University of Ottawa
School of Electrical Engineering and Computer Science
CSI 2101, Winter 2019

Assignment #3 Solution

42. We take $a = 356$ and $b = 252$ to avoid a needless first step. When we apply the Euclidean algorithm we obtain the following quotients and remainders: $q_1 = 1$, $r_2 = 104$, $q_2 = 2$, $r_3 = 44$, $q_3 = 2$, $r_4 = 16$, $q_4 = 2$, $r_5 = 12$, $q_5 = 1$, $r_6 = 4$, $q_6 = 3$. Note that $n = 6$. Thus we compute the successive s's and t's as follows, using the given recurrences:

$s_2 = s_0 - q_1 s_1 = 1 - 1 \cdot 0 = 1,$ $\quad t_2 = t_0 - q_1 t_1 = 0 - 1 \cdot 1 = -1$

$s_3 = s_1 - q_2 s_2 = 0 - 2 \cdot 1 = -2,$ $\quad t_3 = t_1 - q_2 t_2 = 1 - 2 \cdot (-1) = 3$

$s_4 = s_2 - q_3 s_3 = 1 - 2 \cdot (-2) = 5,$ $\quad t_4 = t_2 - q_3 t_3 = -1 - 2 \cdot 3 = -7$

$s_5 = s_3 - q_4 s_4 = -2 - 2 \cdot 5 = -12,$ $\quad t_5 = t_3 - q_4 t_4 = 3 - 2 \cdot (-7) = 17$

$s_6 = s_4 - q_5 s_5 = 5 - 1 \cdot (-12) = 17,$ $\quad t_6 = t_4 - q_5 t_5 = -7 - 1 \cdot 17 = -24$

Thus we have $s_6 a + t_6 b = 17 \cdot 356 + (-24) \cdot 252 = 4$, which is $\gcd(356, 252)$.

50. From $a \equiv b \pmod{m}$ we know that $b = a + sm$ for some integer s. Now if d is a common divisor of a and m, then it divides the right-hand side of this equation, so it also divides b. We can rewrite the equation as $a = b - sm$, and then by similar reasoning, we see that every common divisor of b and m is also a divisor of a. This shows that the set of common divisors of a and m is equal to the set of common divisors of b and m, so certainly $\gcd(a, m) = \gcd(b, m)$.

22. By definition, the first congruence can be written as $x = 6t + 3$ where t is an integer. Substituting this expression for x into the second congruence tells us that $6t + 3 \equiv 4 \pmod{7}$, which can easily be solved to show that $t \equiv 6 \pmod{7}$. From this we can write $t = 7u + 6$ for some integer u. Thus $x = 6t + 3 = 6(7u + 6) + 3 = 42u + 39$. Thus our answer is all numbers congruent to 39 modulo 42. We check our answer by confirming that $39 \equiv 3 \pmod{6}$ and $39 \equiv 4 \pmod{7}$.

26. First we find d, the inverse of $e = 17$ modulo $52 \cdot 60$. A computer algebra system tells us that $d = 2753$. Next we have the CAS compute $c^d \ \mathbf{mod}\ n$ for each of the four given numbers: $3185^{2753} \ \mathbf{mod}\ 3233 = 1816$ (which are the letters SQ), $2038^{2753} \ \mathbf{mod}\ 3233 = 2008$ (which are the letters UI), $2460^{2753} \ \mathbf{mod}\ 3233 = 1717$ (which are the letters RR), and $2550^{2753} \ \mathbf{mod}\ 3233 = 0411$ (which are the letters EL). The message is SQUIRREL.

26. One can get to the proof of this by doing some algebraic tinkering. It turns out to be easier to think about the given statement as $na^{n-1}(a - b) \geq a^n - b^n$. The basis step ($n = 1$) is the true statement that $a - b \geq a - b$. Assume the inductive hypothesis, that $ka^{k-1}(a-b) \geq a^k - b^k$; we must show that $(k+1)a^k(a-b) \geq a^{k+1} - b^{k+1}$. We have

$$\begin{aligned}(k+1)a^k(a-b) &= k \cdot a \cdot a^{k-1}(a-b) + a^k(a-b) \\ &\geq a(a^k - b^k) + a^k(a-b) \\ &= a^{k+1} - ab^k + a^{k+1} - ba^k .\end{aligned}$$

To complete the proof we want to show that $a^{k+1} - ab^k + a^{k+1} - ba^k \geq a^{k+1} - b^{k+1}$. This inequality is equivalent to $a^{k+1} - ab^k - ba^k + b^{k+1} \geq 0$, which factors into $(a^k - b^k)(a - b) \geq 0$, and this is true, because we are given that $a > b$.

38. In Exercise 46 of Section 1.8, we found a closed path that snakes its way around an 8×8 checkerboard to cover all the squares, and using that we were able to prove that when one black and one white square are removed, the remaining board can be covered with dominoes. The same reasoning works for any size board, so it suffices to show that any board with an even number of squares has such a snaking path. Note that a board with an even number of squares must have either an even number of rows or an even number of columns, so without loss of generality, assume that it has an even number of rows, say $2n$ rows and m columns. Number the squares in the usual manner, so that the first row contains squares 1 to m from left to right, the second row contains squares $m+1$ to $2m$ from left to right, and so on, with the final row containing squares $(2n-1)m+1$ to $2nm$ from left to right.

