

**Solution 1.**

Apply induction on  $n$ . It is clear for  $n = 1$ . Assume that  $n = m + 1 \geq 2$  and that the result holds for positive integers  $\leq m$ . If  $n$  is odd,  $2^{\phi(n)} \equiv 1 \pmod{n}$  by Eulers theorem. By the induction hypothesis (since  $\phi(n) < n$ ), the sequence is eventually constant modulo  $\phi(n)$ ; say,  $u_r \equiv c \pmod{\phi(n)}$  for large  $r$ . Consequently,  $u_{r+1} = 2^{u_r} \equiv 2^c \pmod{n}$  is constant which completes this case. If  $n = m + 1 = 2^k l$  for some positive integer  $k$  and odd  $l$ . Again, by induction hypothesis, the sequence is eventually constant modulo  $l$ . Now,  $u_r \equiv 0 \pmod{2^k}$  for all sufficiently large  $r$ . Thus,  $u_r \equiv u_{r+1} \pmod{2^k l}$  for large  $r$  onwards. The induction is complete.

**Solution 2.**

Note first that there are infinitely many primes with the property that they divide a number of the form  $n^4 + 1$  for some  $n$ . Indeed, if  $p_1, \dots, p_r$  were all such primes, then no prime would be able to divide  $(p_1 \cdots p_r)^4 + 1$ ! Let  $P$  denote the set of all primes with this property. For each  $p \in P$ , we may choose  $n < p/2$  with  $p | (n^4 + 1)$  because we may replace any  $n$  by its residue modulo  $p$  and further change  $n$  to  $p - n$  in case  $n > p/2$ . Thus, for each  $p \in P$ , we have got hold of  $n$  with  $2n < p$  and  $p | (n^4 + 1)$ . Of course, a particular  $n^4 + 1$  has only finitely many prime divisors so that infinitely many integers  $n$  are produced from the infinite set  $P$ .

**Solution 3** (Solved also by Sumitra Garai, M.Math. student from I.S.I.)

It suffices to show that for each pair  $a_1, a_2 \in A$ , there is a common  $m, n$ . Let  $a_i^{m_i} = a_i^{n_i}$  for  $i = 1, 2$  and  $m_i \neq n_i$ . Consider  $m = m_1 m_2 + n_1 n_2, n = m_1 n_2 + m_2 n_1$ . Then

$$a_1^m = (a_1^{m_1})^{m_2} (a_1^{n_1})^{n_2} = (a_1^{n_1})^{m_2} (a_1^{m_1})^{n_2} = a_1^n.$$

Similarly,  $a_2^m = a_2^n$ .

**Solution 4.**

The equality

$$\frac{1}{x_1 x_2} = \frac{1}{x_1(x_1 + x_2)} + \frac{1}{x_2(x_2 + x_1)}$$

obviously generalizes (and follows by induction on  $n$ ) to :

$$\frac{1}{x_1 x_2 \cdots x_n} = \sum_{\sigma \in S_n} \frac{1}{x_{\sigma_1} (x_{\sigma_1} + x_{\sigma_2}) \cdots (x_{\sigma_1} + \cdots + x_{\sigma_n})}.$$

In fact, writing the RHS as

$$\frac{1}{x_1 + \cdots + x_n} \sum_{r=1}^n \sum_{\sigma \in S_n, \sigma(n)=r} \frac{1}{x_{\sigma_1}(x_{\sigma_1} + x_{\sigma_2}) \cdots (x_{\sigma_1} + \cdots + x_{\sigma_{n-1}})}$$

and assuming the equality for  $n-1$ , we get

$$\frac{1}{x_1 + \cdots + x_n} \sum_{r=1}^n \sum_{\sigma \in S_n, \sigma(n)=r} \frac{1}{\prod_{i \neq r} x_i}$$

which is simply  $\frac{1}{x_1 x_2 \cdots x_n}$ . Now, if  $(b_1, \dots, b_n) \in B$  then  $b_i$ 's are distinct and let  $\sigma$  be that permutation for which

$$b_{\sigma_1} < b_{\sigma_2} < \cdots < b_{\sigma_n}.$$

Then, writing  $b_{\sigma_i} - b_{\sigma_{i-1}}$  as  $x_{\sigma_i}$ , we have

$$b_1 \cdots b_n = x_{\sigma_1}(x_{\sigma_1} + x_{\sigma_2}) \cdots (x_{\sigma_1} + \cdots + x_{\sigma_n}).$$

Also,  $b \in B$  means  $b_i \leq n$  for all  $n$  and are distinct; so  $(x_1, \dots, x_n) \in A$ . Therefore,

$$\sum_{b \in B} \frac{1}{b_1 \cdots b_n} = \sum_{\sigma \in S_n} \sum_{x \in A} \frac{1}{x_{\sigma_1}(x_{\sigma_1} + x_{\sigma_2}) \cdots (x_{\sigma_1} + \cdots + x_{\sigma_n})} = \sum_{x \in A} \frac{1}{x_1 \cdots x_n}$$

using the earlier equality.

