PROBLEM SET 6: NUMBER THEORY, MODULAR ARITHMETIC

CS 198-087: INTRODUCTION TO MATHEMATICAL THINKING
UC BERKELEY EECS
FALL 2018

This homework is due on Wednesday, October 24th, at 6:30PM, on Gradescope (note the later deadline than usual). As usual, this homework is graded on participation, but it is in your best interest to put full effort into it. This is a good opportunity to learn how to use LaTeX.

---

1. *GCD and LCM mechanics (skip if you feel comfortable)*

   Determine the greatest common divisor and lowest common multiple for each pair of numbers.

   a. 24, 36

   b. 14, 15

   c. 1200, 2350

   d. 144, 768

   e. 24, 152

Solution:

a. $24 = 2^3 \cdot 3$, $36 = 2^2 \cdot 3^2$

$\gcd(24, 36) = 2^2 \cdot 3 = 12$

$\text{lcm}(24, 36) = 2^3 \cdot 3^2 = 72$

b. $14 = 2 \cdot 7$, $15 = 3 \cdot 5$

$\gcd(14, 15) = 2^0 \cdot 3^0 \cdot 5^0 \cdot 7^0 = 1$

$\text{lcm}(14, 15) = 2^1 \cdot 3^1 \cdot 5^1 \cdot 7^1 = 14 * 15 = 210$

c. $1200 = 2^4 \cdot 3 \cdot 5^2$, $2350 = 2 \cdot 5^2 \cdot 47$

$\gcd(1200, 2350) = 2^1 \cdot 3^0 \cdot 5^2 \cdot 47^0 = 50$

$\text{lcm}(1200, 2350) = 2^4 \cdot 3^1 \cdot 5^2 \cdot 47^1 = 56400$

d. $144 = 12^2 = 2^4 \cdot 3^2$, $768 = 2^8 \cdot 3$

$\gcd(144, 768) = 2^4 \cdot 3 = 48$

$\text{lcm}(144, 768) = 2^8 \cdot 3^2 = 2304$

e. $24 = 2^3 \cdot 3$, $152 = 2^3 \cdot 19$

$\gcd(24, 152) = 2^3 \cdot 3^0 \cdot 19^0 = 8$

$\text{lcm}(24, 152) = 2^3 \cdot 3^1 \cdot 19^1 = 456$

2. *GCD and LCM proof*

Prove that $\text{lcm}(a, b) = a \cdot b$ if and only if $\gcd(a, b) = 1$.

Solution:

Recall, if $a = p_1^{a_1} \cdot p_2^{a_2} \cdot ... \cdot p_k^{a_k}$ and $b = p_1^{b_1} \cdot p_2^{b_2} \cdot ... \cdot p_k^{b_k}$, then

$$\gcd(a, b) = p_1^{min(a_1,b_1)} \cdot p_2^{min(a_2,b_2)} \cdot ... \cdot p_k^{min(a_k,b_k)}$$

and

$$\text{lcm}(a, b) = p_1^{max(a_1,b_1)} \cdot p_2^{max(a_2,b_2)} \cdot ... \cdot p_k^{max(a_k,b_k)}$$

.

Instead of having to prove both directions of this statement, we will actually first prove the statement

$$\gcd(a, b) \cdot \text{lcm}(a, b) = a \cdot b$$

$$\begin{aligned}
\gcd(a, b) \cdot \text{lcm}(a, b) &= (p_1^{min(a_1,b_1)} \cdot p_2^{min(a_2,b_2)} \cdot ... \cdot p_k^{min(a_k,b_k)}) \cdot (p_1^{max(a_1,b_1)} \cdot p_2^{max(a_2,b_2)} \cdot ... \cdot p_k^{max(a_k,b_k)}) \\
&= p_1^{max(a_1,b_1)+min(a_1,b_1)} \cdot p_2^{max(a_2,b_2)+min(a_2,b_2)} \cdot ... \cdot p_k^{max(a_k,b_k)+min(a_k,b_k)} \\
&= p_1^{a_1+b_1} \cdot p_2^{a_2+b_2} \cdot ... \cdot p_k^{a_k+b_k} \\
&= (p_1^{a_1} \cdot p_2^{a_2} \cdot ... \cdot p_k^{a_k}) \cdot (p_1^{b_1} \cdot p_2^{b_2} \cdot ... \cdot p_k^{b_k}) \\
&= ab
\end{aligned}$$

From this, we have that if $\text{lcm}(a, b) = ab$, then $\gcd(a, b) = \frac{ab}{ab} = 1$, and vice versa, hence proving the required statement.

