1 Sequences and summations (2 points)

a) Find the first four terms of the sequence $\{a_n\}$ where $n \geq 0$ and $a_n = 2^n + (-2)^n$.

Solution:

$a_n = 2^n + (-2)^n$

To then find the first four terms of this sequence, we plug in {0,1,2,3} into the formula:

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

$a_0 = 1 + 1 = 2$

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

$a_1 = 2 - 2 = 0$

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

$a_2 = 4 + 4 = 8$

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

$a_3 = 8 - 8 = 0$

First four terms of the sequence are {2,0,8,0}

b) An employee joined a company in 2017 with a starting salary of a_0 = NOK 500,000. Every year this employee receives a raise of *b* = NOK 10,000 plus *r* = 5% of the salary of the previous year.

1. Set up a recurrence relation for the salary of this employee *n* years after 2017.

Solution:

Let s_n be the salary of the employee after *n* years from 2009 and onwards.
The salary is increasing by 10 000 NOK plus 1.05 times the previous years salary.

$$s_n = s_{n-1} + 0.05 \cdot s_{n-1} + 10000$$

$$\underline{1.05 \cdot s_{n-1} + 10000}$$

Hence the salary of the previous year (n – 1) times a 5% increase as well as additional base 10 000 NOK salary increase on top of that.

2. Find an explicit formula for the salary of this employee *n* years after 2017.

Solution:

Using the recurrence relation from before.
$s_n = 1.05 \cdot s_{n-1}$
$s_0 = 500000$

$$s_n = 1.05 s_{n-1} + 10000 = 1.05^1 s_{n-1} + 1.05^0 \cdot 10000$$
$$s_n = 1.05(1.05 s^{n-2} + 10000) + 10000$$
$$s_n = 1.05^2 s_{n-2} + (1.05^0 \cdot 10000 + 1.05^1 \cdot 10000)$$
$$s_n = 1.05^2 (1.05 s^{n-3} + 10000) + 10000 + 1.05 \cdot 10000)$$
$$s_n = 1.05^3 s_{n-3} + (1.05^0 \cdot 10000 + 1.05^1 \cdot 10000 + 1.05^2 \cdot 10000$$

From here we use the general sum from before this…

$$s_n = 500000 \cdot 1.05^n + 10000 \cdot \frac{1.05^n - 1}{0.05}$$
$$s_n = 500000 \cdot 1.05^n + 200000 \cdot (1.05^n - 1)$$
$$s_n = 500000 \cdot 1.05^n + 200000 \cdot 1.05^n - 200000$$

$$s_n = 700000 \cdot 1.05^n - 200000$$

2 Number theory (3 points)

a) Find the value of (32 mod 13)^3 mod 11. Use the rules of modular calculus and explicitly write the intermediate steps of your calculation. Do not use a calculator (except to verify the final result) – no points are given if your answer only contains the final result.

Solution:

From

$(32 \bmod 13)^3 \bmod 11$

We can find the value of 32mod13 first.

$32 \bmod 13 = 6$

Now we can swap 6 with 32mod13 and get:

$6^3 \bmod 11$ and using the rules of modular exponentiation we can then rewrite it as

= $(6 \bmod 11 \cdot 6 \bmod 11 \cdot 6 \bmod 11) \bmod 11$

= $7 \bmod 11$ = **7**

b) Use the algorithm for fast modular exponentiation to find the value of 11^644 mod 645. Explicitly write out all the steps of the algorithm to obtain the result. Do not use a calculator (except to verify intermediate results) – no points are given if your answer only contains the final result.

Solution:

$11^{644} \bmod 645$

$11^{644} = (11^2)^{322} = 121^{322}$

$a_2 = a_7 = a_9 = 1$

$a_0 a = a_1 = a_3 = a_4 = a_5 = a_6 = a_8 = 0$

In the start *x* is 1 and the *power* is 11 mod 645

On each iteration the power is multiplied by itself and reduced mod 645.

i = 0, a_0 = 0
x = 1
power = $11^2 \bmod 645 = 121 \bmod 645 = 121$

i = 1, a_1 = 0
x = 1

power = $121^2 \bmod 645 = 14641 \bmod 645 = 451$

i = 2, a_2 = 1
x = 451
power = $451^2 \bmod 645 = 203401 \bmod 645 = 226$

i = 3, a_3 = 0
x = 451
power = $226^2 \bmod 645 = 51076 \bmod 645 = 121$

i = 4, a_4 = 0
x = 451
power = $121^2 \bmod 645 = 14641 \bmod 645 = 451$

i = 5, a_5 = 0
x = 451
power = $451^2 \bmod 645 = 203401 \bmod 645 = 226$

i = 6, a_6 = 0
x = 451
power = $226^2 \bmod 645 = 51076 \bmod 645 = 121$

i = 7, a_7 = 1
x = 451 * 121 mod 645 = 54571 mod 645 = 391

power = $121^2 \bmod 645 = 14641 \bmod 645 = 451$

i = 8, a_8 = 0
x = 391

power = $451^2 \bmod 645 = 203401 \bmod 645 = 226$

i = 9, a_9 = 1
x = 391 * 226 mod 645 = 88366 mod 645 = 1

power = $226^2 \bmod 645 = 203401 \bmod 645 = 226$

The value of $11^{644} \bmod 645$ **is 1.**

c) Find an inverse of a modulo m for a = 34 and m = 89 using the Euclidean algorithm.

