Topic 6: Number Theory I

Example 1

Integer k has his maximum value when it is equal to number of threes in prime factorization of integer P.

When we divide product of first 200 positive integers (first 100 odd numbers are in interval $\langle 1,200 \rangle$) by product of first 100 positive even integers, we get:

$$\frac{1 \cdot 2 \cdot \ldots \cdot 199 \cdot 200}{2 \cdot 4 \cdot \ldots \cdot 198 \cdot 200} = \frac{200!}{2^{100} \cdot 100!}$$

We can see that 2^{100} is not divisible by 3. Thus we can work just with 200! and 100!. To know number of threes in prime factorization of integer P we can use Legendre´s Formula. First we need to know how many threes are in 200! and then subtract from it number of threes in 100! (because $\frac{3^a}{3^b} = 3^{a-b}$).

$$\left\lfloor \frac{200}{3} \right\rfloor + \left\lfloor \frac{200}{3^2} \right\rfloor + \left\lfloor \frac{200}{3^3} \right\rfloor + \left\lfloor \frac{200}{3^4} \right\rfloor - \left\lfloor \frac{100}{3} \right\rfloor - \left\lfloor \frac{100}{3^2} \right\rfloor - \left\lfloor \frac{100}{3^3} \right\rfloor - \left\lfloor \frac{100}{3^4} \right\rfloor = k$$

$$66 + 22 + 7 + 2 - 33 - 11 - 3 - 1 = k$$

$$k = 49$$

The largest k so that P is divisible by 3^k is equal to 49.

Example 2

First way

First of all look at first equation and put it to form what we need for next step.

$$m^2 n + n^2 m = 880$$

$$3m^2 n + 3n^2 m = 3 \cdot 880$$

$$(m+n)^3 = 3 \cdot 880 + m^3 + n^3$$

$$\frac{(m+n)^3 - 3 \cdot 880}{m+n} = m^2 - mn + n^2$$

$$\frac{(m+n)^3 - 3 \cdot 880}{m+n} + mn = m^2 + n^2$$

Now we work with second equation.

$$mn + m + n = 71$$

$$n + m = 71 - mn$$

$$n^2 + 2mn + m^2 = (71 - mn)^2$$

$$n^2 + m^2 = (71 - mn)^2 - 2mn$$

Compare equations.

$$\frac{(m+n)^3 - 3 \cdot 880}{m+n} + mn = (71 - mn)^2 - 2mn$$

$$\frac{(71 - nm)^3 - 3 \cdot 880}{71 - nm} + mn = (71 - mn)^2 - 2mn$$

$$(71 - nm)^3 - 3 \cdot 880 + mn(71 - nm) = (71 - nm)^3 - 2mn(71 - nm)$$

$$-3 \cdot 880 = -3mn(71 - mn)$$

$$880 = mn(71 - mn)$$

Have substitution $x = mn$.

$$x(71 - x) = 880$$

$$x^2 - 71x + 880 = 0$$

There are two roots of this quadratic equation:

<u>$\boldsymbol{x_1 = 55}$</u>

From the equation $n^2 + m^2 = (71 - mn)^2 - 2mn$ and $mn = 55$ we can count this:

$$n^2 + m^2 = 146$$

But we do not know if m and n are both integers so we have to check it. We can express m or n and put it to first equation. After we do it (it is too long and easy so I will not write it) we get m and n are integers $[m, n] = [5,11]$ or $[11,5]$.

<u>$\boldsymbol{x_2 = 16}$</u>

After we do exactly the same as in previous case we get:

$$n^2 + m^2 = 2993$$

When we express m or n and put it to first equation, we find m and n are not integers.

<u>**Conclusion**</u>

We found that there is one solution and it is $n^2 + m^2 = 146$.

Second way

We can put both equations to forms below. Then it is possible to use systematical checking to find possibilities of m and n. After it we can easily find the solutions where m and n are integers and then count $n^2 + m^2$.

$$(m+1)(n+1) = 72 = 2^3 \cdot 3^2$$

$$mn(n+m) = 880 = 2^4 \cdot 5 \cdot 11$$

Example 3

The fraction is in the lowest term when its denominator and numerator are relatively prime. It also means that their greatest common divisor is 1.

