1. Show $7 \div 2222^{5555} + 5555^{2222}$.

Solution. Below is the slickest solution that I’ve been able to come up with and it starts off by using Fermat’s Little Theorem, but there are countless ways of doing this problem. By Fermat’s Little Theorem, with $p = 7$ we have:

If $n$ is a natural number and $n \not\equiv 0 \pmod{7}$ then $n^6 \equiv 1 \pmod{7}$.

So for natural numbers $n$, $q$ and $r$, if $n \not\equiv 0 \pmod{7}$ then

$$n^{6q+r} \equiv (n^6)^q \cdot n^r \pmod{7}$$

$$\equiv 1^q \cdot n^r \pmod{7}$$

$$\equiv n^r \pmod{7}.$$

In other words, if $n \not\equiv 0 \pmod{7}$ then we can reduce the power of $n$ modulo 6. We use this twice in the second line of our reduction below.

$$2222^{5555} + 5555^{2222} \equiv 3^{5555} + (-3)^{2222} \pmod{7}$$

$$\equiv 3^5 + (-3)^2 \pmod{7} \quad \text{since } \pm 3 \not\equiv 0 \pmod{7}$$

$$\equiv 3^2(3^3 + 1) \pmod{7}$$

$$\equiv 3^2 \cdot 28 \pmod{7}$$

$$\equiv 0 \pmod{7}.$$

Hence $7 \div 2222^{5555} + 5555^{2222}$.

Alternatively, one can show directly that

$$2222^6 \equiv 3^6 \equiv (3^2)^3 \equiv 2^3 \equiv 1 \pmod{7}$$

$$5555^3 \equiv 2^3 \equiv 1 \pmod{7}$$

and go from there.
2. For which \( a \) does the congruence \( ax \equiv 1 \pmod{m} \) have a solution, when . . .

(i) \( m = 4 \)?
(ii) \( m = 5 \)?
(iii) \( m = 6 \)?
(iv) \( m = 7 \)?

**Solution.** The congruence \( ax \equiv 1 \pmod{m} \) is equivalent to saying that 
\[
ax + my = 1 \tag{1}
\]
for some integer \( y \). In Problem 2 of the Number Theory II Problem Sheet, we showed that if such a condition was satisfied then \( a, m \) are coprime. Conversely, the Euclidean Algorithm guarantees a solution of (1). Thus, in each case the problem is equivalent to finding integers \( a \) that are coprime with \( m \). Note that, if \( (a_1, m) = 1 \) and \( 0 < a_1 < m \) then any \( a \equiv a_1 \pmod{m} \) also satisfies \( (a, m) \). So we will only list below those \( a \) that are coprime with \( m \) and satisfy \( 0 < a < m \). (Observe \( a \) cannot be 0, since \( (0, m) = m \).)

\[\begin{array}{c}
(i) \text{For } m = 4, \text{ if } a \in \{1, 3\} \text{ then } a, m \text{ are coprime. (If } a = 1 \text{ (respectively } a = 3 \text{) then } x = 1 \text{ (respectively } x = 3 \text{) is a solution of } ax \equiv 1 \pmod{4}.\)
(ii) \text{Since } m = 5 \text{ is prime, for } a \in \{1, 2, 3, 4\} \text{ we have } a, m \text{ are coprime. (Possibilities for } x \text{ are } 1, 3, 2, 4 \text{ respectively. For each } a \text{ there are an infinite number of possibilities for } x \text{ but all the possibilities are congruent modulo } m.\)
(iii) \text{For } m = 6, \text{ if } a \in \{1, 5\} \text{ then } a, m \text{ are coprime. (Possibilities for } x \text{ are } 1, 5 \text{ respectively.)}
(iv) \text{Since } m = 7 \text{ is prime, for } a \in \{1, 2, 3, 4, 5, 6\} \text{ we have } a, m \text{ are coprime. (Possibilities for } x \text{ are } 1, 4, 5, 2, 3, 6 \text{ respectively.)}
\end{array}\]

