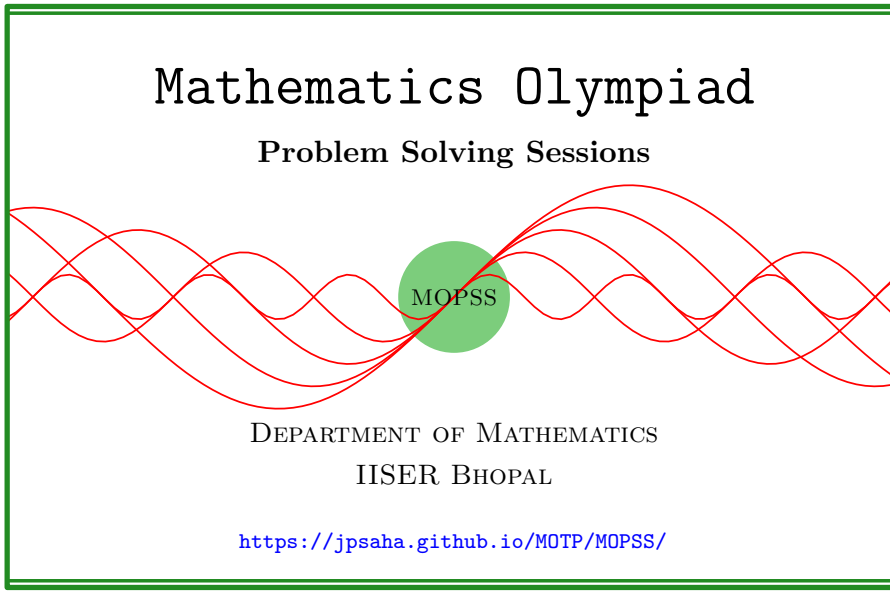
Congruences

MOPSS

3 June 2025



Suggested readings

- Evan Chen's advice On reading solutions, available at https://blog.evanchen.cc/2017/03/06/on-reading-solutions/.
- Evan Chen's Advice for writing proofs/Remarks on English, available at https://web.evanchen.cc/handouts/english/english.pdf.
- Notes on proofs by Evan Chen from OTIS Excerpts [**Che25**, Chapter 1].
- Tips for writing up solutions by Edward Barbeau, available at https://www.math.utoronto.ca/barbeau/writingup.pdf.
- Evan Chen discusses why math olympiads are a valuable experience for high schoolers in the post on Lessons from math olympiads, available at https://blog.evanchen.cc/2018/01/05/lessons-from-math-olympiads/.

List of problems and examples

1.1 Example . . . 3
1.2 Example (Tournament of Towns, Fall 2019, Junior, O Level, P4 by Boris Frenkin) . . . 3
1.3 Example . . . 4
1.4 Example (Australian MO 1982, India RMO 2004 P6) . . . 4
1.5 Example (Moscow MO 1973 Day 1 Grade 8 P4) . . . 5
1.6 Example (cf. Moscow MO 1973 Day 1 Grade 8 P4 **??**) . . . 5
1.7 Example (India INMO 1991 P10, cf. Moscow MO 1973 Day 1 Grade 8 P4 **??**) . . . 5
1.8 Example (India RMO 1992 P2, cf. Moscow MO 1973 Day 1 Grade 8 P4 **??**) . . . 6
1.9 Example (UK BMO 2005 Round 2 P1, cf. Moscow MO 1973 Day 1 Grade 8 P4 **??**) . . . 7
1.10 Example (All-Russian MO 1989 Day 2 Grade 8 P5) . . . 7
1.11 Example (India RMO 1991 P7, cf. All-Russian MO 1989 Day 2 Grade 8 P5 **??**, India BStat 2006 P3) . . . 7
1.12 Example (India INMO 1991 P1) . . . 7
1.13 Example (India RMO 1991 P3) . . . 8
1.14 Example (All-Russian MO 1992–1993 Final Stage Grade 09 P1, India RMO 2011b P2) . . . 8
1.15 Example (India RMO 1994 P5) . . . 9
1.16 Example (India RMO 1994 P3) . . . 10
1.17 Example (Tournament of Towns, India RMO 1995 P3) . . . 10
1.18 Example (China TST 1995 Day 1 P1) . . . 10
1.19 Example (India RMO 1995 P2) . . . 11
1.20 Example (India RMO 1996 P4) . . . 12
1.21 Example (India RMO 1997 P2) . . . 12
1.22 Example (India RMO 1998 P5) . . . 14
1.23 Example (India RMO 1998 P2) . . . 14
1.24 Example (India RMO 1999 P2) . . . 15
1.25 Example (Bay Area MO 1999 P1) . . . 15
1.26 Example (Bay Area MO 2000 P1) . . . 15
1.27 Example (India RMO 2000 P6) . . . 16
1.28 Example (India RMO 2001 P7) . . . 16
1.29 Example (India RMO 2002 P3, India RMO 2012d P2, India RMO 2012a P2, India RMO 2012b P2, India RMO 2012c P2) 17
1.30 Example (India RMO 2003 P2) . . . 18
1.31 Example (India RMO 2005 P2) . . . 19
1.32 Example (India RMO 2006 P2) . . . 19
1.33 Example (India BMath 2007 P1) . . . 21
1.34 Example (India RMO 2009 P3) . . . 21
1.35 Example (India RMO 2011a P3) . . . 21
1.36 Example (India Pre-RMO 2012) . . . 22

