Compulsory Assignment 2

Question 1.

a)

$$\{a_n\} where\ n\ \geq 0\ and\ a_n = 2^n + (-2)^n$$

$$a_0 = 2^0 + (-2)^0 = 2$$

$$a_1 = 2^1 + (-2)^1 = 0$$

$$a_2 = 2^2 + (-2)^2 = 8$$

$$a_3 = 2^3 + (-2)^3 = 0$$

b)

Now, let a_n represent the salary of the employee some n years after the year 2017.

Each year the employee's salary is increase with 10'000 NOK plus an extra 5% of the salary from the year before. With this information we can set up a recurrence relation which looks something like this:

$$a_n = a_{n-1} * 1.05 + 10'000\ NOK$$

We start with 500'000 NOK then we add n times 10'000 NOK, after adding them together we multiply this value by 1,05. Then at the end we add an extra 10'000 NOK.
So our equation will look something like this: $s_n = a_n + (b * n)) * r + b$

And in this equation the year 2017 will be $a = 0$, and $a \geq 0$

Question 2.

a)

$$(32 \; mod \; 13)^3 \; mod \; 11$$

Now in the book it states:

Let m be a positive integer and let a and b be integers. Then (a + b) mod m = ((a mod m) + (b mod m)) mod m and ab mod m = ((a mod m)(b mod m)) mod m.

Therefore, we can split up the equation to look like this:

$$((32 \; mod \; 13)(32 \; mod \; 13)(32 \; mod \; 13)) \; mod \; 11$$

With this much simpler equation we can calculate $32 \; mod \; 13$

$$32 = 13 * x + y$$

We can look how many times 13 goes into 32 and find the remainder.

$$32 = 13 * 2 + 6$$

So, now our equation looks like this:

$$6^3 \; mod \; 11 = 216 \; mod \; 11$$
$$216 = 11 * x + y$$

Again, we can look how many times 11 goes into 216, and the remainder *y* is our answer.

$$216 = 11 * 19 + 7$$
$$y = 7$$

b)

$$11^{644} \; mod \; 645$$

To complete this equation, we use the algorithm for fast modular exponentiation which we can find in the book:

ALGORITHM 5 Fast Modular Exponentiation.

procedure *modular exponentiation*(b: integer, $n = (a_{k-1}a_{k-2} \ldots a_1a_0)_2$,
m: positive integers)
$x := 1$
$power := b$ **mod** m
for $i := 0$ **to** $k - 1$
  if $a_i = 1$ **then** $x := (x \cdot power)$ **mod** m
  $power := (power \cdot power)$ **mod** m
return $x\{x$ equals b^n **mod** $m\}$

In the start, $x = 1$, and our $power$ is $11 \; mod \; 645 = 11$

Then, we need to convert the exponent (644) to binary:

$$644 = 2 * 322 + 0$$
$$322 = 2 * 161 + 0$$
$$161 = 2 * 80 + 1$$
$$80 = 2 * 40 + 0$$
$$40 = 2 * 20 + 0$$
$$20 = 2 * 10 + 0$$
$$10 = 2 * 5 + 0$$
$$5 = 2 * 2 + 1$$
$$2 = 2 * 1 + 0$$
$$1 = 2 * 0 + 1$$

Now we can read the remainders of each equation from bottom to top, and we get our binary number of 244 which is $(1010000100)_2$ this will act as our n in this algorithm.

To be clear we start at $i = 0$ and work our wat up to a_{k-1}, and in our instance $k - 1 = 9$.

$a_0 = 0$:
$x = 1$

$power = 11^2 \; mod \; 645 = 121 \; mod \; 645 = 121$

$a_1 = 0$:
$x = 1$
$power = 121^2 \; mod \; 645 = 1461 \; mod \; 645 = 451$

$a_2 = 1$:
$x = (1 * 451) \; mod \; 645 = 451$
$power = 451^2 \; mod \; 645 = 203401 \; mod \; 645 = 226$

