Assignment 3

Week 3 | Nandan Madhuj
Project NT#4 | Roll: 210648

1. Prove that, $19 \mid 2^{2^{6k+2}} + 3 \ \forall k \in \{0, 1, 2, 3...\}$ **Sol.**

Let $a_k = 2^{2^{6k+2}} + 3$

We see that $a_0 = 19 \implies 19 \mid a_0$

Suppose $19 \mid a_k \implies 2^{2^{6k+2}} \equiv -3 \mod 19$ ....(i)

Then $a_{k+1} = 2^{2^{6(k+1)+2}} + 3 = 2^{2^{6k+8}} + 3$

Now, $2^{2^{6k+8}} = 2^{2^{6k+2} \cdot 2^6} = (2^{2^{6k+2}})^{64}$

Taking modulo 19, and using (i);

$2^{2^{6k+8}} \equiv (-3)^{64} \mod 19 \equiv 3^{64} \mod 19$

By Fermat's little theorem, we know that,

$3^{18} \equiv 1 \mod 19 \implies 3^{54} \equiv 1 \mod 19$

So, $3^{64} \equiv 3^{10} \equiv 9^5 \equiv 81 \cdot 81 \cdot 9 \mod 19 \equiv 5 \cdot 5 \cdot 9 \equiv 25 \cdot 9 \equiv 6 \cdot 9 \mod 19 \equiv 54 \equiv (-3) \mod 19$

And hence we have

$2^{2^{6k+8}} = a_{k+1} - 3 \equiv -3 \mod 19$

$\implies a_{k+1} \equiv 0 \mod 19$

Hence $19 \mid a_k \implies 19 \mid a_{k+1}$

Since, $19 \mid a_0$, by induction $19 \mid a_k \ \forall \ k \in \{0, 1, 2, \dots\}$

Hence proved.

2. Given $F_n = 2^{2^n} + 1$. To prove $F_n \mid 2^{F_n} - 2$

Since, F_n is odd, $F_n \mid 2^{F_n} - 2 \iff F_n \mid 2^{F_n - 1} - 1$

Considereing $a_n = 2^{2^{2^n}} - 1$,

Factorising a_n using $x^2 - y^2 = (x - y)(x + y)$

$a_n = (2^{2^{2^n - 1}} - 1)(2^{2^{2^n - 1}} + 1)$

Further factorising, the first term,

$a_n = (2^{2^{2^n - 2}} - 1)(2^{2^{2^n - 2}} + 1)(2^{2^{2^n - 1}} + 1)$

The exponent of the exponent is decreasing:

Since, $n < 2^n$, continuing to factor the first terms of a_n, we will reach the following factorisation:

$a_n = 2^{2^{2^n}} + 1 = (2^{2^n} - 1)(2^{2^n} + 1)(2^{2^{n+1}} + 1)(2^{2^{n+2}} + 1) \cdots\cdots (2^{2^{2^n - 1}} - 1)(2^{2^{2^n - 1}} + 1)$

Since, the second term is F_n,

$F_n \mid 2^{F_n - 1} - 1 \implies F_n \mid 2^{F_n} - 2$

3. Let $S_n = 1^n + 2^n + \cdots + (n-1)^n$

When n is odd, we note that:

$S_n = 1^n + 2^n + \ldots (\frac{n-1}{2})^n + (\frac{n+1}{2})^n + \cdots + (n-2)^n + (n-1)^n$

Taking modulo n:

$S_n \equiv 1^n + 2^n + \ldots (\frac{n-1}{2})^n + (-\frac{n-1}{2})^n + \cdots + (-2)^n + (-1)^n \mod n$

Since, n is odd, $(-x)^n = -(x)^n$

$\implies S_n \equiv 0 \mod n \implies n \mid S_n$ (whenever n is odd).

If n is even, either $n \equiv 2 \mod 4$ or $n \equiv 0 \mod 4$.

Considering the first case, $n = 4k + 2$

$\implies S_n$ has 4k + 1 terms, of which 2k+1 are odd and 2k are even $\implies S_n$ is odd $\implies n \nmid S_n$ when $(n = 4k + 2)$.

Considering the second case of an Even number n = 4k such that the highest power of 2 in n is x.

