A Collection of Number Theory Problems for IMO camp

Phyoe Min Khant

July 7, 2024

Contents

1 Fundamentals

Well Ordering Axiom

Every non-empty set of natural numbers contains a smallest element.

Theorem 1.1 (Division Algorithm)

For every integer pair a, b, there exists distinct integer quotient and remainders, q and r, that satisfy

$$a = bq + r, 0 \leq r < b$$

Theorem 1.2 (Euclidean Algorithm)

For natural numbers a and b, $a > b$,

$$gcd(a, b) = gcd(a - kb, b)$$

where, k is a positive integer.

Corollary 1.2.1 (Finding GCD using Euclidean Algorithm)

For natural numbers a and b, $a > b$, we use division algorithm to determine a quotient and remainder q, r, such that $a = bq + r$. Then

$$gcd(a, b) = gcd(r, b).$$

We use division algorithm repeatedly

$$\begin{aligned}
a &= bq_1 + r_1 \\
b &= r_1 q_2 + r_2 \\
r_1 &= r_2 q_3 + r_3 \\
&\cdots \\
r_{n-2} &= r_{n-1} q_n + r_n \\
r_{n-1} &= r_n q_{n+1}
\end{aligned}$$

We have

$$gcd(a, b) = gcd(r_1, b) = gcd(r_1, r_2) = \cdots = gcd(r_{n-1}, r_n) = r_n$$

Theorem 1.3 (Bezout's Identity)

For natural numbers a, b, there exist $x, y \in \mathbb{Z}$ such that $ax + by = gcd(a, b)$.

Proof. Run the Euclidean Algorithm backwards.

Divisibility Rules

Let a, b, c be integers.

- The following 5 statements are equivalent.
  1. a divides b.
  2. a is a divisor of b.
  3. a is a factor of b.
  4. $a \mid b$.
  5. $a \cdot k = b$ for some integer k.
- If $c \mid a, b$, then $c \mid ax + by$ for any integers x, y. (possibly negative).
- If $a \mid b$, then either $b = 0$, or $|a| \leq |b|$.
- If $a \mid b$, and $a \mid b$, then $a = \pm b$, i.e., $|a| = |b|$.
- If a prime, $p \mid ab$, then p divides either a or b.
- *(Euclid's Lemma)* If $a \mid bc$ and $gcd(a, b) = 1$, then $a \mid c$.

Euclid's Lemma Proof. Use Bezout's Identity.

Theorem 2.1 (Fundamental Theorem of Arithmetic)

Every integer $n \geq 2$ has a unique prime factorization.

$$n = p_1^{\alpha_1} \cdots p_k^{\alpha_k}$$

where $p_1, \cdots, p_k$ are distinct primes and $\alpha_1, \cdots, \alpha_k$ are positive integers.

Proof. Both existence and uniqueness can be proved by induction.

Theorem 2.2 (GCD and LCM)

Let the prime factorizations of two integers a, b be

$$a = p_1^{e_1} p_2^{e_2} \cdots p_k^{e_k} = \prod_{i=1}^{k} p_i^{e_i} = \prod p_k^{e_k}$$

$$b = p_1^{f_1} p_2^{f_2} \cdots p_k^{f_k} = \prod_{i=1}^{k} p_i^{f_i} = \prod p_k^{f_k}$$

The exponents above can be zero and the p_i's are distinct. Then,

$$gcd(a, b) = p_1^{min(e_1, f_1)} p_2^{min(e_2, f_2)} \cdots p_k^{min(e_k, f_k)}$$

$$lcm(a, b) = p_1^{max(e_1, f_1)} p_2^{max(e_2, f_2)} \cdots p_k^{max(e_k, f_k)}$$

Corollary 2.2.1

For $a, b \in \mathbb{Z}^+$, $gcd(a, b) \cdot lcm(a, b) = ab$.

Theorem 2.3 (Number and sum of divisors)

Let $n \in \mathbb{N}$ such that its prime factorization is

$$n = p_1^{\alpha_1} \cdots p_k^{\alpha_k}$$

where $p_1, \cdots, p_k$ are distinct primes and $\alpha_1, \cdots, \alpha_k$ are positive integers.

- The number of (positive) divisors of n,

$$\tau(n) = (1 + \alpha_1)(1 + \alpha_2) \cdots (1 + \alpha_k).$$

  Note. The function $\tau(n)$ is odd if and only if n is a square.