$a_3 = 0$:
$x = 451$
$power = 226^2 \; mod \; 645 = 51076 \; mod \; 645 = 451$

$a_4 = 0$:
$x = 451$
$power = 121^2 \; mod \; 645 = 14641 \; mod \; 645 = 451$

$a_5 = 0$:
$x = 451$
$power = 451^2 \; mod \; 645 = 203401 \; mod \; 645 = 226$

$a_6 = 0$:
$x = 451$
$power = 226^2 \; mod \; 645 = 51076 \; mod \; 645 = 121$

$a_7 = 1$:
$x = (451 * 121) \; mod \; 645 = 54571 \; mod \; 645 = 391$
$power = 121^2 \; mod \; 645 = 14641 \; mod \; 645 = 451$

$a_8 = 0$:
$x = 391$
$power = 451^2 \; mod \; 645 = 203401 \; mod \; 645 = 226$

$a_9 = 1$:
$x = (391 * 226) \; mod \; 645 = 88366 \; mod \; 645 = 1$
$power = 226^2 \; mod \; 645 = 203401 \; mod \; 645 = 226$

$return \; x = 1$

This means our answer to the equation $11^{644} \; mod \; 645 = 1$.

c)

If a and m are relatively prime integers and m > 1, then a unique inverse of a mod m exists and is denoted a with a < m and a*a=1 mod m

$$a = 34$$
$$m = 89$$

The first step is to show, using the Euclidean algorithm that a and m are relatively prime.

$$Show\ that: gcd(89, 34) = 1$$
$$89 = 34 * 2 + 21$$
$$37 = 21 * 1 + 16$$
$$21 = 16 * 1 + 5$$
$$16 = 5 * 3 + 1$$
$$5 = 1 * 5 + 0$$

So, the greatest common divider is the last nonzero remaining integer, which is 1.

Next, we write the *gcd*. as a multiple of a and m:

$$\gcd(a, m) = 1$$
$$1 = 3 - 1 * 2$$
$$1 = 1 * 3 - 1 * 2$$
$$1 = 1 * 3 - 1 * (5 - 1 * 3)$$
$$1 = 2 * 3 - 1 * 5$$
$$1 = 2 * (8 - 1 * 5) - 1 * 5$$
$$1 = 2 * 8 - 3 * 5$$
$$1 = 2 * 8 - 3 * (13 - 1 * 8)$$
$$1 = 5 * 8 - 3 * 13$$
$$1 = 5 * (21 - 1 * 13) - 3 * 13$$
$$1 = 5 * 21 - 8 * 13$$
$$1 = 5 * 21 - 8 * (34 - 1 * 21)$$
$$1 = 13 * 21 - 8 * 34$$
$$1 = 13 * (89 - 2 * 34) - 8 * 34$$
$$1 = 13 * 89 - 34 * 34$$

Now we can see that the inverse of *a* modulo *m* is the integer -34.

Question 3.

To encrypt this message using RSA we use the formula: $c = m^e mod\ n$.

We start by dividing the message: “ATTACK” into pairs like such: “AT TA CK”. Then we convert the letters to number where A=0, B=1, C=2, etc.

The highest value we can have in one pair is 2525 and since $2525 < 43 * 59 \ = 2525 < 2537$ this is valid.

Our messages will then be: $0019\ 1900\ 0210$.

Then for each pair we use it in the encryption algorithm. Our three equations look like this:

$$19^{13}\ mod\ 2537$$
$$1900^{13}\ mod\ 2537$$
$$210^{13}\ mod\ 2537$$

Then we need to change the exponent from decimal to binary:

$$13 = 2 * 6 + 1$$
$$6 = 2 * 3 + 0$$
$$3 = 2 * 1 + 1$$
$$1 = 2 * 0 + 1$$

Then reading from bottom to top we get the number $(1101)_2$, and since all the equations have the same exponent, we do not need to repeat this for each equation.

Then again using the 5th algorithm from the book:

ALGORITHM 5 Fast Modular Exponentiation.

procedure *modular exponentiation*(b: integer, $n = (a_{k-1}a_{k-2} \dots a_1 a_0)_2$,
  m: positive integers)
$x := 1$
$power := b$ **mod** m
for $i := 0$ **to** $k - 1$
  if $a_i = 1$ **then** $x := (x \cdot power)$ **mod** m
  $power := (power \cdot power)$ **mod** m
return $x\{x$ equals b^n **mod** $m\}$

