Solutions to MATH3411 Problems 1–9

1.

a) Since n is not a prime, we can write $n = km$ where $k, m > 1$ are integers. Suppose that $k, m > \sqrt{n}$; then $n = km > (\sqrt{n})^2 = n$, a contradiction. We see that either $k \leq \sqrt{n}$ or $m \leq \sqrt{n}$; in particular, one of these integers - and thus n - then has a proper factor less than or equal to $\sqrt{n}$.

b) Assume that n is not a prime. By part a), n has a prime factor less than or equal to 20. The prime factors of 51051 are 3, 7, 11, 13, and 17, so if $\gcd(n, 51051) = 1$, then none of these prime factors divide n. If n furthermore does not have 2 or 5 as a prime factor, then this just leaves 19 as n's only prime factor, so n is a power of 19, namely 19, $19^2 = 361$, 19^3, or greater. However, $18 \leq n \leq 400$ and $n \geq 361$, so none of these are possible.

   We conclude that n must be a prime.

c) We just have to check whether any of the numbers 2, 3, 5, 7, 11, 13, 17 divide $n = 323$ and $n = 373$, respectively. We find that none divide 373 (so it is prime) but that $323 = 17 \times 19$.

2. (Extended result, proving that if $a^n - 1$ is prime, then $a = 2$ and n is prime.)
Suppose that $a^n - 1$ is prime and write $n = pq$ where p is a prime factor of n. Now,

$$\begin{array}{rcccccccccl} a^{pq} - 1 & = & a^{pq} & + & a^{(p-1)q} & + & \cdots & + & a^q & & \\ & & & - & a^{(p-1)q} & - & \cdots & - & a^q & - & 1 \; = \; (a^q - 1)(a^{(p-1)q} + \cdots + a^q + 1) \end{array}$$

Since $a^n - 1 = a^{pq} - 1$ is prime, one of the two terms above must be 1. Since $a^{(p-1)q} + \cdots + a^q + 1 > 1$, we have $a^q - 1 = 1$. Therefore, $a^q = 2$, so $a = 2$ and $q = 1$, and $n = p$ is prime.
Suppose that $2^n + 1$ is prime and write $n = rt$ where $r, t > 1$ are positive integers.
Assume that n is not a power of 2; then r or s is odd, say s. Now, for any positive integer a,

$$\begin{array}{rcccccccccccl} a^s + 1 & = & a^s & - & a^{s-1} & + & a^{s-1} & \cdots & - & a^2 & + & a & \\ & & & + & a^{s-1} & - & a^{s-1} & \cdots & + & a^2 & - & a & + \; 1 \; = \; (a+1)(a^{s-1} - a^{s-2} + \cdots - a + 1) \end{array}$$

Therefore, $a + 1 \mid a^s + 1$. Set $a = 2^r$; we then see that $2^r + 1$ divides $(2^r)^s + 1 = 2^n + 1$. But $r < n$, so $2^r + 1$ cannot equal $2^n + 1$ and is therefore a factor of $2^n + 1$, which means that $2^n + 1$ is not prime, a contradiction.
We conclude that n is a power of 2.

3. a) $\frac{1}{13}$

b) $\frac{1}{3}$

c) $\frac{1}{13}$

d) "Pick a Queen" and "pick a face card" are both independent of "pick a black card" but are not independent of each other.

4. (It is perhaps easiest for understanding to draw a tree diagram here but I'll be lazy.)

$$P(0 \text{ received}|0 \text{ sent}) = 1 - P(1 \text{ received}|0 \text{ sent}) = 1 - 0.1 = 0.9$$

so

$$\begin{aligned}
P(0\,\text{received}) &= P(0 \text{ received and } 0 \text{ sent}) + P(0 \text{ received and } 1 \text{ sent}) \\
&= P(0 \text{ received}|0 \text{ sent})P(0 \text{ sent}) + P(0 \text{ received}|1 \text{ sent})P(1 \text{ sent}) \\
&= 0.9 \times 0.5 + 0.2 \times 0.5 \qquad (\text{since } P(0 \text{ sent}) = P(1 \text{ sent}) = \tfrac{1}{2}) \\
&= 0.55
\end{aligned}$$