1.37 Example (India RMO 2012f P2) . . . 22
1.38 Example (India RMO 2012e P6) . . . 22
1.39 Example (India RMO 2013d P2) . . . 23
1.40 Example (India RMO 2013e P5) . . . 23
1.41 Example (India RMO 2014c P3) . . . 24
1.42 Example (India RMO 2014b P3) . . . 25
1.43 Example (India RMO 2014b P4) . . . 25
1.44 Example (India RMO 2014d P3) . . . 26
1.45 Example (India RMO 2016d P3) . . . 26
1.46 Example (India RMO 2016c P3) . . . 28
1.47 Example (India RMO 2016g P3) . . . 28
1.48 Example (India RMO 2016g P6) . . . 29
1.49 Example (India RMO 2016e P2) . . . 30
1.50 Example (India RMO 2017a P2) . . . 32
1.51 Example (India RMO 2017b P2) . . . 33
1.52 Example (India RMO 2018a P5) . . . 34
1.53 Example (India RMO 2018a P3) . . . 35
1.54 Example (India RMO 2019b P1) . . . 36
1.55 Example (India RMO 2023a P2) . . . 37
1.56 Example (India RMO 2023b P1) . . . 38
1.57 Example (India RMO 2024a P1) . . . 38
1.58 Example (India RMO 2024a P4) . . . 39
1.59 Example (India RMO 2024b P1) . . . 41
1.60 Example (India RMO 2024b P2) . . . 42
1.61 Example . . . 43
1.62 Example (IMOSL 1984 P2) . . . 44
1.63 Example (India RMO 1990 P4) . . . 44
1.64 Example (India RMO 1990 P6) . . . 45
1.65 Example (India RMO 1993 P5) . . . 45
1.66 Example (India RMO 2015f P3) . . . 46

§1 Congruences

§1.1 Warm up

Example 1.1. Among any four consecutive positive integers, one of them is coprime to the remaining three.

Proof. Note that among any four consecutive positive integers, at least one of the odd integers is not divisible by 3, and hence, either it is equal to 1, in which case it is coprime to the remaining ones, or it is greater than one, and its smallest prime factor is at least 5, and hence, it is coprime to the remaining ones. □

Example 1.2 (Tournament of Towns, Fall 2019, Junior, O Level, P4 by Boris Frenkin)**.** There are given 1000 integers $a_1, \ldots, a_{1000}$. Their squares $a_1^2, \ldots, a_{1000}^2$ are written along the circumference of a circle. It so happened that the sum of any 41 consecutive numbers on this circle is a multiple of 41^2. Is it necessarily true that every integer $a_1, \ldots, a_{1000}$ is a multiple of 41?

Solution 1. For any integer m, let $\overline{m}$ denote the integer lying between 1 and 1000, which is congruent to m modulo 1000. Note that

$$a_i^2 \equiv a_j^2 \bmod 41^2$$

holds for any integers i, j lying between 1 and 1000, and satisfying $i \equiv j \bmod 41$. It follows that

$$a_1^2 \equiv a_{\overline{41k+1}}^2 \bmod 41^2$$

for any integer k. Since the integers $41, 1000$ are relatively prime, it follows that the integers

$$41, 41 \cdot 2, 41 \cdot 3, \ldots, 41 \cdot 1000$$

are pairwise distinct modulo 1000, that is, these integers are congruence to $1, 2, \ldots, 1000$ modulo 1000 in some order. This shows that a_1^2 is congruent to a_i^2 for any integer $1 \leq i \leq 1000$. It follows that

$$41a_1^2 = a_1^2 + a_2^2 + \cdots + a_{41}^2$$

is divisible by 41^2, and hence, 41 divides a_1. For any integer $1 \leq i \leq 1000$, 41^2 divides $a_1^2 - a_i^2$, and using that 41 divides a_1, we obtain 41 divides a_i.