- The sum of (positive) divisors of n,

$$\sigma(n) = \left(\prod_{\beta_1=0}^{\alpha_1} p_1^{\beta_1} \right) \cdots \left(\prod_{\beta_k=0}^{\alpha_k} p_k^{\beta_k} \right) = \left(\frac{p_1^{\alpha_1+1} - 1}{p_1 - 1} \right) \cdots \left(\frac{p_k^{\alpha_k+1} - 1}{p_k - 1} \right)$$

Congruence Rules

Let a, b, c, d, x be integers and m, n be positive integers.

- The following 3 statements are equivalent.
  1. a is congruent to b modulo m. i.e. $a \equiv b \pmod{m}$
  2. The difference between a and b is a multiple of m. i.e. $m \mid a - b$.
  3. a leaves the same remainder as b when divided by m.
- *(Reflexivity)* $a \equiv a \pmod{m}$.
- *(Transitivity)* If $a \equiv b \pmod{m}$ and $b \equiv c \pmod{m}$, then $a \equiv c \pmod{m}$.
- *(Symmetry)* If $a \equiv b \pmod{m}$, then $b \equiv a \pmod{m}$.
- *(Addition)* If $a \equiv b \pmod{m}$, and $c \equiv d \pmod{m}$, then $a + c \equiv b + d \pmod{m}$ and $a - c \equiv b - d \pmod{m}$.
- *(Multiplication)* If $a \equiv b \pmod{m}$, and $c \equiv d \pmod{m}$, then $ac \equiv bd \pmod{m}$.
- *(Exponentiation)* If $a \equiv b \pmod{m}$, then $a^n \equiv b^n \pmod{m}$.

Fermat Prime Conjecture

Pierre de Fermat (1601-1665) stated that all integers in the form $2^{2^n}+1$ are primes. About a century after Fermat's conjecture, Leonhard Euler (1707-1783) showed that this conjecture was not true. If you were Euler, how would you prove it?
(Hint: It fails at $n = 5$. Prove that $641 \mid 2^{2^5}$.)

Theorem 3.1 (Euler's Totient Theorem)

Let a, m be integers. If $gcd(a, m) = 1$, then

$$a^{\phi(m)} \equiv 1 \pmod{m}.$$

where, $\phi(m) =$ *Euler's Totient Function.*
If prime factorization of m is

$$m = p_1^{\alpha_1} \cdot p_2^{\alpha_2} \cdots p_k^{\alpha_k}.$$

Then

$$\phi(m) = m\left(1 - \frac{1}{p_1}\right)\left(1 - \frac{1}{p_2}\right)\cdots\left(1 - \frac{1}{p_k}\right)$$

Corollary 3.1.1 (Fermat's Little Theorem)

Let a be any integer relatively prime to a prime p. Then

$$a^{p-1} \equiv 1 \pmod{p}.$$

Alternatively,
Let a be any integer. Then

$$a^p \equiv a \pmod{p}.$$

Linear Congruence

- *(Inverses)* If $ax \equiv b \pmod{m}$ and $gcd(a, m) = 1$, then $x \equiv \frac{b}{a} \equiv b \cdot a^{-1} \pmod{m}$.
- *(Inverses add like fractions)* $\frac{a}{m} + \frac{b}{n} \equiv a \cdot m^{-1} + b \cdot n^{-1} \equiv ay + bx \cdot (mn)^{-1} \equiv \frac{an+bm}{mn}$.
- *(Inverses multiply like fractions)* $\frac{a}{m} \cdot \frac{b}{n} \equiv (a \cdot m^{-1}) \cdot (b \cdot n^{-1}) \equiv ab \cdot (mn)^{-1} \equiv \frac{ab}{mn}$.

2 Warm-up Problems

Problems in this section are relatively easy compared to those in the next section. These problems should be assigned as practice or homework problems rather than be discussed in class. Hence, no full solution is provided for this section. The problems are arranged in no particular order.

However, some hints and answers are put right after the problem statements. They are written in almost perfectly white so that the hints that one doesn't want to see yet are not spoiled easily to oneself.

1. (IMO 1959 P1) Prove that the fraction $\frac{21n+4}{14n+3}$ is irreducible for every natural number n.

2. (AIME 1986 P5) What is that largest positive integer n for which $n^3 + 100$ is divisible by $n + 10$?

3. (AIME 1985 P13) The numbers in the sequence $101, 104, 109, 116, \cdots$ are of the form $a_n = 100 + n^2$, where $n = 1, 2, 3, \cdots$. For each n, let d_n be the greatest common divisor of a_n and a_{n+1}. Find the maximum value of d_n as n ranges through the positive integers.