3. Solve \( 58x \equiv 1 \pmod{127} \).

**[Hint. Use the Euclidean Algorithm as one of your steps.]**

**Solution.** Observe that \( 58x \equiv 1 \pmod{127} \) is equivalent to saying that 
\[
58x + 127y = 1 \tag{2}
\]
for some integer \( y \), i.e. a solution exists if and only if \( 58 \) and \( 127 \) are coprime (see discussion in previous question solution). Thus using the Euclidean Algorithm:

\[
\begin{array}{cc|c|c}
58 & 127 & 2 \\
55 & 116 & 2 \\
3 & 11 & 4 \\
3 & 11 & 0 \\
\end{array}
\]

Thus

\[
\begin{align*}
-1 &= 11 - 4.3 \\
&= 11 - 4(58 - 5.11) \\
&= 11 - 4(53 - 5.11) \\
&= 21.11 - 4.58 \\
&= 21.11 - 4.58 \\
&= 21.127 - 46.58 \\
&\text{So... } 1 = -21.127 + 46.58
\end{align*}
\]
Hence, by the Theorem in the section on Diophantine equations of the Number II notes, (2) has general solution

\[ x = 46 + 127t \]
\[ y = -21 - 58t \]

i.e. \( x \equiv 46 \pmod{127} \).

4. Using the Caesar cipher, with \( a, b, m \) as defined in the dangerous bend on page 2 of the notes, encode: CRYPTOLOGY.

**Answer.** With \( a = 1, b = 3 \) and \( m = 27 \), the Caesar cipher amounts to being a cyclic shift of each letter by three letters. Hence CRYPTOLOGY is encoded as:

FUASWRORJA

*5. Decode the following message. Spaces are also encoded. There is one space in the encoded output.

RUOELTWK EINHXFEQHZETYTDJPEHVONERUOEBGCAEMHS

(See additional comments and hint in the problem over the page.)

**Solution.** First observe that the letters occurring in the message have the following frequencies:

\[ E: 8; \quad H: 4; \quad O: 3; \quad N, R, T, U: 2; \]

where \( \# \) represents a (SPACE). Since E also occurs in the message every 4–5 letters or so we can be fairly confident that E encodes a (SPACE). Then RUO is a three letter word that occurs twice and in particular it comes at the beginning of the message. More than likely RUO encodes THE. Also we are given that a Caesar cipher has been used where each letter with numeric encoding \( u \) is encoded as the letter with numeric encoding \( v \) according to

\[ v \equiv au + b \pmod{27}, \]

for some \( a, b \) such that \( (a, 27) = 1 \). Since \( (a, 27) = 1 \), there exists an integer \( c \) such that \( ca \equiv 1 \pmod{27} \) (see the solutions of questions 4. and 5.), and for such a choice of \( c \) we have

\[ cv \equiv cau + cb \pmod{27} \]
\[ u \equiv cv - cb \pmod{27} \]
\[ u \equiv cv + d \pmod{27} \]

rearranging and using \( ca \equiv 1 \pmod{27} \), where \( d = -cb \). This is the decoding rule. Now we use our guesses (beside each letter is its corresponding numeric encoding):

\[ 
\begin{align*}
\# & \rightarrow 0 \quad & \text{encodes as} & \quad E & \rightarrow 5 \\
T & \rightarrow 20 \quad & \text{encodes as} & \quad R & \rightarrow 18 \\
H & \rightarrow 8 \quad & \text{encodes as} & \quad U & \rightarrow 21 \\
E & \rightarrow 5 \quad & \text{encodes as} & \quad O & \rightarrow 15 
\end{align*}
\]
The first two of our guesses give:

\[ 0 \equiv c \cdot 5 + d \pmod{27} \quad (3) \]
\[ 20 \equiv c \cdot 18 + d \pmod{27} \quad (4) \]

Subtracting (3) from (4) (to eliminate \(d\)) we obtain:

\[ 20 \equiv c \cdot 13 \pmod{27} \quad (5) \]

Observe that \(13 \cdot 2 = 26 \equiv -1 \pmod{27}\). So multiplying (5) throughout by 2 we obtain:

\[ 40 \equiv 26c \pmod{27} \]
\[ 13 \equiv -1c \pmod{27} \]
So... \(c \equiv 14 \pmod{27}\)