This proves that it is necessary that every integer $a_1, \ldots, a_{1000}$ is a multiple of 41. ■

Example 1.3. [FGI96, Problem 83, p. 72] Prove that if a prime number is divided by 30, the remainder is prime or 1.

Solution 2. Let p be a prime number. If p is less than 5, then we are done. Henceforth, let us assume that $p \geq 5$. It follows that p is of the form $6k \pm 1$ for some positive integer k. If $k \equiv 1 \pmod 5$, then p is equivalent to one of $5, 7$ modulo 30. If $k \equiv 2 \pmod 5$, then p is equivalent to one of $1, 3$ modulo 30. If $k \equiv 3 \pmod 5$, then p is equivalent to 2 modulo 30. If $k \equiv 4 \pmod 5$, then p is equivalent to one of $3, 5$ modulo 30. This completes the proof. ■

Example 1.4 (Australian MO 1982, India RMO 2004 P6)**.** Let $(p_1, p_2, p_3, \ldots, p_n, \ldots)$ be a sequence of primes, defined by $p_1 = 2$ and for $n \geq 1$, p_{n+1} is the largest prime factor of $p_1 p_2 \cdots p_n + 1$. Prove that $p_n \neq 5$ for any n.

Solution 3. Note that $p_1 p_2 \ldots p_n + 1$ is odd for any $n \geq 1$, and hence p_n is odd for any $n \geq 2$. Since $p_1 = 2$ and $p_2 = 3$, it follows that for any $n \geq 2$, the

integer $p_1p_2 \dots p_n + 1$ is not divisible by any one of 2 and 3. So the least prime divisor of $p_1p_2 \dots p_n + 1$ is at least 5 for any $n \geq 2$. If possible, suppose 5 is the largest prime divisor of $p_1p_2 \dots p_n + 1$ for some integer $n \geq 2$. This yields

$$p_1p_2 \dots p_n + 1 = 5^k$$

for some $k \geq 1$. This implies that 4 divides $p_1p_2 \cdots p_n$, which is impossible since $p_1 = 2$, and p_r is odd for any integer $r \geq 2$. This shows that p_{n+1} is not equal to 5 for any integer $n \geq 2$. Consequently, it follows that $p_n \neq 5$ for any integer $n \geq 1$. ■

Example 1.5 (Moscow MO 1973 Day 1 Grade 8 P4)**.** Prove that the equation

$$\frac{1}{x} + \frac{1}{y} = \frac{1}{p},$$

where x, y are positive integers, has exactly 3 solutions if p is a prime and the number of solutions is greater than three if $p > 1$ is not a prime. We consider solutions (a, b) and (b, a) for $a \neq b$ distinct.

Example 1.6 (cf. Moscow MO 1973 Day 1 Grade 8 P4 **??**)**.** For any positive integer n, show that the number of ordered pairs (x, y) of positive integers for which

$$\frac{1}{x} + \frac{1}{y} = \frac{1}{n}$$

is equal to the number of positive divisors of n^2.

Solution 4. For positive integers x, y, note that

$$\frac{1}{x} + \frac{1}{y} = \frac{1}{n}$$

holds if and only if

$$(x - n)(y - n) = n^2$$

holds. Observe that if x, y are positive integers satisfying the given equation, then $x > n$ and $y > n$ holds. This shows that the solutions of the given equation over the positive integers are in one-to-one correspondence with pairs of positive integers (a, b) such that $ab = n^2$, through the map

$$(a + n, b + n) \leftrightarrow (a, b).$$

This completes the proof. ■

Example 1.7 (India INMO 1991 P10, cf. Moscow MO 1973 Day 1 Grade 8 P4 **??**)**.** For any positive integer n, let $S(n)$ denote the number of ordered pairs (x, y) of positive integers for which

$$\frac{1}{x} + \frac{1}{y} = \frac{1}{n}$$

(for instance, $S(2) = 3$). Determine the set of positive integers n for which $S(n) = 5$.

