Exercise 2 - Randomization

For an RSA encryption choose \( p = 13 \), \( q = 19 \), \( e = 7 \) and \( d = 31 \).

1. By using the public key, encrypt the decimal message \( M = 14 \).

2. Decrypt the message \( M' = 58 \). Specify the obtained values after each recursive call of \texttt{power} given below.

```c
int power(int a, int p, int n) {
    if (p==0)
        return 1;
    x = power(a, p/2, n);
    result = (x*x)%n;
    if (p%2==1)
        result = (a*result)%n;
    return result;
}
```
Exercise 5 - Reduction relations, ADTs

1. Assume $\rightarrow$ has the Church-Rosser property and $x \leftrightarrow y$. Which of the following holds?

- $x \rightarrow y$ if $y$ is in normal form.
- $x = y$ if both $x, y$ are in normal form.
- None of the above.
- Both of the above.

2. Specify an ADT $\text{List}(A)$ for lists. The operations available for this ADT should be as follows:

- $\text{empty}$: Returns a new empty list.
- $\text{cons}$: Returns a new list by prepending the given element to the given list.
- $\text{head}$: Returns the first element of the given list.
- $\text{tail}$: Returns the given list without its first element.
- $\text{empty?}$: Checks whether a given list is empty.

Specify the signatures for these operations and define sensible identities for them. What are the constructors of the list ADT?
Exercise 6 - Database foundations

1. Consider schemata \( R(A, B, C, D) \) nd \( S(C, D) \) with instances \( r, s \) as shown below:

\[
\begin{array}{cccc}
\text{r} = & a & b & c & d \\
a & b & e & f \\
b & c & e & f \\
e & d & c & d \\
a & b & e & f \\
e & d & e & f \\
a & b & d & d \\
\end{array}
\qquad
\begin{array}{cccc}
\text{s} = & C & D \\
c & d \\
e & f \\
\end{array}
\]

Compute \( r \div s = \)

2. Given the schemas \( R(A, B) \), \( S(B, C) \) and \( T(A, B, C) \) provide an equivalent expression in safe calculus to the following algebra-expression:

\[
\pi[A, B]((R \bowtie S) − T) \cup R
\]

3. Consider the following formula:

\[
\{X, Y \mid (X = a \lor \exists Z. \ R(Y, Z)) \land S(Y)\}
\]

Is the formula safe? If no, explain why.