**Solution 6** (Due to Professor David Savitt.)

We shall prove the (apparently) stronger statement with  $p$  replaced by any power  $q$  of  $p$ . We will prove that if  $A^2 = C^3$ , then either  $A^2 = C^3 = I$  or there exists  $C$  with  $A = C^3, B = C^2$ . Note firstly that if  $A, B \in PSL_2(\mathbf{F}_q)$  satisfy  $A^2 = C^3$  and, if there is a solution  $C$  to  $A = C^3, B = C^2$  exists in  $PSL_2(\overline{\mathbf{F}_p})$ , then  $C = AB^{-1}$  is automatically in the subgroup  $G$  of  $PSL_2(\mathbf{F}_q)$  generated by  $A, B$ . Here, of course,  $\overline{\mathbf{F}_p}$  denotes an algebraic closure of  $\mathbf{F}_q$ . Thus, it does not matter for this problem if the matrices  $A, B$  are replaced by conjugates  $PAP^{-1}, PBP^{-1}$  for some  $P \in PSL_2(\overline{\mathbf{F}_p})$ . The crucial result needed for this is a knowledge of the various finite subgroups of  $PSL_2(\overline{\mathbf{F}_p})$ . There are many sources like Suzuki's and Dickson's texts; the latter has in sections 255 and 260 the following result :

*Any finite subgroup of  $PSL_2(\overline{\mathbf{F}_p})$  is either conjugate to a subgroup of  $PGL_2(\mathbf{F}_p^n)$*

or  $PSL_2(\mathbf{F}_p^n)$  for some  $n$  or the upper triangular invertible matrices or, is isomorphic to  $A_4, S_4, A_5$  or  $D_{2m}$  where  $D_{2m}$  is the dihedral group of order  $2m$  for some  $m \geq 2$  not divisible by  $p$ .

Using this, we may consider our  $G = \langle A, B \rangle$  case-by-case. If  $G$  is conjugate (which, by the observation made earlier, can be thought of as equal) to  $PSL_2(\mathbf{F}_p^n)$ , then it is a simple group unless  $p^n = 2$  or  $3$  (in which cases, the result can be verified directly). As  $\langle A^2 \rangle = \langle C^3 \rangle$  is a proper normal subgroup, this must be the identity. In the case of  $PGL_2(\mathbf{F}_p^n)$  also, a similar argument works as  $PSL_2(\mathbf{F}_p^n)$  is its unique proper normal subgroup when  $p^n > 3$ .

Consider the case of upper triangular group in  $PSL_2(\overline{\mathbf{F}}_p)$ . By lifting  $A, B$  to  $X, Y \in GL_2(\overline{\mathbf{F}}_p)$ , we have  $X^2 = tY^3$  for some constant  $t$ . Thus,  $x = tX, y = tY \in GL_2(\overline{\mathbf{F}}_p)$  satisfy  $x^2 = y^3$ . We are in the case where  $G = \langle x, y \rangle$  is a subgroup of the group of upper triangular invertible matrices. Then  $x^2 = y^3$  gives  $x_{11}^2 = y_{11}^3$  and since  $x_{11}, y_{11}$  are in a cyclic group, we have  $x_{11} = a^3, y_{11} = a^2$  for some  $a \in \overline{\mathbf{F}}_p^*$ . Similarly, there is  $b$  for the  $(2, 2)$ -th entries. Thus,

$$x = \begin{pmatrix} a^3 & u \\ 0 & b^3 \end{pmatrix}, \quad y = \begin{pmatrix} a^2 & v \\ 0 & b^2 \end{pmatrix}.$$

Moreover  $x^2 = y^3$  gives

$$(a^2 - ab + b^2)((a + b)u - (a^2 + ab + b^2)v) = 0.$$

From this, it is an easy exercise to conclude that either  $x^2, y^3$  are scalars (when at least one of  $a + b, a^2 - ab + b^2, a^2 + ab + b^2$  is zero) - that is,  $X^2 = Y^3 = I$  - or

$$\frac{u}{a^2 + ab + b^2} = \frac{v}{a + b}.$$

In the latter case, if this ratio is  $s$ , we have

$$x = \begin{pmatrix} a & s \\ 0 & b \end{pmatrix}^3, \quad y = \begin{pmatrix} a & s \\ 0 & b \end{pmatrix}^2.$$

From this, we can get  $C$  for  $A, B$  also.

The cases  $A_4, S_4, A_5, D_{2m} (m > 1)$  are left as exercises as it is a routine calculation.

*The problem numbered 5 will be kept open for solution one more time. Its solution will be given with the next set as that set involves a related problem.*