Solution 5. For positive integers x, y, note that

$$\frac{1}{x} + \frac{1}{y} = \frac{1}{n}$$

holds if and only if

$$(x - n)(y - n) = n^2$$

holds. Observe that if x, y are positive integers satisfying the given equation, then $x > n$ and $y > n$ holds. This shows that the solutions of the given equation over the positive integers are in one-to-one correspondence with pairs of positive integers (a, b) such that $ab = n^2$, through the map

$$(a + n, b + n) \leftrightarrow (a, b).$$

Hence, the set of positive integers n satisfying $S(n) = 5$ is equal to the set of positive integers n such that n^2 has precisely 5 positive divisors. Note that any such integer n is larger than 1. Writing n as a product of powers of distinct primes, it follows that n^2 has precisely 5 positive divisors if and only if n is the square a prime. Indeed, if $p_1, \ldots, p_r$ are distinct primes, and $a_1, \ldots, a_r$ are positive integers, then the integer $(p_1^{a_1} \ldots p_r^{a_r})^2$ has precisely 5 positive divisors if and only if

$$(2a_1 + 1)(2a_2 + 1) \ldots (2a_r + 1) = 5$$

holds, which is equivalent to $r = 1, a_1 = 2$. This proves that the positive integers satisfying $S(n) = 5$ are precisely the squares of the primes. ■

Example 1.8 (India RMO 1992 P2, cf. Moscow MO 1973 Day 1 Grade 8 P4 **??**). If $\frac{1}{a} + \frac{1}{b} = \frac{1}{c}$, where a, b, c are positive integers with no common factor, prove that $(a + b)$ is the square of an integer.

Solution 6. Let a, b, c be positive integers satisfying the given equation. Assume that a, b have no common prime factors. Note that $(a - c)(b - c) = c^2$ holds. Also note that any common prime divisor of $a - c, b - c$ divides $(a - c)(b - c) = c^2$, and hence it divides the integers a, b, which is impossible. This shows that the integers $a - c, b - c$ are relatively prime, and satisfy $(a - c)(b - c) = c^2$. Note also that $a > c$ holds. Hence, there exist relatively prime positive integers x, y such that $c = xy$, $a - c = x^2$ and $b - c = y^2$ holds. This gives

$$a = c + x^2 = xy + x^2, \quad b = c + y^2 = xy + y^2.$$

This implies that $a + b$ is a perfect square. ■

Example 1.9 (UK BMO 2005 Round 2 P1, cf. Moscow MO 1973 Day 1 Grade 8 P4 **??**)**.** The integer N is positive. There are exactly 2005 ordered pairs (x, y) of positive integers satisfying

$$\frac{1}{x} + \frac{1}{y} = \frac{1}{N}.$$

Show that N is a perfect square.

Walkthrough —

(a) Note that it suffices to show that if N^2 has precisely 2005 positive divisors for some positive integer N, then N is a perfect square.

(b) Note that $2005 = 5 \cdot 401$, and all prime factors of 2005 are congruent to 1 modulo 4.

Example 1.10 (All-Russian MO 1989 Day 2 Grade 8 P5)**.** Show that number $4^{545} + 545^4$ is composite.

Example 1.11 (India RMO 1991 P7, cf. All-Russian MO 1989 Day 2 Grade 8 P5 **??**, India BStat 2006 P3)**.** [**Eng98**, p. 121] Show that $n^4 + 4^n$ is prime if and only if $n = 1$.

Solution 7. Let n be a positive integer such that $n^4 + 4^n$ is a prime. Note that n is odd, and

$$\begin{aligned} n^4 + 4^n &= (n^2 + 2^n)^2 - 2^{n+1}n^2 \\ &= (n^2 + 2^n)^2 - (2^{(n+1)/2}n)^2 \\ &= (n^2 + 2^n - 2^{(n+1)/2}n)(n^2 + 2^n + 2^{(n+1)/2}n) \end{aligned}$$

holds. Since $n^4 + 4^n, n^2 + 2^n + 2^{(n+1)/2}n$ are positive, it follows that $n^2 + 2^n - 2^{(n+1)/2}n$ is positive. This gives $n^2 + 2^n - 2^{(n+1)/2}n = 1$. Note that

$$n^2 + 2^n - 2^{(n+1)/2}n \geq 2 \cdot 2^{n/2}n - 2^{(n+1)/2}n = (\sqrt{2} - 1)2^{(n+1)/2}n$$

holds. If $n \geq 2$, then the above yields

$$n^2 + 2^n - 2^{(n+1)/2}n \geq (\sqrt{2} - 1)2^{(n+1)/2}n > 1,$$

which implies that $n^4 + 4^n$ is not a prime. This proves that $n = 1$. Moreover, if $n = 1$, then $n^4 + 4^n$ is a prime. This completes the proof. ■

Example 1.12 (India INMO 1991 P1)**.** Find the number of positive integers n for which

1. $n \leq 1991$ and

2. 6 is a factor of (n^2+3n+2).

