Solutions to Assignment 4

Section 4.2 Problems: 2,4,8,22

2. To convert from decimal to binary, we successively divide by 2. We write down the remainders so obtained from right to left; that is the binary representation of the given number.

a) Since 321/2 is 160 with a remainder of 1, the rightmost digit is 1. Then since 160/2 is 80 with a remainder of 0, the second digit from the right is 0. We continue in this manner, obtaining successive quotients of 40, 20, 10, 5, 2, 1, and 0, and remainders of 0, 0, 0, 0, 1, 0, and 1. Putting all these remainders in order from right to left we obtain $(1\ 0100\ 0001)_2$ as the binary representation. We could, as a check, expand this binary numeral: $2^0 + 2^6 + 2^8 = 1 + 64 + 256 = 321$.

b) We could carry out the same process as in part **(a)**. Alternatively, we might notice that $1023 = 1024 - 1 = 2^{10} - 1$. Therefore the binary representation is 1 less than $(100\ 0000\ 0000)_2$, which is clearly $(11\ 1111\ 1111)_2$.

c) If we carry out the divisions by 2, the quotients are 50316, 25158, 12579, 6289, 3144, 1572, 786, 393, 196, 98, 49, 24, 12, 6, 3, 1, and 0, with remainders of 0, 0, 0, 1, 1, 0, 0, 0, 1, 0, 0, 1, 0, 0, 0, 1, and 1. Putting the remainders in order from right to left we have $(1\ 1000\ 1001\ 0001\ 1000)_2$.

4. **a)** $1 + 2 + 8 + 16 = 27$ **b)** $1 + 4 + 16 + 32 + 128 + 512 = 693$

c) $2 + 4 + 8 + 16 + 32 + 128 + 256 + 512 = 958$

d) $1 + 2 + 4 + 8 + 16 + 1024 + 2048 + 4096 + 8192 + 16384 = 31775$

Section 4.3 Problems: 20,24,32 (c) and (e)

20. We need to find a factor if there is one, or else check all possible prime divisors up to the square root of the given number to verify that there is no nontrivial divisor.

a) $2^7 - 1 = 127$. Division by 2, 3, 5, 7, and 11 shows that these are not factors. Since $\sqrt{127} < 13$, we are done; 127 is prime.

b) $2^9 - 1 = 511 = 7 \cdot 73$, so this number is not prime.

c) $2^{11} - 1 = 2047 = 23 \cdot 89$, so this number is not prime.

d) $2^{13} - 1 = 8191$. Division by 2, 3, 5, 7, 11, 13, 17, 19, 23, 29, 31, 37, 41, 43, 47, 53, 59, 61, 67, 71, 73, 79, 83, and 89 (phew!) shows that these are not factors. Since $\sqrt{8191} < 97$, we are done; 8191 is prime.

24. We form the greatest common divisors by finding the minimum exponent for each prime factor.

a) $2^2 \cdot 3^3 \cdot 5^2$ **b)** $2 \cdot 3 \cdot 11$ **c)** 17 **d)** 1 **e)** 5 **f)** $2 \cdot 3 \cdot 5 \cdot 7$

\

32. To apply the Euclidean algorithm, we divide the larger number by the smaller, replace the larger by the smaller and the smaller by the remainder of this division, and repeat this process until the remainder is 0. At that point, the smaller number is the greatest common divisor.

a) $\gcd(1,5) = \gcd(1,0) = 1$ **b)** $\gcd(100,101) = \gcd(100,1) = \gcd(1,0) = 1$

c) $\gcd(123,277) = \gcd(123,31) = \gcd(31,30) = \gcd(30,1) = \gcd(1,0) = 1$

d) $\gcd(1529,14039) = \gcd(1529,278) = \gcd(278,139) = \gcd(139,0) = 139$

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

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

Section 4.4 Problems: 6 & 10

6. **a)** The first step of the procedure in Example 1 yields $17 = 8 \cdot 2 + 1$, which means that $17 - 8 \cdot 2 = 1$, so -8 is an inverse. We can also report this as 9, because $-8 \equiv 9 \pmod{17}$.

