MA014G
Algebra and Discrete Mathematics
Suggested Solutions to Assignment 3

Question 1

(a) The definition of $d|m$ is that $m = qd$ for some integer q.

(b) The existence of the two integers q_1 and q_2 that satisfy $(*)$ is given directly by the definition in (a).

(c) $sm + tn = s(dq_1) + t(dq_2)$ because $m = dq_1$ and $n = dq_2$ by $(*)$.

$$\begin{aligned} s(dq_1) &+ t(dq_2) \\ &= s(q_1 d) + t(q_2 d) && \text{by the commutative law for multiplication} \\ &= (sq_1)d + (tq_2)d && \text{by the associative law for multiplication} \\ &= (sq_1 + tq_2)d && \text{by the distributive law} \\ &= d(sq_1 + tq_2) && \text{by the commutative law for multiplication.} \end{aligned}$$

(d) s, q_1, t, q_2 are all integers. Multiplying and adding integers yield an integer result, so thus $sq_1 + tq_2$ is an integer.

(e) By (d) $k = sq_1 + tq_2$ is an integer. The calculation $(**)$ shows that $sm + tn = dk$. It thus follows directly from the defintion in (a) that $d|(sm + tn)$.

Question 2

If $3|(2^{n-1} - 1)$ for some integer $n \geq 1$ then $2^{n-1} - 1 = 3k$ for some integer k, and thus

$$2^{n-1} = 3k + 1.$$

From this we get that

$$2^{n+1} - 1 = 4 \cdot 2^{n-1} - 1 = 4(3k + 1) - 1 = 12k + 3 = 3(4k + 1).$$

This shows that $3|(2^{n+1} - 1)$, because k is an integer, so $4k+1$ is also an integer.

Question 3

(a) Using Euclid's algorithm:

$$\begin{aligned} \mathbf{3571} &= 2 \cdot \mathbf{1753} + \mathbf{65}; \\ \mathbf{1753} &= 26 \cdot \mathbf{65} + \mathbf{63}; \\ \mathbf{65} &= 1 \cdot \mathbf{63} + \mathbf{2}; \\ \mathbf{63} &= 31 \cdot \mathbf{2} + \mathbf{1}; \\ \mathbf{2} &= 2 \cdot \mathbf{1} + 0. \end{aligned}$$

Hence $\gcd(3571, 1753) = 1$ because the last non-zero remainder is 1.

(b) Using Euclid's algorithm backwards we get

$$\begin{aligned} \mathbf{1} &= \mathbf{63} - 31 \cdot \mathbf{2} \\ &= \mathbf{63} - 31[\mathbf{65} - \mathbf{63}] = 32 \cdot \mathbf{63} - 31 \cdot \mathbf{65} \\ &= 32 \cdot [\mathbf{1753} - 26 \cdot \mathbf{65}] - 31 \cdot \mathbf{65} = (-863) \cdot \mathbf{65} + 32 \cdot \mathbf{1753} \\ &= (-863) \cdot [\mathbf{3571} - 2 \cdot \mathbf{1753}] + 32 \cdot \mathbf{1753} = (-863) \cdot \mathbf{3571} + 1758 \cdot \mathbf{1753}. \end{aligned}$$

So

$$1 = (-863) \cdot \mathbf{3571} + 1758 \cdot \mathbf{1753},$$

from which you get an answer to (c). Now, to find a solution to (b), add the two equations

$$\begin{aligned} 1 &= (-863) \cdot \mathbf{3571} + 1758 \cdot \mathbf{1753}, \\ 0 &= 1753 \cdot \mathbf{3571} + (-3571) \cdot \mathbf{1753} \end{aligned}$$

to get that

$$1 = 890 \cdot \mathbf{3571} + (-1813) \cdot \mathbf{1753}.$$

(c) Cf. (b).

Question 4

First estimate how many devisions you have to make:

$$22374 < 22500 = 150^2,$$

this means that if you have not found a prime factor when trying with all primes up to 149, then 22374 is prime, so in the worst case we have to check with all positive primes up to 149.
Starting with 2 and 3 we find

$$22374 = 2 \cdot 3^2 \cdot 1243.$$

Now, $1243 < 40^2$, this means that if you have not found a prime factor when trying with all primes up to 39, then 1243 is prime, so in the worst case we

now have to check with all positive primes up to 39, which reduces our problem.

2 clearly does not divide it, and neither do 3, 5, 7, but 11 does divide 1243 and we thus find

$$22374 = 2 \cdot 3^2 \cdot 11 \cdot 113.$$

Now, $113 < 11^2$, so you only need to check divisibility with primes up to 10 in order to test whether it is prime. This has already been done (we have tested up to 11 already), and none of them divide, so 113 is prime. Hence

$$22374 = 1 \cdot 2 \cdot 3^2 \cdot 11 \cdot 113.$$

is the required factorisation into one unit and positive primes.