Solution 8. Note that if n is a positive integer, then 6 divides $(n+1)(n+2)$ if and only if 3 divides $(n+1)(n+2)$, which is equivalent to $n \equiv \pm 1 \bmod 3$. So, the positive integers satisfying the given conditions are precisely the positive integers at most 1991, which are not divisible by 3. Noting that $1991 = 3 \cdot 663 + 2$, it follows that the requires number is equal to

$$664 + 664 = 1328.$$

■

Example 1.13 (India RMO 1991 P3)**.** A four-digit number has the following properties:

1. it is a perfect square,
2. its first two digits are equal to each other,
3. its last two digits are equal to each other.

Find all such four-digit numbers.

Solution 9. Let n be a positive integer satisfying the given conditions. Denote the first two digits of n by a, and the last two digits of n by b. Since n is a perfect square, it follows that n is congruent to one of $0, 1$ modulo 4, which shows that $10b + b = 11b$ is congruent to one of $0, 1$ modulo 4, or equivalently, b is congruent to one of $0, 3$ modulo 4. Similarly, using that a perfect square is congruent to one of $0, 1, -1$ modulo 5, it follows that b is congruent to one of $-1, 0, 1$ modulo 5. This implies that b is equal to one of $0, 4$.

If $b = 0$, then n is the square of a multiple of 10, and hence, its first two digits would not be equal. It follows that $b = 4$, and consequently, we obtain

$$n = 1000a + 100a + 10b + b = 1100a + 11b = 1100a + 44.$$

This shows that 11 divides the perfect square n. So, 11^2 divides n, and hence, 11 divides $100a + 4$, which yields

$$a \equiv 7 \bmod 11.$$

Since $1 \leq a \leq 9$, we obtain $a = 7$, and this gives $n = 7744$. Note that $7744 = 88^2$, it follows that 7744 is the only four-digit number satisfying the given conditions. ■

Example 1.14 (All-Russian MO 1992–1993 Final Stage Grade 09 P1, India RMO 2011b P2)**.** Let n be a positive integer such that $2n + 1$ and $3n + 1$ are both perfect squares. Show that $5n + 3$ is a composite number.

Solution 10. Let a, b be positive integers such that

$$2n+1 = a^2, \quad 3n+1 = b^2$$

holds. Note that

$$5n+3 = 4(2n+1) - (3n+1) = 4a^2 - b^2 = (2a-b)(2a+b). \tag{1}$$

Since $2a+b \geq 2$, it follows that $2a-b$ is positive, and hence, it suffices to show that $2a-b \neq 1$. Using $2n+1$ is a perfect square, it follows that $n \geq 3$. Note that

$$\begin{aligned} 2a-b &= 2\sqrt{2n+1} - \sqrt{3n+1} \\ &= \frac{4(2n+1)-(3n+1)}{2\sqrt{2n+1}+\sqrt{3n+1}} \\ &= \frac{5n}{2\sqrt{2n+1}+\sqrt{3n+1}} \\ &\geq \frac{5n}{2\sqrt{3n}+\sqrt{4n}} \\ &= \frac{5}{2+2\sqrt{3}}\sqrt{n} \\ &> 1, \end{aligned}$$

where the last inequality is obtained using $n \geq 3$. This shows that $2a-b > 1$. From **??**, it follows that $5n+3$ is a composite number. ■

Example 1.15 (India RMO 1994 P5)**.** Let A be a set of 16 positive integers with the property that the product of any two distinct numbers of A will not exceed 1994. Show that there are two numbers a and b in A which are not relatively prime.

Solution 11. Note that if $n \geq 1$, and $a_1, \ldots, a_n$ are distinct and pairwise coprime positive integers such that $a_i \geq 2$ for all i, then one of them admits a prime factor which is at least as large as the n-th prime. Indeed, for each i, if we fix a prime divisor p_i of a_i, then using that $a_1, \ldots, a_n$ are pairwise coprime, it follows that $p_1, \ldots, p_n$ are distinct primes, and hence the largest among them is at least as large as the n-th prime. Consequently, if $n \geq 2$, and $a_1, \ldots, a_n$ are distinct and pairwise coprime positive integers, then at least $(n-1)$ of them are greater than 1, and hence one of them is divisible by a prime at least as large as the $(n-1)$-st prime.