4. Prove that for all integers n, $n^2 + 3n + 5$ is not divisible by 121.
   (**Hint**: Observe that $n^2 + 3n + 5 = (n + 7)(n - 4) + 33$.)

5. Let $a > 2$ be an odd number and let n be a positive integer. Prove that a divides $1^{a^n} + 2^{a^n} + \cdots + (a - 1)^{a^n}$.

6. Prove that

$$3^{4^5} + 4^{5^6}$$

   is a product of two integers each of which is larger than 10^{2002}.
   (**Hint**: Write as $m^4 + 4n^4$.)

7. Find all positive integers a, b, c such that

$$ab + bc + ac > abc.$$

3 Problems

1. Find all positive integers n such that for all odd integers a, if $a^2 \leq n$ then $a \mid n$.

2. (1970 IMO P4) Find all positive integers n such that the set

$$\{n, n+1, n+2, n+3, n+4, n+5\}$$

can be split into two disjoint subsets such that the products of elements in these subsets are the same.

3. (1998 IMO P4) Determine all pairs (x, y) of positive integers such that $x^2y + x + y$ is divisible by $xy^2 + y + 7$.

4. (1992 IMO P1) Find all integers a, b, c with $1 < a < b < c$ such that

$$(a-1)(b-1)(c-1)$$

divides $abc - 1$.

5. (1995 Irish MO) For each integer n such that $n = p_1p_2p_3p_4$, where p_1, p_2, p_3, p_4 are distinct primes, let

$$d_1 = 1 < d_2 < d_3 < \cdots < d_{16} = n$$

be the sixteen positive integers that divide n. Prove that if $n < 1995$, then $d_9 - d_8 \neq 22$.

6. (2023 IMO P1) Determine all composite integers $n > 1$ that satisfy the following property: if $d_1, d_2, \ldots, d_k$ are all the positive divisors of n with $1 = d_1 < d_2 < \cdots < d_k = n$, then d_i divides $d_{i+1} + d_{i+2}$ for every $1 \leq i \leq k-2$.

7. (1989 Russian MO)Find the positive integers n with exactly 12 divisors $1 = d_1 < d_2 < \cdots < d_{12} = n$ such that the divisor with index $d_4 - 1$ (that is, d_{d_4-1}) is $(d_1 + d_2 + d_4)d_8$.

8. (2002 Romanian MO)Let p, q be distinct primes. Prove that there are positive integers a, b such that the arithmetic mean of all the divisors of the number $n = p^a \cdot q^b$ is also an integer.

9. (1969 IMO P1) Prove that there are infinitely many natural numbers a with the following property: the number $z = n^4 + a$ is not prime for any natural number n.

10. (2001 IMO P6) $a > b > c > d$ are positive integers such that

$$ac + bd = (b + d + a - c)(b + d - a + c).$$

Prove that $ab + cd$ is not prime.

11. (1984 IMO P6) Let a, b, c, d be odd integers such that $0 < a < b < c < d$ and $ad = bc$. Prove that if $a + d = 2^k$ and $b + c = 2^m$ for some integers k and m, then $a = 1$.

12. (1996 Spanish MO) The natural numbers a and b are such that

$$\frac{a+1}{b} + \frac{b+1}{a}$$

is an integer. Show that the greatest common divisor of a and b is not greater that $\sqrt{a+b}$.

13. (1999 Iranian MO) Supposes that n is a positive integer and let

$$d_1 < d_2 < d_3 < d_4$$

be the four smallest positive integer divisors of n. Find all integers n such that

$$n = d_1^2 + d_2^2 + d_3^2 + d_4^2.$$

14. (1999 St. Petersburg City MO) How many 10-digit numbers divisible by 66667 are there whose decimal representation contains only the digits 3, 4, 5 and 6?

15. (2002 Romanian TST for JBMO) The last four digits of a perfect square are equal. Prove they are all zero.

16. (1997 Irish MO) Let A be a subset of $\{0, 1, \cdots 1997\}$ containing more than 1000 elements. Prove that A contains either a power of 2, or two distinct integers whose sum is a power of 2.

17. (1998 Balkan MO) Find the number of different terms of the finite sequence $\lfloor \frac{k^2}{1998} \rfloor$, where $k = 1, 2, \cdots 1997$.

18. (1995 Austrian MO) For how many (a) even and (b) odd numbers n does n divide $3^{12} - 1$, yet n does not divide $3^k - 1$ for $k = 1, 2, \cdots, 11$?