b) We need to find s and t such that $34s + 89t = 1$. Then s will be the desired inverse, since $34s \equiv 1 \pmod{89}$ (i.e., $34s - 1 = -89t$ is divisible by 89). To do so, we proceed as in Example 2. First we go through the Euclidean algorithm computation that $\gcd(34,89) = 1$:

$$\begin{aligned} 89 &= 2 \cdot 34 + 21 \\ 34 &= 21 + 13 \\ 21 &= 13 + 8 \\ 13 &= 8 + 5 \\ 8 &= 5 + 3 \\ 5 &= 3 + 2 \\ 3 &= 2 + 1 \end{aligned}$$

Then we reverse our steps and write 1 as the desired linear combination:

$$\begin{aligned} 1 &= 3 - 2 \\ &= 3 - (5 - 3) = 2 \cdot 3 - 5 \\ &= 2 \cdot (8 - 5) - 5 = 2 \cdot 8 - 3 \cdot 5 \\ &= 2 \cdot 8 - 3 \cdot (13 - 8) = 5 \cdot 8 - 3 \cdot 13 \\ &= 5 \cdot (21 - 13) - 3 \cdot 13 = 5 \cdot 21 - 8 \cdot 13 \\ &= 5 \cdot 21 - 8 \cdot (34 - 21) = 13 \cdot 21 - 8 \cdot 34 \\ &= 13 \cdot (89 - 2 \cdot 34) - 8 \cdot 34 = 13 \cdot 89 - 34 \cdot 34 \end{aligned}$$

Thus $s = -34$, so an inverse of 34 modulo 89 is -34, which can also be written as 55.

c) We need to find s and t such that $144s + 233t = 1$. Then clearly s will be the desired inverse, since $144s \equiv 1 \pmod{233}$ (i.e., $144s - 1 = -233t$ is divisible by 233). To do so, we proceed as in Example 2. In fact, once we get to a certain point below, all the work was already done in part **(b)**. First we go through the

Euclidean algorithm computation that $\gcd(144, 233) = 1$:

$$\begin{aligned}
233 &= 144 + 89 \\
144 &= 89 + 55 \\
89 &= 55 + 34 \\
55 &= 34 + 21 \\
34 &= 21 + 13 \\
21 &= 13 + 8 \\
13 &= 8 + 5 \\
8 &= 5 + 3 \\
5 &= 3 + 2 \\
3 &= 2 + 1
\end{aligned}$$

Then we reverse our steps and write 1 as the desired linear combination:

$$\begin{aligned}
1 &= 3 - 2 \\
&= 3 - (5 - 3) = 2 \cdot 3 - 5 \\
&= 2 \cdot (8 - 5) - 5 = 2 \cdot 8 - 3 \cdot 5 \\
&= 2 \cdot 8 - 3 \cdot (13 - 8) = 5 \cdot 8 - 3 \cdot 13 \\
&= 5 \cdot (21 - 13) - 3 \cdot 13 = 5 \cdot 21 - 8 \cdot 13 \\
&= 5 \cdot 21 - 8 \cdot (34 - 21) = 13 \cdot 21 - 8 \cdot 34 \\
&= 13 \cdot (55 - 34) - 8 \cdot 34 = 13 \cdot 55 - 21 \cdot 34 \\
&= 13 \cdot 55 - 21 \cdot (89 - 55) = 34 \cdot 55 - 21 \cdot 89 \\
&= 34 \cdot (144 - 89) - 21 \cdot 89 = 34 \cdot 144 - 55 \cdot 89 \\
&= 34 \cdot 144 - 55 \cdot (233 - 144) = 89 \cdot 144 - 55 \cdot 233
\end{aligned}$$

Thus $s = 89$, so an inverse of 144 modulo 233 is 89, since $144 \cdot 89 = 12816 \equiv 1 \pmod{233}$.

d) The first step in the Euclidean algorithm calculation is $1001 = 5 \cdot 200 + 1$. Thus $-5 \cdot 200 + 1001 = 1$, and -5 (or 996) is the desired inverse.

10. We know from Exercise 6 that 9 is an inverse of 2 modulo 17. Therefore if we multiply both sides of this equation by 9 we will get $x \equiv 9 \cdot 7 \pmod{17}$. Since $63 \textbf{ mod } 17 = 12$, the solutions are all integers congruent to 12 modulo 17, such as 12, 29, and -5. We can check, for example, that $2 \cdot 12 = 24 \equiv 7 \pmod{17}$. This answer can also be stated as all integers of the form $12 + 17k$ for $k \in \mathbf{Z}$.