If possible, let us assume that the elements of A are pairwise coprime. Hence, A contains an element x which is divisible by a prime at least as large as the 15th prime. Similarly, $A \setminus \{x\}$ has an element y which is divisible by a prime at least as large as the 14th prime. Since the 14th and 15th primes are $43, 47$ respectively, it follows that $x \geq 47, y \geq 43$, and consequently,

$$xy \geq 47 \cdot 43 = 2021 > 1994,$$

which contradicts the hypothesis. This proves that there are two numbers a and b in A which are not relatively prime. ■

Example 1.16 (India RMO 1994 P3)**.** Find all 6-digit natural numbers $a_1a_2a_3a_4a_5a_6$ formed by using the digits $1, 2, 3, 4, 5, 6$, once each such that the number $a_1a_2 \dots a_k$ is divisible by k, for $1 \leq k \leq 6$.

Solution 12. Since $a_1a_2, a_1a_2a_3a_4, a_1a_2a_3a_4a_5a_6$ are divisible by 2, it follows that a_2, a_4, a_6 are even, and hence they are equal to $2, 4, 6$ in some order. Using that $a_1a_2a_3a_4a_5$ is divisible by 5, we get that $a_5 = 5$. So a_1, a_3 are equal to $1, 3$ in some order. Using that $a_1a_2a_3$ is a multiple of 3, we obtain

$$a_1 + a_2 + a_3 \equiv 0 \bmod 3,$$

which yields

$$a_2 \equiv 2 \bmod 3,$$

and hence, $a_2 = 2$ holds. Note that $1234, 3214$ are not divisible by 4. This shows that $a_4 = 6$, and hence $a_6 = 4$. It follows that $a_1a_2a_3a_4a_5a_6$ is equal to 321654, or 123654. Note that the integers $321654, 123654$ satisfy the required conditions too. This proves that $321654, 123654$ are precisely all the 6-digit numbers satisfying the given condition. ■

Example 1.17 (Tournament of Towns, India RMO 1995 P3)**.** [**Tao06**, Problem 2.1] Prove that among any 18 consecutive three digit numbers there is at least one number which is divisible by the sum of its digits.

Solution 13. Note that among 18 consecutive three digit numbers, there is an integer divisible by 18. Denote it by $n = 100a + 10b + c$ with a, b, c lying between 0 and 9. It follows that 9 divides n, and hence 9 divides $a+b+c$. This shows that $a + b + c$ is equal to one of $9, 18, 27$. Note that $a + b + c = 27$ holds only if $n = 999$. Since 18 divides n, it follows that $a + b + c \neq 27$, and hence, $a + b + c$ is equal to one of $9, 18$. This proves that $a + b + c$ divides n. ■

Example 1.18 (China TST 1995 Day 1 P1)**.** Find the smallest prime number p that cannot be represented in the form $|3^a - 2^b|$, where a and b are non-negative integers.

Solution 14. Note that any prime smaller than 41 can be expressed as the absolute value of the difference of a nonnegative power of 3 and a nonnegative power of 2, as shown below.

$$2 = 3 - 1,$$
$$3 = 4 - 1,$$
$$5 = 9 - 4,$$

$$\begin{aligned}7 &= 8 - 1,\\ 11 &= 27 - 16,\\ 13 &= 16 - 3,\\ 17 &= 81 - 64,\\ 19 &= 27 - 8,\\ 23 &= 32 - 9,\\ 29 &= 32 - 3,\\ 31 &= 32 - 1,\\ 37 &= 64 - 27.\end{aligned}$$

Let us prove the following claim.

Claim — The prime number 41 cannot be expressed as the absolute value of the difference of a nonnegative power of 3 and a nonnegative power of 2.

Proof of the Claim. On the contrary, let us assume that

$$41 = |3^a - 2^b|$$

holds for some nonnegative integers a, b.

First, let us consider the case that $41 = 2^b - 3^a$. Note that $b \geq 3$ holds, and reducing the above modulo 8, it follows that $3^a \equiv -1 \pmod 8$, which is impossible.