19. (1996 Bulgarian MO) Prove that for all integers $n \geq 3$, there exist odd positive integers x, y such that

$$7x^2 + y^2 = 2^n.$$

20. (2023 IMO Shortlist2) Determine all pairs (a, p) of positive integers with p prime such that $p^a + a^4$ is a perfect square.

4 Solutions

Please feel free to contact the author if you find any typo or error in the solutions or if you have any question.

Problem 1.

Find all positive integers n such that for all odd integers a, if $a^2 \leq n$ then $a \mid n$.

Solution. Consider a fixed positive integer n. Let a be the greatest odd integer such that $a^2 < n$ and hence $n \leq (a+2)^2$. If $a \geq 7$, then $a-4, a-2, a$ are odd integers that divide n. Note that any two of these numbers are relatively prime, so $(a-4)(a-2)(a)$ divides n. It follows that $(a-4)(a-2)a \leq (a+2)^2$, so $a^3 - 6a^2 + 8a \leq a^2 + 4a + 4$. Then $a^3 - 7a^2 + 4a - 4 \leq 0$ or $a^2(a-7) + 4(a-1) \leq 0$. This is false because $a \geq 7$; hence $a = 1, 3$, or 5.

If $a = 1$, then $1^2 \leq n \leq 3^2$, so $n \in \{1, 2, \cdots, 8\}$.

If If $a = 3$, then $3^2 \leq n \leq 5^2$, and $1 \cdot 3 \mid n$, so $n \in \{9, 12, 15, 18, 21, 24\}$.

If If $a = 5$, then $5^2 \leq n \leq 7^2$, and $1 \cdot 3 \cdot 5 \mid n$, so $n \in \{30, 45\}$. Therefore, $n \in \{1, 2, 3, 4, 5, 6, 7, 8, 9, 12, 15, 18, 21, 24, 30, 45\}$. $\square$

Problem 2. (1970 IMO P4)

Find all positive integers n such that the set

$$\{n, n+1, n+2, n+3, n+4, n+5\}$$

can be split into two disjoint subsets such that the products of elements in these subsets are the same.

Solution. At least one of six consecutive numbers is divisible by 5. From the given condition, it follows that two numbers must be divisible by 5. These two numbers are necessarily n and $n+5$. Therefore n and $n+5$ are in distinct subsets. Since $n(n+1) > n+5$ for $n \geq 3$, it follows that a required partition cannot be considered with subsets of different cardinality. For same cardinality, the biggest value you can make with the n subset is $n(n+4)(n+3) = n^3+7n^2+12n$ which is smaller than $(n+1)(n+2)(n+5) = n^3 + 8n^2 + 17n + 10$. So, there is no such integer n. $\square$

Problem 3. (1998 IMO P4)

Determine all pairs (x, y) of positive integers such that x^2y+x+y is divisible by xy^2+y+7.

Solution. $\square$

Problem 4. (1992 IMO P1)

Find all integers a, b, c with $1 < a < b < c$ such that

$$(a-1)(b-1)(c-1)$$

divides $abc - 1$.

Solution. □

Problem 5. (1995 Irish MO)

For each integer n such that $n = p_1p_2p_3p_4$, where p_1, p_2, p_3, p_4 are distinct primes, let

$$d_1 = 1 < d_2 < d_3 < \cdots < d_{16} = n$$

be the sixteen positive integers that divide n. Prove that if $n < 1995$, then $d_9 - d_8 \neq 22$.

Solution. □

Problem 6. (2023 IMO P1)

Determine all composite integers $n > 1$ that satisfy the following property: if $d_1, d_2, \ldots, d_k$ are all the positive divisors of n with $1 = d_1 < d_2 < \cdots < d_k = n$, then d_i divides $d_{i+1} + d_{i+2}$ for every $1 \leq i \leq k-2$.

Solution. □

Problem 7. (1989 Russian MO)

Find the positive integers n with exactly 12 divisors $1 = d_1 < d_2 < \cdots < d_{12} = n$ such that the divisor with index $d_4 - 1$ (that is, d_{d_4-1}) is $(d_1 + d_2 + d_4)d_8$.

