Assignment 3

Gaurang Dangayach
Number Theory and Applications

June 9, 2022

Problem (Question 1). Prove that $19|2^{2^{6k+2}}+3$ for $k = 0, 1, 2, 3, \cdots$

Solution. We would prove this using mathematical induction. Let the statement be true for $n = k$.
Now, for $n = k+1$, we have -

$$\begin{aligned}
2^{2^{6(k+1)+2}}+3 &= (2^{2^{6k+2}})^{2^6}+3\\
&= (19k-3)^{2^6}+3\\
&= (-3)^{2^6}+3(\mod 19)\\
&= 3^{2^6}+3(\mod 19)\\
&= 9^{2^5}+3(\mod 19)\\
&= 81^{2^4}+3(\mod 19)\\
&= 5^{2^4}+3(\mod 19)\\
&= 625^{2^2}+3(\mod 19)\\
&= (-2)^4+3(\mod 19)\\
&= 16+3(\mod 19)\\
&= 0(\mod 19)
\end{aligned}$$

Hence, by mathematical induction, the statement is true. □

Problem (Question 2). Prove that for $F_n = 2^{2^n}+1$ we have $F_n|2^{F_n}-2$ where $n = 1, 2, 3, \cdots$

Solution. I would be using the property that for Fermat numbers FN_n and FN_m where $m > n$, $FN_n|FN_m-2$.
We can see that F_n is a Fermat number. Also, $F_{2^n} = 2^{2^{2^n}}+1$ is also a Fermat number.

$$\begin{aligned}
2^{F_n}-2 &= 2.2^{2^{2^n}}\\
&= 2.(F_{2^n}-1)-2\\
&= 2.(F_{2^n}-2)
\end{aligned}$$

So, by using the above stated property, $F_n|2.(F_{2^n}-2)$ □

Problem (Question 3). Find all integers $n > 1$ such that $1^n+2^n+\cdots+(n-1)^n$ is divisible by n.

Solution. When n is odd, $1^n+2^n+\ +(n-1)^n(\mod n) = 1^n+2^n+\cdots+(-2)^n+(-1)^n(\mod n)$. As number of terms in this expression is even, the i^{th} term from starting (i^n) will be cancelled by i^{th} term from end $((-i)^n)$. So the statement is true for any n where n is odd.
Now, if n is even,
Let e be the highest power of 2 dividing n.
Each of the terms 2^n, 4^n, 6^n ,... , $(n2)^n$ is a multiple of 2^e. On the other hand, for each $k \in \{1, 3, 5, \ldots, n-1\}$,

$k^{\phi(2^e)} \equiv 1(\mod 2^e)$ by Euler's theorem. Since $\phi(2^e) = 2^{e-1}|n$, it follows that $k^n \equiv 1(\mod 2^e)$ for each such k.
Hence, S(n) $= 1^n + 2^n + \cdots + (n-1)^n(\mod 2^e) = n/2(\mod 2^e)$
Now if $n|S(n)$, then $2^e|S(n)$. But then $2^e|(n/2)$, and $2^{e+1}|n$, which contradicts the definition of e given above.
Hence, the statement is true for all odd integers only. □

Problem (Question 4). Prove that for every odd prime p there exist infinitely many positive integers n such that $p|n.2^n + 1$.

Solution. We want to find n such that $n.2^n \equiv (-1)(\mod p)$ Consider the sequences, $a_n = n$ and $b_n = 2^n$.

$$\begin{array}{cccccc} a_n & 1 & 2 & 3 & 4 & .... \\ b_n & 2^1 & 2^2 & 2^3 & 2^4 & .... \end{array}$$

In the $(\mod p)$ periodicity of a_n is p and of b_n is $p-1$ (using Fermat's Little Theorem), so we can get every combination of a_n and b_n in $\mod p$ as p and $p-1$ are co-prime. And, the combination will keep on repeating after $p.(p-1)$ terms, so we can infinitely many such n. □

Problem (Question 5). Does there exist an integer n such that $n/2$ is a perfect square, $n/3$ is a cube and $n/5$ a fifth power?