Substituting \(c \equiv 14 \pmod{27}\) in (3) gives:

\[ d \equiv -14.5 \equiv 13.5 \pmod{27} \]
\[ \equiv 65 \pmod{27} \]
\[ \equiv 11 \pmod{27} \]

So our **decoding** algorithm is:

\[ u \equiv 14v + 11 \pmod{27} \]

By the way, multiplying the **decoding** algorithm by 2 and rearranging gives the **encoding** algorithm:

\[ v \equiv 2u + 5 \pmod{27} \]

Using the **decoding** algorithm we obtain the following **decoding** table:

<table>
<thead>
<tr>
<th>#</th>
<th>A</th>
<th>B</th>
<th>C</th>
<th>D</th>
<th>E</th>
<th>F</th>
<th>G</th>
<th>H</th>
</tr>
</thead>
<tbody>
<tr>
<td>decodes as</td>
<td>K</td>
<td>Y</td>
<td>L</td>
<td>Z</td>
<td>M</td>
<td>#</td>
<td>N</td>
<td>A</td>
</tr>
<tr>
<td>decodes as</td>
<td>I</td>
<td>J</td>
<td>K</td>
<td>L</td>
<td>M</td>
<td>N</td>
<td>O</td>
<td>P</td>
</tr>
<tr>
<td>decodes as</td>
<td>R</td>
<td>S</td>
<td>T</td>
<td>U</td>
<td>V</td>
<td>W</td>
<td>X</td>
<td>Y</td>
</tr>
<tr>
<td>decodes as</td>
<td>T</td>
<td>G</td>
<td>U</td>
<td>H</td>
<td>V</td>
<td>W</td>
<td>I</td>
<td>J</td>
</tr>
</tbody>
</table>

Observe that the **decoding** table does agree with the two guesses we did not use for working it out. (So things are looking good.) Using the table, we get that the message decodes as:

**THE QUICK BROWN FOX JUMPS OVER THE LAZY DOG**

and since this is a perfectly sensible English sentence it would seem we have cracked the code.
6. Find the values of $p, q, k$ for Example 2 ($n = 2773$, $d = 157$ and $e = 17$).

**Solution.** From the RSA Theorem we know that $n, p, q, k, d, e$ satisfy

\[
p, q \text{ are distinct primes,} \\
n = pq, \\
k = (p - 1)(q - 1), \\
(d, k) = 1 \text{ and} \\
de \equiv 1 \pmod{k}.
\]

In particular,

\[
k = (p - 1)(q - 1) \\
= pq - p - q + 1 \\
= n - (p + q) + 1.
\]

Without loss of generality, assume $p < q$. Then $2 \leq p < \sqrt{n}$ and so $n/2 - 1 \leq k < n/2 \sqrt{n} + 1$. Also the possibilities for $de$ are: $1, k + 1, 2k + 1, \ldots$. Since $de = 157 \cdot 17 = 2669$ is both greater than $n/2 - 1$ and less than $n$ we see that the only possibility is: $de = k + 1$. So $k = de - 1 = 2668$. Thus:

\[
p + q = n - k + 1 \\
= 2773 - 2668 + 1 = 106.
\]

So we have:

\[
p + q = 106 \\
pq = 2773.
\]

Observe that

\[
(x - p)(x - q) = x^2 - (p + q)x + pq,
\]

and so $p, q$ are the solutions of the following quadratic equation

\[
x^2 - 106x + 2773 = 0
\]

i.e.

\[
p, q = \frac{106 \pm \sqrt{106^2 - 4 \cdot 2773}}{2} \\
= 53 \pm \sqrt{53^2 - 2773} \\
= 53 \pm 6 \\
= 47, 59.
\]

So $p = 47$, $q = 59$, $k = 2668$. (Remember, we assumed $p < q$. Of course, $p = 59$, $q = 47$ would also have been a correct solution.)
7. Use $e = 3$ and $n = 2773$ to encode the following message using the RSA cryptosystem:

CODING IS EASY

Use 2-letter blocks and don’t omit spaces.