We will prove the stronger statement that any such board contains a path that includes the top row traversed from left to right. The basis step is $n=1$, and in that case the path is simply $1,\ 2,\ \ldots,\ m,\ 2m,\ 2m-1,\ \ldots,\ m+1,\ 1$. Assume the inductive hypothesis and consider a board with $2n+2$ rows. By the inductive hypothesis, the board obtained by deleting the top two rows has a closed path that includes its top

row from left to right (i.e., $2m+1,\ 2m+2,\ \ldots,\ 3m$). Replace this subsequence by $2m+1,\ m+1,\ 1,\ 2,\ \ldots,\ m,\ 2m,\ 2m-1,\ \ldots,\ m+2,\ 2m+2,\ \ldots,\ 3m$, and we have the desired path.

32. **a)** $ones(\lambda)=0$ and $ones(wx)=x+ones(w)$, where w is a bit string and x is a bit (viewed as an integer when being added)

b) The basis step is when $t=\lambda$, in which case we have $ones(s\lambda)=ones(s)=ones(s)+0=ones(s)+ones(\lambda)$. For the inductive step, write $t=wx$, where w is a bit string and x is a bit. Then we have $ones(s(wx))=ones((sw)x)=x+ones(sw)$ by the recursive definition, which is $x+ones(s)+ones(w)$ by the inductive hypothesis, which is $ones(s)+(x+ones(w))$ by commutativity and associativity of addition, which finally equals $ones(s)+ones(wx)$ by the recursive definition.

14. This is actually quite subtle. The recursive algorithm will need to keep track not only of what the mode actually is, but also of how often the mode appears. We will describe this algorithm in words, rather than in pseudocode. The input is a list $a_1,a_2,\ldots,a_n$ of integers. Call this list L. If $n=1$ (the base case), then the output is that the mode is a_1 and it appears 1 time. For the recursive case ($n>1$), form a new list L' by deleting from L the term a_n and all terms in L equal to a_n. Let k be the number of terms deleted. If $k=n$ (in other words, if L' is the empty list), then the output is that the mode is a_n and it appears n times. Otherwise, apply the algorithm recursively to L', obtaining a mode m, which appears t times. Now if $t\ge k$, then the output is that the mode is m and it appears t times; otherwise the output is that the mode is a_n and it appears k times.

12. This is identical to Exercise 11, one level deeper.

a) Let a_n be the number of ways to climb n stairs. In order to climb n stairs, a person must either start with a step of one stair and then climb $n-1$ stairs (and this can be done in a_{n-1} ways) or else start with a step of two stairs and then climb $n-2$ stairs (and this can be done in a_{n-2} ways) or else start with a step of three stairs and then climb $n-3$ stairs (and this can be done in a_{n-3} ways). From this analysis we can immediately write down the recurrence relation, valid for all $n\ge 3$: $a_n=a_{n-1}+a_{n-2}+a_{n-3}$.

b) The initial conditions are $a_0=1$, $a_1=1$, and $a_2=2$, since there is one way to climb no stairs (do nothing), clearly only one way to climb one stair, and two ways to climb two stairs (one step twice or two steps at once). Note that the recurrence relation is the same as that for Exercise 9.

c) Each term in our sequence $\{a_n\}$ is the sum of the previous three terms, so the sequence begins $a_0=1$, $a_1=1$, $a_2=2$, $a_3=4$, $a_4=7$, $a_5=13$, $a_6=24$, $a_7=44$, $a_8=81$. Thus a person can climb a flight of 8 stairs in 81 ways under the restrictions in this problem.

30. **a)** The associated homogeneous recurrence relation is $a_n = -5a_{n-1} - 6a_{n-2}$. To solve it we find the characteristic equation $r^2 + 5r + 6 = 0$, find that $r = -2$ and $r = -3$ are its solutions, and therefore obtain the homogeneous solution $a_n^{(h)} = \alpha(-2)^n + \beta(-3)^n$. Next we need a particular solution to the given recurrence relation. By Theorem 6 we want to look for a function of the form $a_n = c \cdot 4^n$. We plug this into our recurrence relation and obtain $c \cdot 4^n = -5c \cdot 4^{n-1} - 6c \cdot 4^{n-2} + 42 \cdot 4^n$. We divide through by 4^{n-2}, obtaining $16c = -20c - 6c + 42 \cdot 16$, whence with a little simple algebra $c = 16$. Therefore the particular solution we seek is $a_n^{(p)} = 16 \cdot 4^n = 4^{n+2}$. So the general solution is the sum of the homogeneous solution and this particular solution, namely $a_n = \alpha(-2)^n + \beta(-3)^n + 4^{n+2}$.

b) We plug the initial conditions into our solution from part **(a)** to obtain $56 = a_1 = -2\alpha - 3\beta + 64$ and $278 = a_2 = 4\alpha + 9\beta + 256$. A little algebra yields $\alpha = 1$ and $\beta = 2$. So the solution is $a_n = (-2)^n + 2(-3)^n + 4^{n+2}$.