Solution. Let $d_i = d_1 + d_2 + d_4$ where $1 \leq i \leq 12$. We will prove that $i = 5$. Since $d_i > d_4$, we have $i \geq 5$. Also, observe that $d_jd_{13-j} = n$ for all j and since $d_id_8 = d_{d_4-1} \leq n$,, we must have $i \leq 5$., thus $i = 5$ and $d_1 + d_2 + d_4 = d_5$. Also, $d_{d_4-1} = d_5d_8 = n = d_12$, thus $d_4 = 12$ and $d_5 = 14 + d_2$.. Of course, d_2 is the smallest prime divisor of n, and since $d_4 = 13$, we can only have $d_2 \in \{2, 3, 5, 7, 11\}$. Also, since n has 12 divisors, it has at most 3 prime divisors. If $d_2 = 2$ then $d_5 = 16$ and then 4 and 8 are divisors of n smaller than $d_4 = 13$,, impossible. A similar argument shows that $d_2 = 3$ and $d_5 = 17$. Since n has 12 divisors and is a multiple of $3 \cdot 13 \cdot 17$, the only possibilities are $9 \cdot 13 \cdot 17, 3 \cdot 169 \cdot 17, 3 \cdot 13 \cdot 289$. One can easily check that only $9 \cdot 13 \cdot 17 = 1989$ is a solution. □

Problem 8. (2002 Romanian MO)

Let p, q be distinct primes. Prove that there are positive integers a, b such that the arithmetic mean of all the divisors of the number $n = p^a \cdot q^b$ is also an integer.

Solution. The sum of all divisors of n is given by the formula

$$(1 + p + p^2 + \cdots + p^a)(1 + q + q^2 + \cdots + q^b),$$

The number n has $(a + 1)(b + 1)$ positive divisors and their arithmetic mean is

$$M = \frac{(1 + p + p^2 + \cdots + p^a)(1 + q + q^2 + \cdots + q^b)}{(a + 1)(b + 1)}.$$

If p and q are both odd, we can take $a = p$ and $b = q$, and it is easy to see that M is an integer because $1 + p + p^2 + \cdots + p^a \equiv 1 - 1 + 1 - 1 \cdots - 1 = 0 \pmod{p+1}$. If $p = 2$ and q odd, taking b as q, M becomes

$$M = \frac{(1 + p + p^2 + \cdots + p^a)(1 + q^2 + \cdots + q^{b-1})}{(a + 1)}.$$

If we take a as $q^2 + \cdots + q^{b-1}$, then M is an integer. □

Problem 9. (1969 IMO P1)

Prove that there are infinitely many natural numbers a with the following property: the number $z = n^4 + a$ is not prime for any natural number n.

Solution. □

Problem 10. (2001 IMO P6)

$a > b > c > d$ are positive integers such that

$$ac + bd = (b + d + a - c)(b + d - a + c).$$

Prove that $ab + cd$ is not prime.

Solution. The given equality is equivalent to $a^2 - ac + c^2 = b^2 + bd + d^2$. Since

$$(ab + cd)(ad + bc) = ac(b^2 + bd + d^2) + bd(a^2 - ac + c^2),$$

that is,

$$(ab + cd)(ad + bc) = (ac + bd)(a^2 - ac + c^2).$$

Again, it follows from $a > b > c > d$ that $ab + cd - ac - bd = (a - d)(b - c) > 0$ and $ac + bd - ad - bc = (a - b)(c - d) > 0$. Therefore,

$$ab + cd > ac + bd > ad + bc;$$

Suppose $ab + cd$ is a prime, then $ac + bd$ is relatively prime to $ab + cd$. But then, in the first equation implies that $ac + bd$ divides $ad + bc$ which is impossible due to the inequality. □

Problem 11. (1984 IMO P6)

Let a, b, c, d be odd integers such that $0 < a < b < c < d$ and $ad = bc$. Prove that if $a + d = 2^k$ and $b + c = 2^m$ for some integers k and m, then $a = 1$.

Solution. Since $ad = bc$, we have

$$a((a + d) - (b + c)) = (a - b)(a - c) > 0.$$

Thus, we have $a + d > b + c, 2^k > 2^m$, and $k > m$. Since $ad = a(2^k - a) = bc = b(2^m - b)$, we obtain $2^m b - 2^k a = b^2 - a^2 = (b - a)(b + a)$. By the equality $2^m(b - 2^{k-m}a) = (b - a)(b + a)$, we infer that $2^m \mid (b - a)(b + a)$. But $b - a$ and $b + a$ differ by $2a$, an odd multiple of 2, so either $b - a$ or $b + a$ is not divisible by 4. Hence, either $2^{m-1} \mid b - a$ or $2^{m-1} \mid b + a$. But $0 < b - a < b < 2^{m-1}$, so it must be that $2^{m-1} \mid b + a$.