Solution. Let $n = 2^a.3^b.5^c.m$, where $\gcd(m, 30) = 1$.
$n/2$ is a square $\iff 2|(a-1)$, $2|b$, $2|c$, and m is a square.
$n/3$ is a cube $\iff 3|a$, $3|(b-1)$, $3|c$, and m is a cube.
$n/5$ is a fifth power $\iff 5|a$, $5|b$, $5|(c-1)$, and m is a fifth power.
Now, $a = 15.r$, $r = 1(\mod 2)$, $b = 10.s$, $s = 1(\mod 3)$, $c = 15.t$, $t = 1(\mod 5)$
From m is a square, a cube, and a fifth power, we have m=u^{30}So,n=$2^{15r}.3^{10s}.5^{6t}$ with $r = 1(\mod 2)$, $s = 1(\mod 3)$, $t = 1(\mod 5)$.
The least positive n obtained by setting $r = s = t = u = 1$ is $n = 2^{15}.3^{10}.5^6$. □

Problem (Question 6). (AIME-1989-9) One of the Euler's conjectures was disproved in the 1960s by three American mathematicians when they showed there was a positive integer such that

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

Find the value of n.

Solution. Evaluating the equation in $\mod 2, 3or5, weget-$Using Fermat's Little Theorem, we get -

$$\begin{aligned} n &\equiv 0(\mod 2) \\ n &\equiv 0(\mod 3) \\ n &\equiv 4(\mod 5) \end{aligned}$$

By using Chinese Remainder Theorem, we get $n \equiv 24(\mod 30)$ Now, $n > 133$ also,

$$\begin{aligned} n^5 &= 133^5 + 110^5 + 84^5 + 27^5 \\ &< 133^5 + 110^5 + (84+27)^5 \\ &= 133^5 + 110^5 + 111^5 \\ &< 3.133^5 \end{aligned}$$

So, $(n/133)^5 < 3$.
If n$\geq 174, then$(n/133)$^5 > 3$ So, only possible value of $n = 144$ □

Problem (Question 7). (AIME-2006-II-14) Let S_n be the sum of the reciprocals of the non-zero digits of the integers from 1 to 10^n inclusive. Find the smallest positive integer n for which S_n is an integer.

Solution. Every digit from 1 to 9 repeats $n.10^{(}n-1)$ in 1 to 10^n with 10^n excluded. This can be proved by induction or can be seen by observation. For S_n to be an integer, $n.10^{(}n-1)$ should be divisible by all integers from 2 to 9. As, 10 has 2 and 5 as its factors. For $n > 3$, $10^{(}n-1)$ is divisible by 2,4,5,8. Now, S_n should be divisible by 3,6,7 9. This is equivalent to n being divisible by 7 and 9.
So, the smallest possible value of n=63. □

Problem (Question 8). Implement Euler's Totient function in code. Given a number n, find $\phi(n)$.

Solution. *#Code in Python*
```
def gcd(a,b):
    if b>a :
        i=b
        b=a
        a=i
    while (b!=0):
        rem=a%b
        a=b
        b=rem
    return a

n=int(input())
count=0
for i in range(1,n+1):
    if gcd(i,n)==1:
        count=count+1
print(count)
```
□

Problem (Question 9). (Code) Given a number n, find ϕ for all number less than and equal to n.

Solution. *#Code in Python*
```
def gcd(a,b):
    if b>a :
        i=b
        b=a
        a=i
    while (b!=0):
        rem=a%b
        a=b
        b=rem
    return a

def utf(n):
    count=0
    for i in range(1,n+1):
        if gcd(i,n)==1:
            count=count+1
    return count

n=int(input())
for i in range(n):
    print(i+1,":",utf(i+1))
```
□

Problem (Question 10). (Code) Compute the remainder when C_r^n is divided by p using fermat's little theorem. You are given n, r and p. Here p is a prime greater than n.

Solution.
```
#Code in Python
def mod_fact(n,p):
    if (n==1 or n==0):
        return 1
    else:
        return (n*mod_fact(n-1,p))%p

def mod_inv(a,p):
    return (a**(p-2))%p

n,r,p=input().split()
n=int(n)
r=int(r)
p=int(p)

inv_r=mod_inv(mod_fact(r,p),p)
inv_nr=mod_inv(mod_fact(n-r,p),p)

print((mod_fact(n,p)*inv_r*inv_nr)%p)
```
□

Problem (Question 11). Implement Sieve of Eratosthenes in code. Given a number n, print all primes smaller than or equal to n.

Solution.
```
#Code in Python
n=int(input())
nums=list(range(2,n+1))
for i in range(2,n//2+1):
    k=2
    while (i*k<=n):
        if (i*k in nums):
            nums.remove(i*k)
        k=k+1
print(nums)
```
□