Shape of Ideas: Problem Set 2

Mathematics Club IITM
Arjun Arunanchalam, Swaminath Shiju

- Feel free to reach out to us for doubts! Contact information of the problem-set creators:
  - Arjun - +91 9150716759
  - Swaminath - +91 9740351951

---

§1 Questions

1. a) Prove using induction (3 marks)

$$1^3 + 2^3 + \cdots + n^3 = \frac{n^2(n+1)^2}{4}$$

   b) Prove the cube of any number can be written as the difference between the squares of 2 integers

Solution:

a) The summation is clearly true for $n = 1$. Now assume it is true for $n = m$ i.e

$$1^3 + 2^3 + \cdots + m^3 = \frac{m^2(m+1)^2}{4}$$

Adding $m+1$ to both sides we get

$$\begin{aligned} 1^3 + 2^3 + \cdots + m^3 + (m+1)^3 &= \frac{m^2(m+1)^2}{4} + (m+1)^3 \\ &= (m+1)^2\left(\frac{m^2+4(m+1)}{4}\right) \\ &= \frac{(m+1)^2(m+2)^2}{4} \end{aligned}$$

So by using induction this is true for all $n \in \mathbb{N}$.

b) Given some n^3 we can write it as

$$\begin{aligned} n^3 &= \left(1^3 + 2^3 + \cdots + n^3\right) - \left(1^3 + 2^3 + \cdots + (n-1)^3\right) \\ &= \frac{n^2(n+1)^2}{4} - \frac{(n-1)^2n^2}{4} \end{aligned}$$

Both of those numbers are clearly integral square numbers so QED.

2. Find $(1^p+1)(2^p+1)(3^p+1)\cdots(99^p+1) \pmod{p}$, where $p = 101$. (3 marks)

Solution:

Let the expression be S. Note that 101 is prime. Thus $\gcd(101, i) = 1$ for any integer $i \in [1, 100]$. By FLT,

$$i^p + 1 \equiv i \cdot i^{p-1} + 1 \equiv i + 1 \pmod{101}.$$

Now, the entire expression becomes equivalent to

$$S \equiv (1+1)(2+1)\cdots(100+1) \equiv 100! \equiv -1 \equiv 100 \pmod{p}.$$

3. Find all pairs of positive primes p, q satisfying $p - q = 5$ (2 marks)

Solution:

The difference of two numbers is a positive odd numbers so $p > q$ and one of them must be even. Since 2 is the only even prime and also the smallest $q = 7$. So the only solution is

$$(p, q) = (7, 2)$$

4. For all positive integers n, let $T_n = 2^{2^n} + 1$. Show that if $m \neq n$, then T_m and T_n are relatively prime. (4 marks)

Hints: Subtract a quantity from T_n to obtain a neat factorisation.

Solution:

Let's subtract 2 from T_n.

$$T_n - 2 = 2^{2^n} - 1 = (2^{2^{n-1}} - 1)(2^{2^{n-1}} + 1) = (T_{n-1} - 2)(T_{n-1}) = (T_1 - 2)(T_1)T_2 \cdots T_{n-1} = T_0 T_1 T_2 \cdots T_{n-1}.$$

Now, assume $m > n$. Then, $T_m = T_n \cdot K + 2$. Observe that for T_n, every positive factor > 1 is also $>$ 2. Thus, for a factor $d > 1$ of T_n, $d \nmid T_m$. Thus, no factor of T_n divides T_m, implying they are coprime.

5. Find the general form of solution to the following system of equation (5 marks)

$$18x - 23y = 31$$
$$3x + 12 \equiv 17 \text{ mod } (29)$$
$$5x - 8 \equiv 22 \text{ mod } (17)$$

Hint: You can construct solutions using the Chinese Remainder Theorem, research how to do that

Solution:

We first begin by analyzing eq $2, 3$. Taking constants to the other side we get.

$$3x \equiv 5 \text{ mod } (29)$$
$$5x \equiv 30 \text{ mod } (17)$$

We multiply the first equation by 10 and the second equation by 7 on both sides to simplify.

$$30x \equiv 50 \text{ mod } (29)$$
$$\implies x \equiv 21 \text{ mod } (29)$$

$$35x \equiv 210 \text{ mod } (17)$$
$$\implies x \equiv 6 \text{ mod } (17)$$

By the Chinese Remainder theorem the general solution of these 2 equations are congruent to $6 \cdot 29 \cdot 10 + 21 \cdot 17 \cdot 12 \equiv 6024 \equiv 108$ modulo $29 \cdot 17 = 493$

$$x \equiv 108 \text{ mod } (493)$$

Now the first equation is simply a linear Diophantine equation which has infinite solutions. One of them being $(x, y) = (3, 1)$ then the general solution is $(x, y) = (3 + 23k, \frac{18x - 31}{23})$.
Looking at x again this gives another pair congruence equations

$$x \equiv 3 \text{ mod } (23)$$
$$x \equiv 108 \text{ mod } (493)$$

Again using CRT we get

$$x \equiv 3 \cdot 493 \cdot 7 + 108 \cdot 23 \cdot 343 \text{ mod } (23 \cdot 493)$$
$$\implies x \equiv 601 \text{ mod } (11339)$$