Since $0 < b + a < b + c = 2^m$, it follows that $b + a = 2^{m-1}$. That is, $2(a + b) = 2^m = b + c$. Thus, $c = 2a + b$. Furthermore, $\gcd(b, c) = 1$ because both of them are odd and from $b + c = 2^m$, $\gcd(b, c) \mid 2^{m-1}$. If $\gcd(a, b) = k, k \mid c$. Then $k \mid b, c$; but $gcd(b, c) = 1$. Therefore, $k = 1$ and $gcd(a, b) = 1$. Similarly, it can be proved that $gcd(a, c) = 1$. Combining with $ad = bc, a = 1$. $\square$

Problem 12. (1996 Spanish MO)

The natural numbers a and b are such that

$$\frac{a+1}{b} + \frac{b+1}{a}$$

is an integer. Show that the greatest common divisor of a and b is not greater that $\sqrt{a + b}$.

Solution. Let $d = \gcd(a, b)$. Adding 2, we see that

$$\frac{a+1}{b} + \frac{b+1}{a} + 2 = \frac{(a + b)(a + b + 1)}{ab}$$

is an integer. Since d^2 divides the denominator and $gcd(d, a+b+1) = 1$, we must have $d^2 \mid a+b$; hence $d \leq \sqrt{a + b}$. $\square$

Problem 13. (1999 Iranian MO)

Supposes that n is a positive integer and let

$$d_1 < d_2 < d_3 < d_4$$

be the four smallest positive integer divisors of n. Find all integers n such that

$$n = d_1^2 + d_2^2 + d_3^2 + d_4^2.$$

Solution. The answer is $n = 130$. Note that $x^2 \equiv 0 \pmod 4$ when x is even and $x^2 \equiv 1 \pmod 4$ when x is odd.

If n is odd, then all the d_i are odd and $n \equiv d_1^2 + d_2^2 + d_3^2 + d_4^2 \equiv 1 + 1 + 1 + 1 \equiv 0 \pmod 4$, a contradiction. Thus, $2 \mid n$.

If $4 \mid n$ then $d_1 = 1$ and $d_2 = 2$, and $n \equiv 1 + 0 + d_3^2 + d_4^2 \not\equiv 0 \pmod 4$, a contradiction. Thus, $4 \nmid n$.

Therefore $\{d_1, d_2, d_3, d_4\} = \{1, 2, p, q\}$ or $\{1, 2, p, 2p\}$ for some odd primes p, q. In the first case, $n \equiv 3 \pmod 4$, a contradiction. Thus $n \equiv 5(1 + p^2)$ and $5 \mid n$, so $p = d_3 = 5$ and $n = 130$. $\square$

Problem 14. (1999 St. Petersburg City MO)

How many 10-digit numbers divisible by 66667 are there whose decimal representation contains only the digits 3, 4, 5 and 6?

Solution. Suppose that $66667n$ has 10 digits, all of which are 3,4,5, and 6. Then

$$3333333333 \le 66667n \le 6666666666 \implies 50000 \le n \le 99999.$$

We will consider for $n = 3k, 3k + 1$ and $3k + 2$.

When $n = 3k$, then $16667 \le k \le 33333$,

$$66667n = (10^5 - 33333)(3k) = (3 \times 10^5 - 99999)k = 2k \times 10^5 + k,$$

the five digits of $2k$ followed by the five digits of k. These digits are all 3, 4, 5 or 6 if an only if $k = 33333$.

When $n = 3k + 1$, then $16666 \le k \le 33332$,

$$66667n = (10^5 - 33333)(3k + 1) = (3 \times 10^5 - 99999)k + 10^5 - 33333 = 2k \times 10^5 + k + 66667,$$

the five digits of $2k$ followed by the five digits of $k + 66667$. Since $k + 66667$ is greater than 66666 and less than 99999, there are no satisfactory values.

When $n = 3k + 2$, then $16666 \le k \le 33332$,

$$66667n = (10^5 - 33333)(3k + 2) = (3 \times 10^5 - 99999)k + 2 \times 10^5 - 66666 = (2k + 1) \times 10^5 + k + 33334,$$

the five digits of $2k + 1$ followed by the five digits of $k + 33334$. For both $2k + 1$ and $k + 33334$ to have only 3,4,5 or 6, firstly the unit digit must be only 1 or 2. The same condition is required for the preceding four digits. So there are $2^5 = 32$ numbers of k. In total, there are 33 numbers. $\square$

Problem 15. (2002 Romanian TST for JBMO)

The last four digits of a perfect square are equal. Prove they are all zero.

Solution. Denote the perfect square by k^2 and the digit that appears in the last four positions by a. It is easy to see that a is one of the numbers from $0, 1, 4, 5, 6, 9$.