3. *Order of Operations – Multiplication*

In lecture, we showed that if $a \equiv b \pmod{m}$ and $c \equiv d \pmod{m}$, then $a + c \equiv b + d \pmod{m}$.

Prove that if $a \equiv b \pmod{m}$ and $c \equiv d \pmod{m}$, then $a \cdot c \equiv b \cdot d \pmod{m}$.

Solution:

Since we have $a \equiv b \pmod{m}$ and $c \equiv d \pmod{m}$, we can write the following relations:

$$b = a + mk_1$$
$$d = c + mk_2$$

Multiplying our expressions for b and d:

$$\begin{aligned} bd &= (a + mk_1)(c + mk_2) \\ &= ac + ak_2m + ck_1m + k_1k_2m^2 \\ &= ac + m(ak_2 + ck_1 + k_1k_2m) \\ \implies bd - ac &= m \cdot (\text{some integer}) \end{aligned}$$

We've shown that m divides $bd - ac$, hence showing that under these conditions $bd \equiv ac \pmod{m}$.

4. *Last Digit Trick*

   Consider the task of finding the last digit of 3^{15}. One *could* multiply out and determine 3^{15} and read out the last digit, but there is an easier solution.

   When multiplying 3 by itself, there is a pattern in the last digit. Observe:

   $$3^1 = (3), 3^2 = (9), 3^3 = 2(7), 3^4 = 8(1), 3^5 = 24(3), 3^6 = 72(9), ...$$

   We see that the last digits of the first four powers of 3 are 3, 9, 7 and 1. The fifth power of 3 ends in a 3, meaning the pattern will now repeat itself. The key realization is that the last digit of 3^n only depends on the last digit of 3^{n-1}, and nothing else.

   We can generalize this pattern: If we let $L(n)$ represent the last digit of n, we have:

   $$L(3^n) = \begin{cases} 3, & n \equiv 1 \pmod{4} \\ 9, & n \equiv 2 \pmod{4} \\ 7, & n \equiv 3 \pmod{4} \\ 1, & n \equiv 0 \pmod{4} \end{cases}$$

   Similar patterns can also be found for all other digits. However, we don't necessarily need to consider powers of digits. We could also use the same properties when looking at powers of 23 — again, all we care about is the last digit. Looking at only the last digit of a number is equivalent to considering all numbers mod 10.

It should also be noted that $L(a+b) = L(L(a)+L(b))$, for all natural numbers a, b (reason to yourself why this is true).

a. Write a one-line Python function that takes in n and returns $L(n)$ *(this is just to check your understanding; don't use this function for the rest of the problems!).*

b. Determine $L(23^{23})$.

c. Determine $L(7^7 + 8^7 + 9^7)$.

d. Show that when n is any odd positive integer, $L(1^n + 2^n + 3^n + ... + 9^n) = 5$. *(Hint: Look at the last sentence of the above paragraph.)*

Solution:

a. def L(n): return n % 10

b. As mentioned in the problem, the last digit of the powers of 23 follows the same sequence as the last digit of the powers of 3. Since $23 \equiv 3 \pmod 4$, we have that the last digit of 23^{23} is 7.

For reassurance: A quick Python calculation tells us that

$$23^{23} = 208804679998479120343550329105 67$$

c. Here, we need to find the last digit of 7^7, 8^7 and 9^7, add them all together, and find the last digit of that result.

Writing out the last digits of the first few powers of 7, we see the following repeating pattern: 7, 9, 3, 1. To generalize, we have

$$L(7^n) = \begin{cases} 7, & n \equiv 1 \pmod 4 \\ 9, & n \equiv 2 \pmod 4 \\ 3, & n \equiv 3 \pmod 4 \\ 1, & n \equiv 0 \pmod 4 \end{cases}$$

We then know the last digit of 7^7 is 3 (we also could have done this by continuing to write out the pattern, as 7 is not a large number).

Doing the same for the powers of 8, we see the pattern 8, 4, 2, 6 appear. This means the last digit of 8^7 is 2.