Solution:

Since the inverse of a modulo *m* is the integer *b* in which *ab* = 1 (mod m)

$a = 34$
$m = 89$

Using the Euclidean algorithm

$$89 = 2 \cdot 34 + 21$$
$$34 = 1 \cdot 21 + 13$$
$$21 = 1 \cdot 13 + 8$$
$$13 = 1 \cdot 8 + 5$$
$$8 = 1 \cdot 5 + 3$$
$$5 = 1 \cdot 3 + 2$$
$$3 = 1 \cdot 2 + 1$$
$$2 = 1 \cdot 2$$

Meaning 1 is the greatest common divisor. We then write it as a multiple of *a* and *m*,

$$\begin{aligned}
&\gcd(a, m) = 1 \\
&= 3 - 1 \cdot 2 \\
&= 1 \cdot 3 - 1 \cdot 2 \\
&= 1 \cdot 3 - 1(5 - 1 \cdot 3) \\
&= 2 \cdot 3 - 1 \cdot 5 \\
&= 2(8 - 1 \cdot 5) - 1 \cdot 5 \\
&= 2 \cdot 8 - 3 \cdot 5 \\
&= 2 \cdot 8 - 3(13 - 1 \cdot 8) \\
&= 5 \cdot 8 - 3 \cdot 13 \\
&= 5(21 - 1 \cdot 13) - 3 \cdot 13 \\
&= 5 \cdot 21 - 8 \cdot 13 \\
&= 5 \cdot 21 - 8(34 - 1 \cdot 21) \\
&= 13 \cdot 21 - 8 \cdot 34 \\
&= 13(89 - 2 \cdot 34) - 8 \cdot 34 \\
&= 13 \cdot 89 - 34 \cdot 34
\end{aligned}$$

All the operations that have been done above equal 1 and since the inverse is the coefficient of *a*.

The final answer to the question is that the inverse of the modulo m is -34.

3 Cryptography (2 points)

Encrypt the message ATTACK using the RSA system with $n = 43 \cdot 59$ and $e = 13$, translating each letter into integers and grouping together pairs of integers, as done in Example 8 (Rosen Ed 8, pg. 316). Explicitly write out the intermediate steps in your calculation and return the encrypted message again as blocks of four digits.

<u>**Solution:**</u>

Assuming

A = 00, B = 01, C = 02, and so forth…

We divide the message ATTACK into groups of two (pairs of integers). = AT|TA|CK

Then,

AT = 0019 (00 for A, 19 for T)

TA = 1900

CK = 0210,

We know from the text that

$n = 43 \cdot 59$ and $e = 13$.

$n = 2537$ and $e = 13$.

Using this information, we can setup

$P^e \bmod n$, where P will be each pair of integers from the beginning, $e = 13$ and $n = 2537$.

From here now, we can insert the values from the groups into the equation.

AT: 0019 = 19^{13} mod 2537 = 2299

TA : 1900 = 1900^{13} mod 2537 = 1317

CK : 0210 = 210^{13} mod 2537 = 2117

Thus, the encrypted message ATTACK using the RSA system with $n = 43 \cdot 59$ and $e = 13$ is:

<u>2299 1317 2117</u>

4 Induction (3 points)

Let $P(n)$ be the statement that $1^3 + 2^3 + \cdots + n^3 = \left(\frac{n(n+1)}{2}\right)^2$ for the positive integer n. Use mathematical induction to show that $P(n)$ is true for all positive integers n:

a) Show that $P(1)$ is true.

Solution:

$P(1)$:

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

$$= (\frac{2}{2})^2 = 1^2 = 1$$

Therefore, since

$1^3 = (\frac{1(1+1)}{2})^2$ is true.

$P(1)$ is true.

b) What is the inductive hypothesis?

Solution:

The inductive hypothesis is,

$P(\text{k})$ for $k \geq 1$: $1^3 + 2^3 + ... + k^3 = (\frac{k(k+1)}{2})^2$

c) Prove the inductive step, identifying where you use the inductive hypothesis.

Solution:

Proving the inductive step:

In order to do that we have to show $P(k+1)$,

$$(\frac{(k+1)((k+1)+1)}{2})^2 = 1^3 + 2^3 + ... + k^3 + (k+1)^3$$

inductive hypothesis

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

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

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

$$(\frac{(k+1)(k+2)}{2}) \cdot (\frac{(k+1)(k+2)}{2}) = (\frac{k^2+k}{2})^2 + (k+1)^3$$

$$(\frac{(k+1)(k+2)}{2}) \cdot (\frac{(k+1)(k+2)}{2}) = (\frac{k^2+k}{2}) \cdot (\frac{k^2+k}{2}) + (k+1)^3$$

$$\frac{k^4+6k^3+13k^2+12k+4}{4} = (\frac{k^2+k}{2}) \cdot (\frac{k^2+k}{2}) + (k+1)^3$$

$$\frac{k^4+6k^3+13k^2+12k+4}{4} = \frac{(k^2+k) \cdot (k^2+k)}{4} + (k+1)^3$$

$$\frac{k^4+6k^3+13k^2+12k+4}{4} = \frac{(k^2+k) \cdot (k^2+k)}{4} + \frac{4(k+1)^3}{4}$$

$$\frac{k^4+6k^3+13k^2+12k+4}{4} = \frac{(k^2+k) \cdot (k^2+k) + 4(k+1)^3}{4}$$

$$\frac{k^4+6k^3+13k^2+12k+4}{4} = \frac{(k^2+k) \cdot (k^2+k) + 4(k+1)^3}{4}$$

$$\frac{k^4+6k^3+13k^2+12k+4}{4} = \frac{k^4+2k^3+k^2+4k^3+12k^2+12k+4}{4}$$

$$\frac{k^4+6k^3+13k^2+12k+4}{4} = \frac{k^4+6k^3+13k^2+12k+4}{4}$$

Both sides are equal, QED.