Now, $P(0 \text{ received and } 0 \text{ sent}) = P(0 \text{ received}|0 \text{ sent})P(0 \text{ sent})$, so

$$P(0 \text{ received}|0 \text{ sent}) = \frac{P(0 \text{ received and } 0 \text{ sent})}{P(0 \text{ sent})} = \frac{P(0 \text{ received}|0 \text{ sent})P(0 \text{ sent})}{P(0 \text{ sent})} = \frac{0.9 \times 0.5}{0.55} \approx 0.82$$

5. Call the door the contestant chooses Door 1 and the door opened by host Door 2. Let W_i be the event "major prize behind door i", and H_i be "host opens door i". We know that $P(W_i) = \frac{1}{3}$ for each i and that

$$P(H_2 \mid W_2) = 0 \qquad P(H_2 \mid W_3) = 1 \qquad P(H_2 \mid W_1) = 0.5\,.$$

We want to find $P(W_3 \mid H_2)$. Now

$$P(H_2) = P(H_2 \mid W_1)P(W_1) + P(H_2 \mid W_2)P(W_2) + P(H_2 \mid W_3)P(W_3) = \frac{1}{2} \times \frac{1}{3} + 0 \times \frac{1}{3} + 1 \times \frac{1}{3} = \frac{1}{2}$$

so (by Bayes' rule)

$$P(W_3 \mid H_2) = \frac{P(H_2 \mid W_3)P(W_3)}{P(H_2)} = \frac{1/3}{1/2} = \frac{2}{3}$$

Given that

$$P(W_1 \mid H_2) = 1 - P(W_2 \mid H_2) - P(W_3 \mid H_2) = 1 - 0 - \frac{2}{3} = \frac{1}{3}\,,$$

we see that the prize is twice as likely to be behind the third door: so swap.

6. a) $\binom{n}{k} p^k (1-p)^{n-k}$

b) $\displaystyle\sum_{j=0}^{\lfloor \frac{n}{2} \rfloor} \binom{n}{2j} p^{2j}(1-p)^{n-2j}$

c) Setting $q = 1-p$ and using the Binomial Theorem,

$$\begin{aligned}
\frac{1+(1-2p)^n}{2} &= \frac{(q+p)^n + (q-p)^n}{2} \\
&= \frac{1}{2}\Big(\sum_{k=0}^{n} \binom{n}{k} p^k q^{n-k} + \sum_{k=0}^{n} \binom{n}{k} (-p)^k q^{n-k}\Big) \\
&= \frac{1}{2}\Big(\sum_{j=0}^{\lfloor \frac{n}{2} \rfloor} \binom{n}{2j} (p^{2j} + p^{2j}) q^{n-2j} + \sum_{j=0}^{\lfloor \frac{n-1}{2} \rfloor} \binom{n}{2j+1} (p^{2j+1} - p^{2j+1}) q^{n-2j+1}\Big) \\
&= \frac{1}{2}\sum_{j=0}^{\lfloor \frac{n}{2} \rfloor} \binom{n}{2j} 2p^{2j} q^{n-2j} + 0 \\
&= \sum_{j=0}^{\lfloor \frac{n}{2} \rfloor} \binom{n}{2j} p^{2j} q^{n-2j} \\
&= \sum_{j=0}^{\lfloor \frac{n}{2} \rfloor} \binom{n}{2j} p^{2j} (1-p)^{n-2j}
\end{aligned}$$

We recognise this as the sum in part b).

7. a) $(1-p)^n = .999^{100} \approx 0.9048$

b) By parts b) and c) in Problem **6**, we see that the probability of an undetected error (i.e., the probability of an even, non-zero number of errors) is

$$\frac{1+(1-2p)^n}{2} - (1-p)^n = 0.9092834024 - 0.9047921471 = 0.0044912553 \approx 0.0045$$

8. $(1 \times 0 + 2 \times 5 + 3 \times 5 + 4 \times 2 + 5 \times 0 + 6 \times 8 + 7 \times 6 + 8 \times 3 + 9 \times 8) \mod 11 = (219 \mod 11) = 10$

so the first number is a valid ISBN. In contrast,

$$(1 \times 0 + 2 \times 5 + 3 \times 7 + 4 \times 6 + 5 \times 0 + 6 \times 8 + 7 \times 3 + 8 \times 1 + 9 \times 4) \mod 11 = (168 \mod 11) = 0$$

so the second number is not an ISBN; the correct check digit would have been 0.