**Solution.**

- First we numerically encode the letters of the message as per the table on page 1 of the Number Theory III notes:

  C O D I N G # I S # E A S Y
  03 15 04 09 14 07 00 09 19 00 05 01 19 25

- Now we encode each block $a$ with $b$ according to the algorithm: $b = a^e \mod n$. This gives us the encoding:

  1392 2473 1336 0729 1138 1497 1919

As an example, the first block of the encoding was obtained as follows:

$315^3 = 99225.315 \equiv 2173.315 \mod 2773 \equiv 1392 \mod 2773$

Thus the RSA encoding of the message is: 1392247313360729113814971919.

*8. Decode the following message. Spaces are also encoded. (It just so happens that no spaces appear after the encoding.)

**BKDAKUNFKDWTDBJKNWKNANTTNLKWNTKBKIDS**

**CKMCCUKYCMFCTJDYKDUKBBKHNSCCKFNJDY**

Note that a *Caesar cipher* has been used (i.e. (SPACE), A, ..., Z are encoded as 00, 01, ..., 26 (as per the table on page 1 of the notes), the Caesar cipher algorithm

$v \equiv au + b \pmod{27}$

has been applied for each letter $u$ of the message for some $a, b$ (which you essentially have to find), and the encoded letter $v$ has been changed back to a letter using the table on page 1 of the notes again.)

**Note:** Letters and spaces occurring in English text, arranged approximately in order of highest frequency to lowest frequency are

⟨SPACE⟩, E, T, A, I, O, N, S, H, R, D, L, U, ...

Also, use the fact that inter-word spaces occur on average every 4–5 letters and use what you know about the possibilities of letters in short words of 1, 2 or 3 letters.

If this problem seems too hard, try doing it without using the fact that a Caesar cipher has been used.

**Hint.** Since you want to decode you really want to express $u$ in terms of $v$, i.e. you really want to find a $c, d$ such that

$u \equiv cv + d \pmod{27}$. 

6
Solution. First observe that the letters occurring in the message have the following frequen-
cies:

\begin{align*}
    \text{K: } & 14; \quad \text{N: } 8; \quad \text{D: } 7; \quad \text{C: } 6; \quad \text{T: } 5; \\
    \text{F,B,J: } & 4; \quad \text{U,Y,W: } 3; \quad \text{M,A,S: } 2; \quad \text{H,L,I: } 1.
\end{align*}

Since K is the most frequent letter of the encoded message and it also occurs in the message
every 4–5 letters or so we can be fairly confident that K encodes a \langle \text{SPACE} \rangle. Under this
assumption, the message starts with a 1-letter word, followed by a 2-letter word. So we
guess that B either represents A or I. If B decodes as A, then we are left with only strange
possibilities for the following 2-letter word; so it is more likely that B decodes as I.

Now let’s try to work out which letter decodes as E. In the encoded message we find N and
D are the next most frequently occurring letters (after K), but both of these occur at the
beginning of a 2-letter word – so it would seem unlikely that either of these letters decodes as
E. The next most frequently occurring letter in the encoded message is C – it occurs doubled
in one word and at the end of several others; so there is a pretty good chance that C decodes
as E.

Our guesses are as follows (beside each letter is its corresponding numeric encoding, as per
the table on page 1 of the notes):

\begin{align*}
    \# & \leftrightarrow 0 \quad & \text{encodes as } & K & \leftrightarrow 11 \\
    I & \leftrightarrow 9 \quad & \text{encodes as } & B & \leftrightarrow 2 \\
    E & \leftrightarrow 5 \quad & \text{encodes as } & C & \leftrightarrow 3
\end{align*}

from which we obtain the following congruences:

\begin{align*}
    0 & \equiv c.11 + d \pmod{27} \quad (6) \\
    9 & \equiv c.2 + d \pmod{27} \quad (7) \\
    5 & \equiv c.3 + d \pmod{27} \quad (8)
\end{align*}

Subtracting (7) from (5) (to eliminate \(d\)) we obtain:

\[ c \equiv -4 \equiv 23 \pmod{27} \quad (9) \]

Substituting (9) back in (7) and rearranging we obtain

\[ d \equiv 9 - (-4.2) \equiv 17 \pmod{27} \]

So our \textit{decoding} algorithm is:

\[ u \equiv -4v + 17 \pmod{27} \]