Lastly, for 9^7, we notice the pattern 9, 1, 9, 1 (the "cycle" only has length 2, instead of 4). For odd n, the last digit of 9^n is 9, and for even n, the last digit of 9^n is 1. This means the last digit of 9^7 is 9. (We also could have done this by rewriting $9^7 = (3^2)^7 = 3^14$ and using the pattern we noticed for the powers of 3 in the introduction for this question.)

Now, we have $L(7^7 + 8^7 + 9^7) = L(3 + 2 + 9) = L(14) = 4$.

Python tells us that $7^7 + 8^7 + 9^7 = 7703664$, verifying our result.

d. Here's where we will use the power of modular arithmetic. An alternate way of phrasing what we are looking for is $1^n + 2^n + ... + 9^n \pmod{n}$.

Also, in mod 10, we have that $9 \equiv -1$, $8 \equiv -2$, $7 \equiv -3$ and $6 \equiv -4$. This means we are now looking at the quantity

$$(1^n + (-1)^n) + (2^n + (-2)^n) + (3^n + (-3)^n) + (4^n + (-4)^n) + 5^n$$

In the case where n is odd, we have that $(-c)^n = c^n$, and thus $c^n + (-c)^n = 0$, which applies for the first four parentheses. This means that when n is odd, $L(\sum_{i=1}^{9} i^n) = 0 + 0 + 0 + 0 + 5 = 5$, because the last digit of any power of 5 is 5.

(The following is an extension of the question.)

When n is even, things are not as simple. For even n, $c^n + (-c)^n = c^n + c^n = 2c^n$. This means $L(\sum_{i=1}^{9} i^n) = L(2(1^n + 2^n + 3^n + 4^n) + 5^n)$. We'd need to do some casework to determine the value of this quantity for each of the four cases $n \equiv 0 \pmod 4, n \equiv 1 \pmod 4, n \equiv 2 \pmod 4$ and $n \equiv 3 \pmod 4$.

It turns out the following holds true $\forall n \in \mathbb{N}$:

$$L(1^n + 2^n + ... + 9^n) = \begin{cases} 3, & n \equiv 0 \pmod 4 \\ 5, & \text{else} \end{cases}$$

For fun, try and prove that this is the case.

5. *Products of Relative Primes*

Consider the following statement:

$$\forall x, p, q \in \mathbb{N}, x \equiv 0 \pmod{pq} \implies x \equiv 0 \pmod p \wedge x \equiv 0 \pmod q$$

a. Prove this statement.

b. Is the converse of this statement true in general?

c. For what p, q is the converse of this statement true? Prove your hypothesis using the results from Problem 2.

Solution:

a. Since we have that $x \equiv 0 \pmod{pq}$, we have that x is a multiple of pq, meaning we can write $x = cpq$, for some constant $c \in \mathbb{Z}$.

But, this also means we can write $x = (cq)p$, meaning x is a multiple of p, and $x = (cp)q$, meaning x is a multiple of q. This proves our claim.

b. No, it is not. Consider $p = 5$ and $q = 25$. $50 \equiv 0 \pmod 5$ and $50 \equiv 0 \pmod{25}$, but $50 \not\equiv 0 \pmod{125}$.

c. For relatively prime p, q (i.e. for any p, q such that $\gcd(p, q) = 1$). Let's prove this to be true.

To proceed, we use the result from Problem 2, which says that $\text{lcm}(p, q) = pq \iff \gcd(p, q) = 1$. This tells that the lowest common multiple of p, q is pq, which is x itself. Then, we have

$$x \equiv pq \equiv 0 \pmod{pq}$$

as we needed.

6. *Introduction to Fermat's Little Theorem*

Fermat's Little Theorem (also known as FLT) states that for some prime p and any natural number $0 < a < p$:

$$a^{p-1} \equiv 1 \bmod p$$

We will save the proof of Fermat's Little Theorem for future courses.

Use FLT to help you in solving the following problems.

a. Evaluate $5^6 \pmod 7$.

b. Evaluate $25^6 \pmod 7$. How can we use Fermat's Little Theorem here, even though we had the condition that $a < p$?

c. Evaluate $5^{23} + 6^{23} + 7^{23} \pmod{23}$.

d. Why do we require $a > 0$ in our original statement?

e. Show that FLT can also be expressed as $a^p \equiv a \bmod p$ for any $a \geq 0$.

f. Determine $a^{-1} \pmod p$, where p is prime and $a < p$.