Now we have to show it using The Euclidean Algorithm - $GCD(a,b) = GCD(a, b-a)$ where $b > a$.

$$GCD\ (14n+3, 21n+4) = GCD(14n+3, 7n+1) = GCD(7n+1, 7n+2) = GCD(7n+1, 1) = 1$$

We showed that that greatest common divisor of $14n+3$ and $21n+4$ is 1. As was already mentioned, when the greatest common divisor of two numbers is 1 then these numbers are relatively prime. That also means that the fraction $\frac{21n+4}{14n+3}$ is for all positive integers in the lowest term.

Example 4

<u>Part 1</u>

We have to determine all positive integers for which $2^n - 1$ is divisible by 7. It is also possible to write is as below.

$$2^n - 1 \equiv 0\ (mod\ 7)$$

$$2^n \equiv 1\ (mod\ 7)$$

Let´s make a table and see for which n it is true.

n	1	2	3	4	5	6
$2^n - 1\ (mod\ 7)$	1	3	0	1	3	0

From the table above we can assume that $2^n \equiv 1\ (mod\ 7)$ is valid for every third positive integer. In this case we can write n as $n = 3k$.

$$2^{3k} \equiv 1\ (mod\ 7)$$

$$(2^3)^k \equiv 1\ (mod\ 7)$$

Number 2^3 is congruent $1\ (mod\ 7)$. So we get:

$$1^k \equiv 1\ (mod\ 7)$$

Number $1^k = 1$ is always congruent $1\ (mod\ 7)$. We proved 2^n is congruent $1\ (mod\ 7)$ for every n which are divisible by 3.

However we cannot be sure there are not any other integers n for which is 2^n congruent 1 modulo 7. So let´s look at $n = 3k+1$ and $n = 3k+2$. When $n = 3k$, $n = 3k+1$ and $n = 3k+2$ we cover all numbers in set of positive integers.

<u>First case $n = 3k+1$</u>

Let´s assume it is true.

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

$$2 \cdot 2^{3k} \equiv 1\ (mod\ 7)$$

As we already proved $2^{3k} \equiv 1\ (mod\ 7)$. Then:

$$2 \cdot 1 \equiv 1\ (mod\ 7)$$

Form above is not right so no integer n what we can express in form $n = 3k + 1$ is congruent $1\ (mod\ 7)$.

<u>Second case $n = 3k + 2$</u>

Let´s assume it is true.

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

$$4 \cdot 2^{3k} \equiv 1\ (mod\ 7)$$

We know that $2^{3k} \equiv 1\ (mod\ 7)$. Then:

$$4 \cdot 1 \equiv 1\ (mod\ 7)$$

This is not right so no integer n what we can express in form $n = 3k + 2$ is congruent $1\ (mod\ 7)$.

<u>**Conclusion**</u>

We found that 2^n is congruent to $1\ (mod\ 7)$ just in case n is divisible by 3.

<u>Part 2</u>

We have to determine all positive integers for which $2^n + 1$ is divisible by 7. Write it as below:

$$2^n \equiv -1\ (mod\ 7)$$

Let´s again have 3 cases of n:

<u>$\boldsymbol{n = 3k}$</u>

We already proved that $2^{3k} \equiv 1\ (mod\ 7)$. So congruence $2^{3k} \equiv -1\ (mod\ 7)$ cannot be valid.

<u>$\boldsymbol{n = 3k + 1}$</u>

In previous part we showed that $2^{3k+1} \equiv 2\ (mod\ 7)$. Then congruence $2^{3k+1} \equiv -1\ (mod\ 7)$ cannot be valid.

<u>$\boldsymbol{n = 3k + 2}$</u>

We showed that $2^{3k+2} \equiv 4\ (mod\ 7)$. Thus $2^{3k+2} \equiv -1\ (mod\ 7)$ cannot be right.

<u>**Conclusion**</u>

We found that 2^n is not congruent $-1\ (mod\ 7)$ for any positive integer n.