$\implies 2^x \mid n$ and $2^{x+1} \nmid n$

Then, $x < n \implies 2^x$ divides $2^n, 4^n, 6^n .....(n-2)^n$

Also, for the remaining odd numbers:

By Euler's theorem, Since $gcd(2^x, k) = 1$ where k is odd, we have, $k^{2^{x-1}} \equiv 1 \mod 2^x$

Raising both sides of equivalence to suitable powers:

$k^n \equiv 1 \mod 2^x$ for all odd k $\in \{1, 3, 5, 7, \ldots, n-1\}$

Hence, $S_n \equiv \frac{n}{2} \mod 2^x$ for even n.

Let $n \mid S_n \implies 2^x \mid S_n \implies 2^x \mid \frac{n}{2} \implies 2^x \mid 2^{x-1}$. This is not posibble for any x.

Hence, no even n divides S_n

$n \mid S_n \iff 2 \nmid n$ i.e. n is odd.

4. To prove, there are infinitely many n for which $p \mid n \cdot 2^n + 1$

Let such an n exists...

$\implies n \cdot 2^n \equiv -1 \mod p$

Then for m = n + p(p-1).

We see that $m \cdot 2^m \equiv (n + p(p-1)) \cdot 2^{n+p(p-1)} \equiv (n+0) \cdot 2^n \cdot 2^{(p-1)\cdot(p)} \mod p$

We use Fermat's Little Theorem for 2^{p-1}

$\implies m \cdot 2^m \equiv n \cdot 2^n \cdot 1 \mod p \equiv -1 \mod p$

$\implies m \cdot 2^m + 1 \equiv 0 \mod p$

So, if $p \mid n \cdot 2^n + 1 \implies p \mid m \cdot 2^m + 1$ where m = n + p(p-1).

Now we observe that the relation holds at $n = p - 1$

As, $p - 1 \cdot 2^{p-1} + 1 \equiv -1 + 1 \mod p \equiv 0 \mod p$

So we have the following values of n by induction...

Starting at $n_1 = p - 1$ defining $n_k = n_{k-1} + p(p-1)$.

Hence, $\forall\ k \in \mathbb{N}$, n_k satisfies given relation.

5. Does there exist a natural number n such that $\frac{n}{2}$ is a square, $\frac{n}{3}$ is a cube and $\frac{n}{5}$ is a fifth power?

Applying the FTA on n,

Let the power of primes be a,b,c,d,e .... (we can run out of alphabets of-course :P)

$n = 2^a \cdot 3^b \cdot 5^c \cdot 7^d \cdot 11^e ....$

since, $\frac{n}{2}$ is a perfect square,

$\implies 2|a-1$

$2|b$

$2|c$

$2|d$

similarly, 3 and 5 give:

$a \equiv 1 \mod 2$	$a \equiv 0 \mod 3$	$a \equiv 0 \mod 5$
$b \equiv 0 \mod 2$	$b \equiv 1 \mod 3$	$b \equiv 0 \mod 5$
$c \equiv 0 \mod 2$	$c \equiv 0 \mod 3$	$c \equiv 1 \mod 5$

$d \equiv e \equiv f \equiv .... \equiv 0 \mod r \ \forall \ r \in \{2, 3, 5\}$

Hence, by CRT we have unique solutions for a,b,c,d, e, f .... modulo 30.

Hence, $d = 30 \cdot k_1, \quad e = 30 \cdot k_2$ .. and so on.

for a, b, c, using the CRT we get,

$a \equiv 15 \mod 30$

$b \equiv 10 \mod 30$

$c \equiv 6 \mod 30$

Hence the number n has a prime factorisation of the form:

$n = 2^{30 \cdot k_1 + 15} \cdot 3^{30 \cdot k_2 + 10} \cdot 5^{30 \cdot k_3 + 6} \cdot 7^{30 \cdot k_3} \cdot 11^{30 \cdot k_4} \cdot 13^{30 \cdot k_5} \cdot \cdot \cdot \cdot$

Hence, infinite number of such numbers exist with the given form... k_i being naturals.