Solution:

a. Using FLT, we know that $a^6 \equiv 1 \pmod 7$ for any $0 < a < 7$, so $5^6 \equiv 1 \pmod 7$.

b. We know that $25 \equiv 4 \pmod 7$. Using this fact, we find $25^6 \equiv 4^6 \equiv 1 \pmod 7$.

c. We know that $5^{22}, 6^{22}$ and 7^{22} are all equivalent to 1 in mod 23. Then, we have $5^{23} \equiv 5$, $6^{23} \equiv 6$ and $7^{23} \equiv 7$, giving $5^{23} + 6^{23} + 7^{23} \equiv 5 + 6 + 7 \equiv 18 \pmod{23}$.

d. Suppose we had $a = 0$, or equivalently, $a \equiv 0 (\text{mod } p)$. Then, $0^{p-1} \equiv 1 (\text{mod } p)$ would imply some power of 0 has a remainder of 1 when divided by p. This is impossible as all (non-zero) powers of 0 are defined to be equal to 0; $0 \equiv 0 \pmod{n}$ for all $n \in \mathbb{N}$.

e. Take our original statement $a^{p-1} \equiv 1 \text{mod } p$ and multiply both sides of the expression by a (we can do this, from the rules we proved in Problem 3). This gives us the statement we are looking for; it is in fact stronger because it works for the case when $a = 0$.

f. We know $a^{p-1} \equiv 1 \pmod{p}$. This also means that $a \cdot a^{p-2} \equiv 1 \pmod{p}$, implying that $a^{-1} \equiv a^{p-2} \pmod{p}$.

7. *Exponentiation – Mechanical*

Determine each of the following values. You may need to use Fermat's Little Theorem, or other techniques discussed in lecture.

a. $5^6 \pmod 7$

b. $14^{18} \pmod{15}$

c. $12^{20} \pmod{20}$

d. $17^{63} \pmod{22}$

e. $9^{61} \pmod{11}$

Solution:

a. $5^6 \equiv 1 \pmod 7$, from Fermat's Little Theorem ($7 - 1 = 6$).

b. $14^{18} \equiv (-1)^{18} \equiv 1 \pmod{15}$

c. Here, we will use repeated squaring.

We see that we can write $20 = 16 + 4$, and therefore can write 12^{20} as $12^{16} \cdot 12^4$.

$$
\begin{aligned}
12^1 &\equiv 12 \pmod{20} \\
12^2 &\equiv 144 \equiv 4 \pmod{20} \\
12^4 &\equiv (12^2)^2 \equiv 4^2 \equiv 16 \pmod{20} \\
12^8 &\equiv (12^4)^2 \equiv 16^2 \equiv (-4)^2 \equiv 16 \pmod{20} \\
12^{16} &\equiv (12^8)^2 \equiv 16^2 \equiv (-4)^2 \equiv 16 \pmod{20}
\end{aligned}
$$

Then, we have $12^{20} \equiv 12^{16} \cdot 12^4 \equiv 16 \cdot 16 \equiv (-4)^2 \equiv 16 \pmod{20}$.

d. Again, we will proceed with repeated squaring; we see that $63 = 32+16+8+4+2+1$. We will heavily rely on the fact that $12^2 \equiv 144 \equiv 12 \pmod{22}$.

$$
\begin{aligned}
17^1 &\equiv 17 \pmod{22} \\
17^2 &\equiv (-5)^2 \equiv 25 \equiv 3 \pmod{22} \\
17^4 &\equiv 3^2 \equiv 9 \pmod{22} \\
17^8 &\equiv 9^2 \equiv 15 \pmod{22} \\
17^{16} &\equiv 15^2 \equiv (-7)^2 \equiv 49 \equiv 5 \pmod{22} \\
17^{32} &\equiv 5^2 \equiv 25 \equiv 3 \pmod{22}
\end{aligned}
$$