Multiplying the \textit{decoding} algorithm by \(-7\) and rearranging gives the \textit{encoding} algorithm:

\[ v \equiv -7u + 11 \pmod{27} \]

Observe that we did not use (6) at all. If we had subtracted (7) from (6) we would have
obtained:

\[ -9 \equiv 9c \pmod{27} \]

whence by Lemma ?? of the notes,

\[ -1 \equiv c \pmod{3}, \]

giving us several possibilities for \(c\) \textit{modulo} 27, namely: \(c \equiv 2, 5, 8, 11, 14, 17, 20, 23, 26 \pmod{27}\).
Using the *decoding* algorithm we obtain the following *decoding* table:

<table>
<thead>
<tr>
<th>#</th>
<th>A</th>
<th>B</th>
<th>C</th>
<th>D</th>
<th>E</th>
<th>F</th>
<th>G</th>
<th>H</th>
</tr>
</thead>
<tbody>
<tr>
<td>0</td>
<td>1</td>
<td>2</td>
<td>3</td>
<td>4</td>
<td>5</td>
<td>6</td>
<td>7</td>
<td>8</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>I</th>
<th>J</th>
<th>K</th>
<th>L</th>
<th>M</th>
<th>N</th>
<th>O</th>
<th>P</th>
<th>Q</th>
</tr>
</thead>
<tbody>
<tr>
<td>9</td>
<td>10</td>
<td>11</td>
<td>12</td>
<td>13</td>
<td>14</td>
<td>15</td>
<td>16</td>
<td>17</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>R</th>
<th>S</th>
<th>T</th>
<th>U</th>
<th>V</th>
<th>W</th>
<th>X</th>
<th>Y</th>
<th>Z</th>
</tr>
</thead>
<tbody>
<tr>
<td>18</td>
<td>19</td>
<td>20</td>
<td>21</td>
<td>22</td>
<td>23</td>
<td>24</td>
<td>25</td>
<td>26</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>I</th>
<th>J</th>
<th>K</th>
<th>L</th>
<th>M</th>
<th>N</th>
<th>O</th>
<th>P</th>
<th>Q</th>
</tr>
</thead>
<tbody>
<tr>
<td>9</td>
<td>10</td>
<td>11</td>
<td>12</td>
<td>13</td>
<td>14</td>
<td>15</td>
<td>16</td>
<td>17</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>R</th>
<th>S</th>
<th>T</th>
<th>U</th>
<th>V</th>
<th>W</th>
<th>X</th>
<th>Y</th>
<th>Z</th>
</tr>
</thead>
<tbody>
<tr>
<td>18</td>
<td>19</td>
<td>20</td>
<td>21</td>
<td>22</td>
<td>23</td>
<td>24</td>
<td>25</td>
<td>26</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>I</th>
<th>J</th>
<th>K</th>
<th>L</th>
<th>M</th>
<th>N</th>
<th>O</th>
<th>P</th>
<th>Q</th>
</tr>
</thead>
<tbody>
<tr>
<td>9</td>
<td>10</td>
<td>11</td>
<td>12</td>
<td>13</td>
<td>14</td>
<td>15</td>
<td>16</td>
<td>17</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>R</th>
<th>S</th>
<th>T</th>
<th>U</th>
<th>V</th>
<th>W</th>
<th>X</th>
<th>Y</th>
<th>Z</th>
</tr>
</thead>
<tbody>
<tr>
<td>18</td>
<td>19</td>
<td>20</td>
<td>21</td>
<td>22</td>
<td>23</td>
<td>24</td>
<td>25</td>
<td>26</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>W</th>
<th>S</th>
<th>T</th>
<th>U</th>
<th>V</th>
<th>W</th>
<th>X</th>
<th>Y</th>
<th>Z</th>
</tr>
</thead>
<tbody>
<tr>
<td>23</td>
<td>19</td>
<td>20</td>
<td>21</td>
<td>22</td>
<td>23</td>
<td>24</td>
<td>25</td>
<td>26</td>
</tr>
</tbody>
</table>

Observe that the *decoding* table does agree with our other guess (K encodes #) that we did not use for working it out. (So things are looking good.) Using the table, we get that the message decodes as:

I AM NOT AFRAID OF TOMORROW FOR I HAVE SEEN YESTERDAY AND I LOVE TODAY

and since this is a perfectly sensible English sentence we can be fairly confident that we have cracked the code.

