Solutions to HW #2

2.2:#3 \( \left( \binom{6}{3} + \binom{6}{4} \right) / 2^6 = 22/64 \).

2.2:#14 Drawing this region in the plane it is half of the unit square, so 1/2. For the product \( xy > 1/2 \) we do a double integral to find the area

\[
\int_{1/2}^{1} \int_{1/2x}^{1} dy dx = \int_{1/2}^{1} (1 - 1/2x) dx = (1 - \log(2)) / 2.
\]

2.3: #1 \( (1 - 0.1167)^{10} = 29\% \), \( (1 - 0.1167)^{100} = 4 \times 10^{-6} \).

4.1: #6: Because it is the same as a single Vignere encryption of the same length: just shift the first key by the second key.

#9: For the slice which are the odd numbered characters, “B” is most common, so guess a key of “X”. For the slice which are the even numbered character, “C” is most common, so guess a key of “Y”. The key “XY” decrypts to

REALLY MEET ME AFTER MIDNIGHT IN THE ALLEY
BEFORE YOU GO HOME FROM WORN AND DON’T TELL ANYONE

4.4: #4: Let \( p = 1/2 \). Then we have H repeated k times and then a T with probability \( p^k(1 - p) \), so the expected number of H’s is

\[
\sum_{k=0}^{\infty} kp^k(1 - p) = p/(1 - p)
\]

which is 1 for \( p = 1/2 \).

#9: Solution #1: Let’s take a fair coin. We could have

\[
HH(2 \text{flips}, \text{prob} = 1/4)
\]

\[
THH(3 \text{flips}, \text{prob} = 1/8)
\]

\[
TTTHH
\]

\[
HTTHH(4 \text{flips}, \text{each prob} = 1/16)
\]

\[
TTHHH
\]

\[
THTTH(5 \text{flips}, \text{each prob} = 1/32)
\]

Let \( a_n \) be the number of words of length \( n \) in H and T, with no HH until the last two letters. The expected number of flips before the HH is

\[
E = \sum_{n \geq 2} (n - 2) * a_n (1/2)^n.
\]
Note that since the 3rd to last letter must be a T, \( a_n \) is also equal (***) to the number of words of length \( n - 3 \) without an HH.

\[
a_2 = 1, \quad a_3 = 1, \quad a_4 = 2, \quad a_5 = 3, \quad a_6 = 5, \ldots
\]

Note that (***) says that \( a_n = a_{n-1} + a_{n-2} \): if the last letter is a T, the previous \( n - 4 \) letters can be any word without an HH. If the last letter is an H, the next to last letter must be a T, and the previous \( n - 5 \) letters can be any word without an HH.

This is the recurrence of the Fibonacci numbers, and \( a_n = F_{n-2} \). The Fibonacci numbers satisfy

\[
\sum_{n \geq 0} F_n x^n = 1/(1 - x - x^2).
\]

So taking the derivative with respect to \( x \) gives

\[
\sum_{n \geq 0} n \cdot F_n x^{n-1} = d/dx(1/(1 - x - x^2)) = (1 + 2x)/(1 - x - x^2).
\]

So \( E = 2 \cdot (1/2)/(1 - 1/2 - 1/4) = 4 \) flips before the HH, 6 flips including the HH.

Solution #2: Let \( E \) be the expected number of flips including the HH. If the first flip is a T, with probability 1/2 we’ll need on the average \( E + 1 \) total flips. This occurs with prob 1/2. If the first flip is an H, either the second flip is a T, and we need \( (E + 2) \) flips with prob 1/4, or the second flip is another H, HH, and we stop with 2 flips with prob 1/4. Thus \( E = (E + 1)/2 + (E + 2)/4 + 2/4 \), whose solution is \( E = 6 \) total flips including the HH.

10.1: #1: Let \( x = 6k + 2 \), so we have \( 6k + 2 \equiv 3 \pmod{4} \), which is \( 2k \equiv 1 \pmod{4} \). But this has no solution since the left is always even while the right side is always odd.

10.2 #1 By the CRT, the solution set is \( x \equiv 1 \pmod{(12 \cdot 35)} \).