9. a) Since $0 \equiv \sum_{i=1}^{10} ix_i \equiv \sum_{i=1}^{9} ix_i + 10x_{10} \equiv \sum_{i=1}^{9} ix_i - x_{10} \pmod{11}$, we see that x_{10} is given by $x_1, \ldots, x_9$:

$$x_{10} = \sum_{i=1}^{9} ix_i \mod 11$$

(If $x_{10} = 10$, then the word is not a valid codeword, so we don't count it.)
Adding the two congruences gives the congruence

$$\sum_{i=1}^{10}(i+1)x_i \equiv 0 \pmod{11} \qquad \text{or, since } 11 \equiv 0 \pmod{11}\,, \qquad \sum_{i=1}^{9}(i+1)x_i \equiv 0 \pmod{11}\,.$$

As with x_{10}, we see that $2x_1$ and thus x_1 depends on $x_2, \ldots, x_9$; in particular,

$$2x_1 \equiv -\sum_{i=2}^{9}(i+1)x_i \pmod{11}$$

so, since $2^{-1} = 6$ and $-6 = 5$ in $\mathbb{Z}_{11}$,

$$x_1 \equiv 5\sum_{i=2}^{9}(i+1)x_i \mod 11\,.$$

We can choose the 8 digits $x_2, \ldots, x_9$ (almost) freely, apart from the estimated $\frac{1}{11} \approx 0.9$ of the time when the congruences will not be satisfied, but then x_1 and x_{10} are fixed. Therefore, a rough estimation for $|\mathcal{C}|$ is 10^8. A slightly better one might be 9×10^7.

b) Suppose that $\mathbf{x} = x_1 \cdots x_{10} \in \mathcal{C}$ is sent and that $\mathbf{y} = y_1 \cdots y_{10}$ is received.
Now assume that exactly 1 error has occured, changing x_k to $y_k = x_k + m$ for some k and m.

Then since $\mathbf{x} \in \mathcal{C}$, $0 \equiv \sum_{i=1}^{10} x_i \equiv \sum_{i=1}^{10} y_i - m \pmod{11}$, we see that $m = \sum_{i=1}^{10} y_i \mod 11$.

Similarly, $0 \equiv \sum_{i=1}^{10} ix_i \equiv \sum_{i=1}^{10} iy_i - km \pmod{11}$, so $km \equiv \sum_{i=1}^{10} iy_i \pmod{11}$.

Since 11 is prime, we can thus determine $k = m^{-1}\sum_{i=1}^{10} iy_i \mod 11$.

We now know which digit (k) is incorrect and by how much it is incorrect (m), so we can correct it.

To show that the code can also detect the error caused by a swapping two digits, just re-use the course notes/slides proof of this property for ISBN.

c) Use part b): $m = \sum_{i=1}^{10} y_i \mod 11 = (0+6+8+0+2+7+1+3+8+5) \mod 11 = 7$.
The inverse of 7 in $\mathbb{Z}_{11}$ is 8, so

$$\begin{aligned} k &= m^{-1}\sum_{i=1}^{10} iy_i \mod 11 = 8\sum_{i=1}^{10} iy_i \mod 11 \\ &= 8(1\times 0 + 2\times 6 + 3\times 8 + 4\times 0 + 5\times 2 + 6\times 7 + 7\times 1 + 8\times 3 + 9\times 8 + 10\times 5) \mod 11 \\ &= 3 \end{aligned}$$

In other words, the 3rd digit is wrong and is 7 too big, modulo 11: it should be $8 - 7 = 1$ (in $\mathbb{Z}_{11}$).
The corrected number is then 0610271385.