When $a = 1, 5, 6$ or 9, $k^2 \not\equiv 0$ or $1 \pmod 4$, looking at the remainders when 11, 55, 66, 99 are divided by 4, a contradiction.

When $a = 4$, $k^2 \equiv 12 \pmod{16}$, which is a contradiction since $k^2 \equiv 0, 1, 4, 9 \pmod{16}$. Thus a must be zero. $\square$

Problem 16. (1996 Bulgarian MO)

Prove that for all integers $n \geq 3$, there exist odd positive integers x, y such that

$$7x^2 + y^2 = 2^n.$$

Solution. We will prove by induction. For $n = 3$, we have $x_3 = y_3 = 1$. Let there exist odd positive integers x, y satisfying $7x^2 + y^2 = 2^k$ with $k \geq 3$. We will prove that there exist odd positive integers a, b such that $7a^2 + b^2 = 2^{k+1}$.

$$2^{k+1} = 2(7x^2 + y^2) = 7\left(\left(\frac{x}{2}\right)^2 + \left(\frac{y}{2}\right)^2\right) + \left(\frac{7x}{2}\right)^2 + \left(\frac{y}{2}\right)^2 = 7\left(\frac{x \pm y}{2}\right)^2 + \left(\frac{7x \mp y}{2}\right)^2$$

Since x and y are odd, they can be expressed with integers x_1 and y_1 as $2x_1 + 1$ and $2y_1 + 1$ respectively. When both of x_1 and y_1 are odd or both are even,

$$\frac{x+y}{2} = x_1 + y_1 + 1 = odd, \frac{7x-y}{2} = 3x - \frac{x-y}{2} = 3x - (a-b) = odd$$

When one of x_1 and y_1 is even and the other is odd,

$$\frac{x-y}{2} = x_1 - y_1 = odd, \frac{7x+y}{2} = 3x + \frac{x+y}{2} = 3x + (a+b+1) = odd.$$

$\square$

Problem 17. (2023 IMO Shortlist2)

Determine all pairs (a, p) of positive integers with p prime such that $p^a + a^4$ is a perfect square.

Solution. Let $p^a + a^4 = b^2$ for some positive integer b. Then we have

$$p^a = b^2 - a^4 = (b + a^2)(b - a^2).$$

Hence both $b + a^2$ and $b - a^2$ are powers of p. Let $b + a^2 = p^x$ and $b - a^2 = p^y$ for some integers x and y such that $x + y = a$ and $x > y$.

$$2a^2 = (b + a^2) - (b - a^2) = p^x - p^y = p^y(p^{x-y} - 1).$$

Case 1. $p = 2$: In this case,

$$a^2 = 2^{y-1}(2^{x-y} - 1).$$

If y is even, a^2 will never be a perfect square as $\gcd(2, 2^{x-y}-1) = 1$.

If y is an odd number greater than 1, a will be even because $2^{y-1} \mid a^2$. Since $x+y = a$, x will be odd. Let $x-y = odd - odd = 2k$ for some integer k. Therefore $2^{x-y}-1 = 2^{2k}-1 = 4^k - 1 \equiv 3 \pmod 4$, thus cannot be a perfect square. This contradicts that $2^{x-y}-1$ must be a perfect square as 2^{y-1} is a perfect square.

If $y = 1$, $a^2 = 2^{x-1} - 1 = 2^{a-2} - 1$. The inequality $a^2 < 2^{a-2} - 1$ holds true for $a > 9$ and can be proved by induction: $(k+1)^2 = k^2 + 2k + 1 < 2^{k-2} + 2k + 1 < 2 \cdot 2^{k-2} - 1 = 2^{k-1} - 1$. By manual checking, there is no solution for $a \le 9$

Case 1. $p = 2$ **(Alternative way)** : In this case,

$$a^2 = 2^{y-1}(2^{a-2y} - 1) = 2^{2v_2(a)}(2^{a-2y} - 1),$$

where the the second equality comes from $\gcd(2, 2^{a-2y}-1) = 1$. So $2^{a-2y}-1$ is a square.

If $v_2(a) > 0$, then 2^{a-2y} is also a square. So, $2^{a-2y}-1 = 0$ and $a = 0$ which is a contradiction.

If $v_2(a) = 0$, then $x = 1$, and $a^2 = 2^{a-2} - 1$. If $a \ge 4$, the right hand side is congruent to 3 modulo 4, thus cannot be a square. It is easy to see that $a = 1, 2, 3$ do not satisfy this condition.