#7: Since 35 and 48 are relatively prime, we can use the CRT to find the solution modulo 35 \( \cdot 48 \). Let \( x = 48A + 5 \) and reduce modulo 35 to get \( 3 \equiv 13A + 5 \pmod{35} \) so \( 13A \equiv -2 \pmod{35} \). The inverse of 13 \pmod{35} is 27, so \( A \equiv -54 \equiv 16 \pmod{35} \). So \( x \equiv 773 \pmod{(35 \cdot 48)} \).

10.3 #1: The inverse of 3 \pmod{5} is 2 so multiplying by 2 we get \( x \equiv 4 \pmod{5} \) and also multiplying the second equation by 2 gives \( x \equiv 3 \pmod{7} \). The CRT solution is \( x \equiv 24 \pmod{35} \).

10.3 #3: \( x^2 \equiv 1 \pmod{5} \) has solutions \( x \equiv \pm 1 \pmod{5} \) and \( x^2 \equiv 1 \pmod{7} \) has solutions \( x \equiv \pm 1 \pmod{7} \). So we apply the CRT four times for these four cases. The solutions are \( x \equiv 1, 6, 29, 34 \pmod{35} \).
E1: (a) $\varphi(80)/80 = (1 - 1/2)(1 - 1/5) = 0.4$. (b) $\sum_{k=1}^{80} [80/k]/80^2 = 368/80^2$.

E2: $10 \times 9 \times 8 \times 7 / 10^4 = 50.4\%$. Note that the breakeven value $\sqrt{2 \log(2) \times 10} = 3.7$, even though $N = 10$ is not large!

E3: The dot products of the probabilities of the letters for the slices which are 1 mod $L$ are for $L = 1$ to $L = 27$ are

$\{0.0471012, 0.0473481, 0.0577778, 0.0534889, 0.054321, 0.0599111, 0.0575148, 0.0630963, 0.0928, 0.0607407, 0.0648424, 0.0595568, 0.0759184, 0.0707071, 0.0866667, 0.0796671, 0.0727023, 0.1296, 0.0729167, 0.0812854, 0.0867769, 0.0657596, 0.075, 0.0637119, 0.104938, 0.0925926, 0.121107\}$

So it looks like the key length might be 9.

Computing the dot products of the slice which is 1 modulo 9 against shifts of the English probabilities we get

$\{0.0335977, 0.0504419, 0.0391233, 0.0258767, 0.0318837, 0.0772326, 0.0403186, 0.0312837, 0.0304907, 0.0441907, 0.0247116, 0.0424419, 0.0436907, 0.0318, 0.0323977, 0.0401977, 0.047, 0.0397721, 0.0449535, 0.0365558, 0.0399047, 0.038886, 0.0313535, 0.0329233, 0.0383349, 0.0344372\}$

So the first letter of the key is F. Continuing we find a key of FUNNYJOKE and th eplainext of

AMATHEMATICIANABIOLIGISTANDAPHYSICISTARESITTING
INASTREETCAFEWATCHINGPEOPLEGOINGINANDCOMINGOUTOFTHEHOUSE
ONTHEOTHERSIDEOFTHESTREETFIRSTTHEYSEETWOPEOPLEGOING
INTOTHEHOUSETIMEPASSESAFTERAWHILETHEYNOTICETHREEPERSONS
COMINGOUTOFTHEHOUSETHEPHYSICISTSAYSTHEMEASUREMENTWASN
ACCURATETHEBIOLOGISTSAITHEYHAVORPREPRODUCEDTHEMATHEMATICIAN
SAIDIFEXACTLYONEPERSONENTERSTHEHOUSETHENITWILLBEEMPTYAGAIN

E4: (a) $p = (0.5, 0.2, 0.2, 0.1)$, $p.p = 0.34$.

(b) The dot products of $p$ with cyclic shifts of $p$ are 0.21, 0.24, 0.21.

(c) The probability vector for odd letters is (0.2, 0.2, 0.4, 0.2), so probably the shift is two to go from 50% A to 40% C. The probability vector for even letters is (0.2, 0.1, 0.0, 0.7), so probably the shift is three to go from 50% A to 70% D. Key = CD. The original plaintext message is AA CB AB DA AC BA AA BA CA DA.