

USEFUL ON EXAM. We can also note that 11 is a prime and thus the $\gcd(x, 11)$ for any x that is not a multiple of 11 will be 1. Also, when we find s and t such that $9s + 11t = 1 = \gcd(9, 11)$, we are finding s , the multiplicative inverse of 9 mod 11. E.g. $5 \times 9 = 1 \pmod{11}$ because $1 = 5 \times 9 + (-4) \times 11$. See also Exercises 6 and 12 below, and understand the reasoning.

2.b We take the same approach as above to represent $\gcd(33, 44)$ as a linear combination of 33 and 44. We start with $44 = 33 + 11$, and note that $\gcd(11, 33) = 11$. Since $44 = 33 + 11$, $11 = 44 - 33$, thus $1 \times 44 + (-1) \times 33 = \gcd(33, 44)$.

6. We need to find a number x such that $2x \pmod{17} = 1$. This can be done easily since $18 \pmod{17} = 1$, and thus $2 \times 9 \pmod{17} = 1$. If it were not this obvious, we could find coefficients s and t such that $2s + t17 = \gcd(2, 17) = 1$.

12. Solve the congruence $2x = 7 \pmod{17}$. From Exercise 6, we know that the inverse of 2 mod 17 is 9. Therefore if we multiply both sides of $2x = 7 \pmod{17}$ by 9, we get $x = 7 \times 9 \pmod{17} = 63 \pmod{17} = 12 \pmod{17}$. To check, note that $2 \times 12 \pmod{17} = 7 \pmod{17}$.

28.a Use Fermat's Little Theorem to compute $3^{302} \bmod 5$, $3^{302} \bmod 7$ and $3^{302} \bmod 11$. By Fermat's Little Theorem, we know that $3^4 = 1 \bmod 5$; therefore $3^{300} = (3^4)^{75} = 1 \bmod 5$. Thus, $3^{302} = 3^2 3^{300} = 9 \times 1 \bmod 5 = 4 \bmod 5$. Similarly, $3^6 = 1 \bmod 7$, so $3^{300} = (3^6)^{50} = 1 \bmod 7$, and we see $3^{302} \bmod 7 = 9 \bmod 7 = 2 \bmod 7$. Finally, $3^{10} = 1 \bmod 11$ so $3^{300} = 1 \bmod 11$ and $3^{302} = 9 \bmod 11$.