Now, let us consider the case that $41 = 3^a - 2^b$. Reducing modulo 3, it follows that $2^b \equiv 1 \pmod 3$, which shows that b is even. Note that b is nonzero. Next, reducing modulo 4, we obtain $3^a \equiv 1 \pmod 4$, which implies that a is even. Writing $a = 2x, b = 2y$ for some positive integers x, y, we obtain

$$41 = 3^{2x} - 2^{2y} = (3^x - 2^y)(3^x + 2^y)$$

with $1 \leq 3^x - 2^y < 3^x + 2^y$, which yields

$$3^x - 2^y = 1, 3^x + 2^y = 41,$$

which is impossible.

Considering the above cases, the claim follows. □

This proves that 41 is smallest prime that cannot be expressed in the given form. ■

Example 1.19 (India RMO 1995 P2)**.** Call a positive integer n *good* if there are n integers, positive or negative, and not necessarily distinct, such that their sum and products are both equal to n. Show that the integers of the form $4k + 1$ and 4ℓ are good.

Solution 15. Note that 1 is good. Let k be a positive integer. Put

$$a_1 = \cdots = a_k = 1, \quad b_1 = \cdots = b_k = -1.$$

Noting that

$$4k+1 = (4k+1) + 2(a_1 + \cdots + a_k) + 2(b_1 + \cdots + b_k),$$
$$4k+1 = (4k+1)\left(\prod_{i=1}^{k} a_i b_i\right)^2,$$

it follows that $4k+1$ is good. Also note that for a positive integer ℓ, 4ℓ is equal to the sum, and also equal to the product, of $2, 2, \ell$ and $4\ell - 2 - 2 - \ell$ many 1's, and hence, 4ℓ is good. ■

Example 1.20 (India RMO 1996 P4)**.** Suppose N is an n-digit positive integer such that

1. all the n-digits are distinct, and
2. the sum of any three consecutive digits is divisible by 5.

Prove that n is at most 6. Further, show that starting with any digit one can find a six-digit number with these properties.

Solution 16. If $n \geq 7$, then note that the first digit of N is congruent to its fourth digit modulo 5, and its fourth digit is congruent to its seventh digit modulo 5, and hence, its first, fourth and seventh digits are congruent to each other modulo 5, which is impossible since the digits of n are distinct and no three integers among $0, 1, 2, 3, 4, 5, 6, 7, 8, 9$ are congruent modulo 5. This shows that n is at most 6.

Let $0 \leq a \leq 4$ be an integer. Considering the 3-digit numbers

$$140, 230, 320, 410,$$

it follows that there are integers $0 \leq b, c \leq 4$ such that a, b, c are distinct, and their sum is divisible by 5. Taking

$$a_1 = a, a_2 = b, a_3 = c, a_4 = a_1 + 5, a_5 = a_2 + 5, a_6 = a_3 + 5,$$

it follows that the 6-digit integer

$$10^5 a_1 + 10^4 a_2 + 10^3 a_3 + 10^2 a_4 + 10 a_5 + a_6$$

has the required properties. ■

Example 1.21 (India RMO 1997 P2)**.** For each positive integer n, define $a_n = 20 + n^2$, and $d_n = \gcd(a_n, a_{n+1})$. Find the set of all values that are taken by d_n and show by examples that each of these values are attained.

Solution 17. Let n be a positive integer. Since d_n divides the integers $20+n^2, 20+(n+1)^2$, it follows that d_n divides

$$20+(n+1)^2-(20+n^2)=2n+1,$$

and d_n also divides

$$20+(n+1)^2+20+n^2=41+2n^2+2n.$$

This shows that d_n divides

$$2(41+2n^2+2n)-(2n+1)^2=81.$$

So, d_n is equal to one of $1,3,9,27,81$.

Note that

$$\begin{aligned} d_1 &= \gcd(a_1,a_2)\\ &= \gcd(21,24)\\ &= 3,\\ d_2 &= \gcd(a_2,a_3)\\ &= \gcd(24,29)\\ &= 1 \end{aligned}$$

holds.