Then,

$$
\begin{aligned}
17^{63} &= 17^{32} \cdot 17^{16} \cdot 17^8 \cdot 17^4 \cdot 17^2 \cdot 17^1 \\
&\equiv 3 \cdot 5 \cdot 15 \cdot 9 \cdot 3 \cdot 17 \\
&\equiv 15^2 \cdot 27 \cdot 17 \\
&\equiv (-7)^2 \cdot 5 \cdot (-5) \\
&\equiv 5^2 \cdot (-5) \\
&\equiv 3 \cdot (-5) \\
&\equiv -15 + 22 \equiv 7 \pmod{22}
\end{aligned}
$$

Our final result is that $17^{63} \equiv 7 \pmod{22}$.

e. *Solution 1:* From Fermat's Little Theorem, $a^{10} \equiv 1 \pmod{11}$ for any $a < 11$.

$$9^{61} \equiv (9^{10})^6 \cdot 9 \equiv 1^6 \cdot 9 \equiv 9 \pmod{11}$$

Solution 2:

We have $61 = 32 + 16 + 8 + 4 + 1$.

$$
\begin{aligned}
9^1 &\equiv 9 \pmod{11} \\
9^2 &\equiv 4 \pmod{11} \\
9^4 &\equiv 4^2 \equiv 16 \equiv 5 \pmod{11} \\
9^8 &\equiv 5^2 \equiv 3 \pmod{11} \\
9^{16} &\equiv 3^2 \equiv 9 \pmod{11} \\
9^{32} &\equiv 9^2 \equiv 4 \pmod{11}
\end{aligned}
$$

Putting this all together, we have

$$\begin{aligned} 9^{61} &\equiv 9^{32} \cdot 9^{16} \cdot 9^8 \cdot 9^4 \cdot 9^1 \\ &\equiv 4 \cdot 9 \cdot 3 \cdot 5 \cdot 9 \\ &\equiv 36 \cdot 15 \cdot 9 \\ &\equiv 3 \cdot 4 \cdot (-2) \\ &\equiv 1 \cdot (-2) \\ &\equiv -2 \equiv 9 \pmod{11} \end{aligned}$$

Either way, our final result is that $9^{61} \equiv 9 \pmod{11}$.

8. *Extending Fermat's Little Theorem*

As we saw in the last problem, FLT says $a^{p-1} \equiv 1 \bmod p$ for any prime p and $0 < a < p$.

In this problem, we will use FLT to prove the following statement for any relatively prime natural numbers p, q:

$$a^{(p-1)(q-1)} \equiv 1 \bmod pq \quad (1)$$

We will do so by instead proving the following statement:

$$a^{(p-1)(q-1)} - 1 \equiv 0 \bmod pq \quad (2)$$

This result is very important in proving why the RSA encryption algorithm works.

a. i. Show that $a^{(p-1)(q-1)} - 1 \equiv 0 \bmod p$.

ii. Argue why $a^{(p-1)(q-1)} - 1 \equiv 0 \bmod q$. *(Hint: Think about symmetry.)*

b. Use the result from the last part of Problem 5 to show that part (a) implies that equation (2) is true.

c. Now, reason as to why equation (1) is true (this should only take a line).

d. Use this result to evaluate $5^{37} \pmod{26}$.

Solution:

a. i. $a^{(p-1)(q-1)} - 1 \equiv (a^{p-1})^{q-1} - 1 \equiv 1^{q-1} - 1 \equiv 0 \pmod{p}$, using FLT on a^{p-1}.

ii. p and q are symmetric in this equation (i.e. we multiply by $(p-1)(q-1)$), and so the reasoning is the exact same.

b. The last part of Problem 5 tells us that $x \equiv 0 \pmod{p} \wedge x \equiv 0 \pmod{q} \implies x \equiv 0 \pmod{pq}$ if and only if p, q are relatively prime. In this question we are given p, q

are relatively prime, and since we already showed that $(a^{p-1})^{q-1} - 1$ is equivalent to 0 in both mod p and mod q, we have that

$$a^{(p-1)(q-1)} - 1 \equiv 0 \bmod pq$$

c. Adding 1 to both sides shows that this is true.

d. We can factor 26 as $2 \cdot 13$. We have that $(2-1)(13-1) = 12$. From this extension of FLT, we have that $5^{(2-1)(13-1)} \equiv 5^{12} \equiv 1 \pmod{26}$. Then, we have

$$5^{37} \equiv (5^{12})^3 \cdot 5 \equiv 1^3 \cdot 5 \equiv 5 \pmod{26}$$

9. *Finding Inverses – Euclidean Algorithm*

(You likely will not be able to complete later parts until we finish our discussion on the Extended Euclidean Algorithm on Monday.)