So the general solution is

$$(x, y) = (601 + 11339k, 469 + 8874k)$$

6. Derived a rational approximation of $\sqrt{23}$ by using the continued fraction representation and Pell's equation. (4 marks)

Solution:

First, write $\sqrt{23}$ as $\lfloor\sqrt{23}\rfloor = 4 + (\sqrt{23} - 4)$. Now,

$$\sqrt{23} - 4 = \frac{7}{\sqrt{23} + 4} = \frac{1}{\frac{\sqrt{23}+4}{7}}.$$

Consider the denominator d and write it again as the integer part and the fractional part. $\lfloor d \rfloor = 1, \{d\} = \dfrac{\sqrt{23} - 3}{7}$. Thus,

$$\sqrt{23} - 4 = \frac{1}{1 + \frac{\sqrt{23}-3}{7}} = \frac{1}{1 + \frac{14}{7(\sqrt{23}+3)}}.$$

Write the denominator d of the fractional part as $(\sqrt{23} + 3)/2$, making the numerator 1. Now, $\lfloor d \rfloor = 3, \{d\} = (\sqrt{23} - 3)/2$. Thus,

$$\sqrt{23} - 4 = \frac{1}{1 + \frac{1}{3+\frac{\sqrt{23}-3}{2}}}.$$

Again, write it as $\dfrac{1}{(\sqrt{23} + 3)/7}$, with $\lfloor d \rfloor = 1, \{d\} = (\sqrt{23} - 4)/7$. Write as done previously.

Now, consider $d = \sqrt{23} - 4/7 = \dfrac{1}{\sqrt{23} + 4}$. We get $\lfloor d \rfloor = 8, \{d\} = \sqrt{23} - 4$, which is a repeat of the first residual; the expansion repeats from here on.

The residuals we obtained were $1, 3, 1, 8$. Hence, $\sqrt{23} - 4 = [\overline{1, 3, 1, 8}] \implies \sqrt{23} = [4, \overline{1, 3, 1, 8}]$.

Now, compute the first few terms of the continued expansion. You get $4, 5, 19/4, 24/5, \ldots$. Note that $(24, 5)$ is a solution to the Pell's equation $x^2 - 23y^2 = 1$. Thus, $24/5$ is a rational approximation to $\sqrt{d} = \sqrt{23}$.

7. Use theory of congruences to prove that there doesn't exists integral solutions for the equation (4 marks)

$$x^2 - y^2 = 1002.$$

Hint: Try using small moduli to derive contradictions

Solution:

Consider the equation in mod 4. In mod 4, squares are congruent to 1 or 0. So every term is congruent to either 1 or 0. The RHS is however congruent to 2 which can never be congruent to the RHS.

$(1 - 1 \equiv 0,\ 1 - 0 \equiv 1,\ 0 - 1 \equiv 3,\ 0 - 0 \equiv 0)$

8. a) Prove (5 marks)

$$n = \sum_{d|n} \phi(d)$$

where ϕ is the Euler totient function.

Hint: Try dividing all numbers from 1 to n into classes based on $\gcd(x, n)$.

b) Prove

$$\phi(n) = \sum_{d|n} d\mu\left(\frac{d}{n}\right)$$

where μ is the Möbius function.

(This is a continuation of the above question so you may assume (a) is true)

Solution:

a) Consider all the numbers from 1 to n and divide them into classes S_k defined as

$$S_k = \{m : \gcd(m, n) = k, 1 \leq m < n\}$$

and k belongs to the set of divisors of n.

Clearly each S_k has no common elements and sum of the number of elements in each class is n.

Now $\gcd(m, n) = k$ implies $\gcd\left(\frac{m}{k}, \frac{n}{k}\right) = 1$. This means S_k is the same size as the set of all numbers co-prime to $\frac{n}{k}$.

Bring it all together

$$n = \sum_{k|n} N(S_k) = \sum_{k|n} \phi\left(\frac{n}{k}\right) = \sum_{k|n} \phi(k)$$

b) Now simply applying the inversion formula we get

$$\phi(n) = \sum_{d|n} d\mu\left(\frac{d}{n}\right)$$