Smallest of such numbers is $2^{15} \cdot 3^{10} \cdot 5^6$

6. We assume such an n exists:

$n^5 = 133^5 + 110^5 + 84^5 + 27^5$

To start, we take modulo 2 on both sides:

$n^5 \equiv 1 + 0 + 0 + 1 \mod 2 \implies n^5 \equiv 0 \mod 2 \implies n \equiv 0 \mod 2$ (n is even)

Now, We take modulo 3,

$n^5 \equiv 1 - 1 + 0 + 0 \mod 3 \equiv 0 \mod 3$

This is possible only when $n \equiv 0 \mod 3$

Now we take modulo 5,

$n^5 \equiv 3^5 + 0 - 1 + (-3)^5 \mod 5 \equiv 4 \mod 5$

We consider cases when n$\equiv$ 0 or 1 or 2 or 3 or 4 $\mod 5$ and note that $n \equiv 4 \mod 5$ is the only possibility.

Next we take modulo 7:

$n^5 \equiv 0 + 5^5 + 0 + (-1)^5 \mod 7 \equiv 2 \mod 7$

Now, we take all remainders for n (when divided by 7) and find that only for $n \equiv 4 \mod 7$ then $n^5 \equiv 2 \mod 7$

Hence, we have the following relations for n:

$n \equiv 0 \mod 2$

$n \equiv 0 \mod 3$

$n \equiv 4 \mod 5$

$n \equiv 4 \mod 7$

By Chinese remainder theorem, we have unique solution for n (modulo 210).

Applying the CRT, we get $n \equiv 144 \mod 210$

Hence, $n = 210 \cdot k + 144$

We know that, $a^5 + b^5 < (a+b)^5$

Hence, $n^5 = 133^5 + 110^5 + 84^5 + 27^5 < (133 + 110 + 84 + 27)^5 \implies n^5 < 354^5 \implies n < 354$

Hence, if $n = 210k + 144, n < 354 \implies k < 1 \implies k = 0$

Hence, $n = 144$ is the only possibility.(if such n exists.)

7

Firstly, we see that,

$S_1 = \frac{1}{1} + \frac{1}{2} + \frac{1}{3} + \frac{1}{4} + \frac{1}{5} + \frac{1}{6} + \frac{1}{7} + \frac{1}{8} + \frac{1}{9} + 1 = x + 1$

where x $= \frac{1}{1} + \frac{1}{2} + \frac{1}{3} + \frac{1}{4} + \frac{1}{5} + \frac{1}{6} + \frac{1}{7} + \frac{1}{8} + \frac{1}{9}$

For, S2, taking 10 numbers at a time, 1 to 9, 10 to 19... etc

$S_2 = (x)+(x+\frac{10}{1})+(x+\frac{10}{2})+(x+\frac{10}{3})+(x+\frac{10}{4})+(x+\frac{10}{5})+(x+\frac{10}{6})+(x+\frac{10}{7})+(x+\frac{10}{8})+(x+\frac{10}{9})+1$

$\implies S_2 = 20x + 1$

For S3, taking 100 numbers at a time, 1 to 99, 100 to 199 etc

$S_3 = 20x + (20x + \frac{100}{1}) + (20x + \frac{100}{2}) + (20x + \frac{100}{3}) + (20x + \frac{100}{4}) + (20x + \frac{100}{5}) + (20x + \frac{100}{6}) + (20x + \frac{100}{7}) + (20x + \frac{100}{8}) + (20x + \frac{100}{9}) + 1$

$\implies S_3 = 10 \cdot 20x + 100x + 1$

$\implies S_3 = 300x + 1$

The general pattern is: $S_n = n \cdot 10^{n-1} \cdot x + 1$

For, S_n to be an integer, $8 \mid n \cdot 10^{n-1}$

Also $9 \mid n \cdot 10^{n-1}$ $\quad 7 \mid n \cdot 10^{n-1}$ $\quad 5 \mid n \cdot 10^{n-1}$

These relations ensure that $n \cdot 10^{n-1} \cdot x$ is a natural number.

Since, factors of 2 and 5 are presenet in 10 also, firstly n must have 7 and 9 as factors.

$\implies n = 63 \cdot k$

Clearly, for k=1, $8 \mid 10^{62}$ and $5 \mid 10^{62}$

Hence, smallest posibble n is 63.

8

Follwing code in C;

Euler's Totient Function

9

Follwoing code in C;

Totient Function evaluated till a number

10

Remainder for $\binom{n}{r} \mod p$

11

Following code in C;

The Sieve of Eratosthenes