The task of finding the inverse of a in $\pmod m$ is equivalent to finding integer solutions to the equation

$$ax + my = 1$$

If we find an ordered pair (x, y) that satisfies this, then we've found x to be the inverse of a. Often times this can be done by guessing and checking, but we need a more robust way to find these coefficients x, y in general.

We've already discussed a method for finding the GCD of two numbers, but we now present another way, called the Euclidean algorithm.

```
def gcd(a, b):
    if b == 0:
        return 1
    else:
        return (b, a % b)
```

In discussion, we will see how to extend the Euclidean algorithm such that it will also find us our values of x, y that we need. For now, attempt to find each of the following quantities, or state that they do not exist.

a. $5^{-1} \pmod{24}$

b. $x : 5x \equiv 3 \pmod{24}$

c. $(n-1)^{-1} \pmod n$, where $n \geq 2 \in \mathbb{N}$

d. $5^{-1} \pmod{23}$

e. $12^{-1} \pmod{42}$

f. $24^{-1} \pmod{47}$

Solution:

a. $5 \equiv 5^{-1} \pmod{24}$, since $5 \cdot 5 \equiv 25 \equiv 1 \pmod{24}$. This one is simple enough to discover via trial and error.

b. To solve, we need to multiply both sides of $5x \equiv 3 \pmod{24}$ by the inverse of 5, in order to isolate x. Doing so yields $x \equiv 3 \cdot 5^{-1} \equiv 3 \cdot 5 \equiv 15 \pmod{24}$. To confirm, $5 \cdot 15 \equiv 75 \equiv 3 \pmod{24}$.

c. In general, $(n-1)^{-1} \equiv n-1 \pmod{n}$. Looking at the expansion of $(n-1)^2 = n^2 - 2n + 1$, we see that the first two terms both reduce to 0 in $\pmod{n}$. This gives that $(n-1)(n-1) \equiv 1 \pmod{n}$, meaning that $n-1$ is its own inverse, modulo n.

d. The calls we'd make to the Euclidean algorithm are $(23, 5)$, $(5, 3)$, $(3, 2)$ and $(2, 1)$. We can then write the following relationships using the division algorithm:

$$\begin{aligned} 23 &= 4 \cdot 5 + 3 \\ 5 &= 1 \cdot 3 + 2 \\ 3 &= 1 \cdot 2 + 1 \end{aligned}$$

Rearranging for the remainders, we have

$$\begin{aligned} 3 &= 23 - 4 \cdot 5 \\ 2 &= 5 - 1 \cdot 3 \\ 1 &= 3 - 1 \cdot 2 \end{aligned}$$

Substituting, we have

$$\begin{aligned} 1 &= 3 - 1 \cdot 2 \\ &= 3 - 1 \cdot (5 - 1 \cdot 3) = 2 \cdot 3 - 1 \cdot 5 \\ &= 2 \cdot (23 - 4 \cdot 5) - 1 \cdot 5 \\ &= 2 \cdot 23 - 9 \cdot 5 \end{aligned}$$

We've written 1 as $2 \cdot 23 - 9 \cdot 5$, giving us that -9, or 14 (which we get from $-9 + 23$), is the inverse of 5 in modulo 23. To verify:

$$5 \cdot 14 \equiv 70 \equiv 69 + 1 \equiv 1 \pmod{23}$$

e. This inverse does not exist, as $\gcd(12, 42) = 6 \neq 1$. Quick reminder: if we were able to find an inverse, it would mean we are able to find integers x, y such that $12x + 42y = 1$. But these integers would also satisfy $2x + 7y = \frac{1}{6}$, however this is a contradiction (the sum of two integers cannot be a fraction).

f. We can see that $24 \cdot 2 \equiv 48 \equiv 1 \pmod{47}$. However, we can do this using the longer Euclidean algorithm extension as well.

$$
\begin{aligned}
47 &= 1 \cdot 24 + 23 \\
24 &= 1 \cdot 23 + 1 \\
\implies 1 &= 24 - 1 \cdot 23 = 24 - 1 \cdot (47 - 1 \cdot 24) \\
&= 2 \cdot 24 - 1 \cdot 47
\end{aligned}
$$