9. Use \( e = 3 \) and \( n = 2773 \) to encode the following message using the RSA cryptosystem:

THE HUNS ARE COMING

Use 2-letter blocks and don’t omit spaces.

**Solution.**

- First we numerically encode the letters of the message as per the table on page 1 of the Number Theory III notes:

| T   | H   | E   | #   | H   | U   | N   | S   | #   | A   | R   | E   | #   | C   | O   | M   | I   | N   | G   | #   |
|-----|-----|-----|-----|-----|-----|-----|-----|-----|-----|-----|-----|-----|-----|-----|-----|-----|-----|-----|-----|-----|-----|
| 20  | 08  | 05  | 00  | 08  | 21  | 14  | 19  | 00  | 01  | 18  | 05  | 00  | 03  | 15  | 13  | 09  | 14  | 07  | 00  |

- Now we encode each block \( a \) with \( b \) according to the algorithm: \( b = a^e \mod n \). This gives us the encoding:

0952 1479 2235 2092 0001 0749 0027 2421 0848 2084

As an example, the first block of the encoding was obtained as follows

\[
2008^3 = 2008^2 \cdot 2008 = 4032064 \cdot 2008 \\
\equiv 122.2008 \pmod{2773} \\
\equiv 952 \pmod{2773}
\]

Thus the RSA encoding of the message is: 0952147922352092000107490027242108482084.
10. Find the decoding algorithm for the previous problem.

**Solution.** Let us suppose we don’t have available to us the results of Problem 8 of the non-homework set. From the RSA theorem we know that \( n = pq \), where \( p, q \) are distinct primes. Without loss of generality, take \( p < q \). Then \( p < \sqrt{2773} < 53 \). So we need to check \( n = 2773 \) for divisibility by each of 2, 3, 5, 7, 11, 13, 17, 19, 23, 29, 31, 37, 41, 43, and 47 (there’s no shorter way); except that, of course, you might guess that \( p, q \) must surely be “close” to \( \sqrt{2773} \) and thus find \( p = 47 \) and \( q = 59 \) straight away. Hence, the parameter \( k \) of the RSA Theorem is:

\[
k = (p - 1)(q - 1) = 46.58 = 2668.
\]

Now, the parameter \( d \) satisfies: \( de \equiv 1 \pmod{k} \). Using the method of Problem 5, we apply the Euclidean Algorithm to \( e = 3 \) and \( k = 2668 \).

\[
\begin{array}{c|cccc}
3 & 2668 \\
& 2667 & 1 & 889 \\
\hline
& 1 & & &
\end{array}
\]

Thus

\[
1 = 2668 - 889.3 \\
\equiv -889.3 \pmod{2668} \\
\equiv 1779.3 \pmod{2668}
\]

So we may take \( d = 1779 \), i.e. the **decoding algorithm** is: \( a = b^{1779} \mod 2773 \), where \( b \) is a 4-digit block of the encoded message and \( a \) is the corresponding decoded block, which we recognise as a pair of two-digit numbers which in turn represent letters according to the table on page 1 of the notes.

\[\begin{array}{c}
11011110011 \\
\end{array}\]

is the **binary** (i.e. base two) representation of 1779, write

\[
b^{1779} = b.b^2.b^{32}.b^{64}.b^{128}.b^{256}.b^{1024}.b^{2048}
\]

where

\[
\begin{align*}
b^{32} &= (((b^2)^2)^2)^2 \\
b^{64} &= (b^{32})^2 \\
b^{128} &= (b^{64})^2 \\
b^{256} &= (b^{128})^2 \\
b^{1024} &= (b^{256})^2 \\
b^{2048} &= (b^{1024})^2
\end{align*}
\]

Each time we square or calculate a product we reduce **modulo 2773**. We need to perform 12 squaring operations and 7 product operations to calculate \( b^{1779} \) for any \( b \). We can write a computer program to do this in the twinkle of an eye and what’s more no intermediate calculation involves a number of greater than 7 digits.