$First\ pair$:
$x = 1$
$power = 19\ mod\ 2537 = 19$

$a_0 = 1$:
$x = (1 * 19)\ mod\ 2537 = 19$
$power = 19^2\ mod\ 2537 = 361$

$a_1 = 0$:
$x = 19$
$power = 361^2 mod\ 2537 = 130321\ mod\ 2537 = 934$

$a_2 = 1$:
$x = (19 * 934)\ mod\ 2537 = 17746\ mod\ 2537 = 2524$
$power = 934^2\ mod\ 2537 = 872356\ mod\ 2537 = 2165$

$a_3 = 1$:
$x = (2524 * 2165) mod\ 2537 = 5464460\ mod\ 2537 = 2299$
$power = 2165^2\ mod\ 2537 = 4687225\ mod\ 2537 = 1386$

$return\ x = 2299$

$Second\ pair$:
$x = 1$
$power = 1900\ mod\ 2537 = 1900$

$a_0 = 1$:
$x = (1 * 1900)\ mod\ 2537 = 1900$
$power = 1900^2\ mod\ 2537 = 3610000\ mod\ 2537 = 2386$

$a_1 = 0$:
$x = 19$
$power = 2386^2 mod\ 2537 = 5692996\ mod\ 2537 = 2505$

$a_2 = 1$:
$x = (1900 * 2505)\ mod\ 2537 = 4759500\ mod\ 2537 = 88$
$power = 2505^2\ mod\ 2537 = 6275025\ mod\ 2537 = 1024$

$a_3 = 1$:
$x = (88 * 1024) mod\ 2537 = 90112\ mod\ 2537 = 1317$
$power = 1024^2\ mod\ 2537 = 1048576\ mod\ 2537 = 795$

$return\ x = 1317$

$Third\ pair$:
$x = 1$
$power = 210\ mod\ 2537 = 210$

$a_0 = 1$:
$x = (1 * 210)\ mod\ 2537 = 210$
$power = 210^2\ mod\ 2537 = 44100\ mod\ 2537 = 971$

$a_1 = 0$:
$x = 210$
$power = 971^2 mod\ 2537 = 942841\ mod\ 2537 = 1614$

$a_2 = 1$:
$x = (210 * 1614)\ mod\ 2537 = 338940\ mod\ 2537 = 1519$
$power = 1614^2\ mod\ 2537 = 2604996\ mod\ 2537 = 2034$

$a_3 = 1$:
$x = (1519 * 2034) mod\ 2537 = 3089646\ mod\ 2537 = 2117$
$power = 2034^2\ mod\ 2537 = 4137156\ mod\ 2537 = 1846$

$return\ x = 2117$

After using the RSA encryption algorithm for each group of four integer we get the new value of: 2299 1317 2117, which is the encrypted message.

Question 4.

$$Let\ P(n) be\ the\ statement\ that\ 1^3 + 2^3 + \ldots + n^3 = \left(\frac{n(n+1)}{2}\right)^2\ for\ \mathbb{Z}^+$$

a)

To show that $P(1)$ is true we just plug just plug it in $P(n)$.

$$1^3 = \left(\frac{1(1+1)}{2}\right)^2$$
$$1 = \left(\frac{2}{2}\right)^2$$
$$1 = 1^2 = 1$$

Thus making $P(1)$ true.

b)

The inductive hypothesis is $p(k)$ where $k \geq 1$, and

$$1^3 + 2^3 + \ldots + k^3 = \left(\frac{k(k+1)}{2}\right)^2$$

c)

To prove the inductive step, we look at the function $P(k+1)$.

$$\left(\frac{(k+1)\big((k+1)+1\big)}{2}\right)^2 = 1^3 + 2^3 + \ldots + k^3 + (k+1)^3$$
$$\left(\frac{(k+1)\big((k+1)+1\big)}{2}\right)^2 = \left(\frac{k(k+1)}{2}\right)^2 + (k+1)^3$$
$$\left(\frac{(k+1)(k+2)}{2}\right)^2 = \left(\frac{k^2+k}{2}\right)^2 + \frac{4(k+1)^3}{4}$$
$$\frac{k^4 + 6k^3 + 13l^2 + 12k + 4}{4} = \frac{k^4 + 2k^3 + k^2 + 4k^3 + 12k^2 + 4}{4}$$
$$\frac{k^4 + 6k^3 + 13l^2 + 12k + 4}{4} = \frac{k^4 + 6k^3 + 13l^2 + 12k + 4}{4}$$
$$QED$$