Therefore, we do not get any solutions in this case.

Case 2. $p \ne 2$: Both $b + a^2$ and $b - a^2$ are powers of p, so $b - a^2 \mid b + a^2 = b - a^2 + 2a^2$ and thus $b - a^2 \mid 2a^2$. Since $\gcd(2, b - a^2) = 1$, $b - a^2 \mid a^2$.

Therefore, $b - a^2 \le a^2$ and $b \le 2a^2$. This leads to $p^x = a^2 + b \le 3a^2$ and $p^y = p^x - 2a^2 \le a^2$. Multiplying them, $p^a = p^x \cdot p^y \le 3a^4$.

Subcase 2.1 $p \ge 7$: We will prove that the inequality $p^a \le 3a^4$ does not hold true for $p \ge 7$ by induction. It is obvious that the base case for $a \le 3$ holds true for $7^a > 3a^4$. For $a \ge 4$, $p^{a+1} \ge 7^{a+1} > 5 \cdot 7^a \ge 3a^4 + 3a^4 + 3a^4 + 3a^4 + 3a^4 \ge 3a^4 + 12a^3 + 18a^2 + 12a + 3 = 3(a+1)^4$.

Subcase 2.2 $p = 3$ **or** 5 : It is easy to prove that the inequality $3^a > 3a^4$ holds true for $a > 9$ by induction. Checking $p = 3, a \le 9$, $(p, a) = (3,1), (3,2), (3,6), (3,9)$ are the solutions. Similarly, $5^a > 5a^4$ for $a > 4$ can be proved by induction. By checking $p = 5, a \le 4$,, there is no solution in this case.

Case 2. $p \ne 2$ **(Alternative way)** : In this case, we have $2v_p(a) = y$. Let $m = v_p(a)$. Then we have $a^2 = p^{2m} \cdot n^2$ for some integer $n \ge 1$ where $gcd(p, n) = 1$. So, $2a^2 = 2p^{2m} \cdot n^2 = p^y(p^{x-y} - 1)$ and from this $2n^2 = p^{x-y} - 1 = p^{a-2y} - 1 = p^{p^m \cdot n - 4m} - 1$.

We consider two subcases.

Subcase 2.1 $p \ge 5$ By induction, one can easily prove that $p^m \ge 5^m > 4m$ for all m. Then we have

$$2n^2 + 1 = p^{p^m \cdot n - 4m} > p^{p^m \cdot n - p^m} \ge 5^{5^m \cdot (n-1)} \ge 5^{n-1}.$$

But by induction, one can easily prove that $5^{n-1} > 2n^2 + 1$ for all $n \ge 3$. Therefore, we conclude that $n = 1$ or 2. If $n = 1$ or 2, then $p = 3$, which is a contradiction. So there are no solutions in this subcase.

Subcase 2.2 $p = 3$: Then we have $2n^2 + 1 = 3^{3^m \cdot n - 4m}$. If $m \ge 2$, one can easily prove by induction that $3^m > 4m$. Then we have

$$2n^2 + 1 = 3^{3^m \cdot n - 4m} > 3^{3^m \cdot n - 3^m} = 3^{3^m \cdot (n-1)} \ge 3^{9(n-1)}.$$

Again, by induction, one can easily prove that $3^{9(n-1)} > 2n^2 + 1$ for all $n \geq 2$. Therefore, we conclude that $n = 1$. Then we have $2 \cdot 1^2 + 1 = 3^{3^m - 4m}$. Consequently we have $3^m - 4m = 1$. The only solution of this equation is $m = 2$ in which case we have $a = 3^m \cdot n = 3^2 \cdot 1 = 9$.

If $m \leq 1$, there are two possible cases $m = 0$ or $m = 1$.

If $m = 1$, then we have $2n^2 + 1 = 3^{3n-4}$. Again by induction, one can easily prove that $3^{3n-4} > 2n^2 + 1$ for all $n \geq 3$. By checking $n = 1, 2$, we only get $n = 2$ as a solution. This give $a = 3^m \cdot n = 3^1 \cdot 2 = 6$.

If $m = 0$, then we have $2n^2 + 1 = 3^n$. By induction, one can easily prove that $3^n > 2n^2 + 1$ for all $n \geq 3$. By checking $n = 1, 2$, we find the solutions $a = 3^0 \cdot 1 = 1$ and $a = 3^0 \cdot 2 = 2$.

Therefore, $a, p = (1, 3), (2, 3), (6, 3), (9, 3)$ are all the possible solutions. □