If $d_n=9$, then 9 divides $2n+1$, showing that $n\equiv 4 \bmod 9$. Note that

$$d_4=\gcd(a_4,a_5)=\gcd(36,45)=9$$

holds. If $d_n=27$, then 27 divides $2n+1$, implying that $n\equiv 13 \bmod 27$. Note that

$$d_{13}=\gcd(a_{13},a_{14})=\gcd(189,216)=\gcd(189,216-189)=\gcd(189,27)=27$$

holds. Also note that if $d_n=81$, then 81 divides $2n+1$, which shows that $n\equiv 40 \bmod 81$. Observe that

$$\begin{aligned} d_{40} &= \gcd(a_{40},a_{41})\\ &= \gcd(20+40^2,20+41^2)\\ &= \gcd(1620,2\cdot 40+1)\\ &= 81 \end{aligned}$$

holds.

This proves that the set of values taken by d_n are precisely

$$1,3,9,27,81.$$

■

Example 1.22 (India RMO 1998 P5)**.** Find the minimum possible least common multiple (lcm) of twenty (not necessarily distinct) natural numbers whose sum is 801.

Solution 18. Let L denote the minimum possible least common multiple of twenty (not necessarily distinct) natural numbers, whose sum is 801. Note that one of these natural numbers is larger than 40 (otherwise their sum would be no larger than $40 \times 20 = 800$), and so L is at least 41. Since 801 can be written as

$$3 + \underbrace{42 + 42 + \cdots + 42}_{19 \text{ times}} = 801,$$

we get $L \leq 42$. Let us prove the claim below.

Claim — The integer L is not equal to 41.

Proof of the Claim. On the contrary, assume that there exist twenty natural number numbers $x_1, \ldots, x_{20}$ satisfying

$$x_1 + \cdots + x_{20} = 801, \quad \operatorname{lcm}(x_1, \ldots, x_{20}) = 41.$$

Since 41 is a prime, it follows that 41 divides x_i for some $1 \leq i \leq 20$. Since 41 is the least common multiple of $x_1, \ldots, x_{20}$, we obtain $x_i = 41$. Note that the sum $x_1 + \cdots + x_{20}$ is less than $20 \cdot 41$. This shows that not all of $x_1 + \cdots + x_{20}$ is divisible by 41. Reordering the integers $x_1 + \cdots + x_{20}$ (if necessary), let $1 \leq k < 20$ denote the integer such that none of $x_1, x_2, \ldots, x_k$ is divisible by 41, and $x_{k+1}, x_{k+2}, \ldots, x_{20}$ are equal to 41. We obtain that

$$41 = \operatorname{lcm}(x_1, \ldots, x_{41}) = \operatorname{lcm}(\operatorname{lcm}(x_1, \ldots, x_k), 41).$$

Since none of $x_1, \ldots, x_k$ is divisible by 41, it follows that $\operatorname{lcm}(x_1, \ldots, x_k) = 1$, and hence,

$$x_1 = x_2 = \cdots = x_k = 1.$$

This yields

$$k + 41(20 - k) = 801,$$

which implies that $k \equiv 22 \bmod 41$, which is impossible since $1 \leq k \leq 19$. This proves the Claim. □

We obtain that $L = 42$. ■

Example 1.23 (India RMO 1998 P2)**.** Let n be a positive integer and $p_1, p_2, \ldots, p_n$ be n prime numbers all larger than 5 such that 6 divides $p_1^2 + p_2^2 + \cdots + p_n^2$. Prove that 6 divides n.

Solution 19. Note that any prime number larger than 5 is of the form $6k \pm 1$. This yields

$$p_1^2 + p_2^2 + \cdots + p_n^2 \equiv (\pm 1)^2 + (\pm 1)^2 + \cdots + (\pm 1)^2 \bmod 6 \equiv n \bmod 6.$$

Since 6 divides $p_1^2 + p_2^2 + \cdots + p_n^2$, it follows that 6 divides n. ■

Example 1.24 (India RMO 1999 P2)**.** Find the number of positive integers which divide 10^{999} but not 10^{998}.

Solution 20. Since every divisor of 10^{998} divides 10^{999}, the required number is equal to the difference of the number of divisors of 10^{999} and 10^{998}, which is equal to $(999+1)(999+1) - (998+1)(998+1) = 1999$. ■

Example 1.25 (Bay Area MO 1999 P1)**.** Prove that among any 12 consecutive positive integers, there is at least one which is smaller than the sum of its proper divisors. (The proper divisors of a positive integer n are all positive integers other than 1 and n which divide n. For example, the proper divisors of 14 are 2 and 7.)

Solution 21. Among any twelve consecutive integers, there is a multiple of 12. For any positive integer n, note that

$$3n, 4n, 6n$$

are proper divisors of $12n$, and

$$12n < 3n + 4n + 6n$$

holds. This completes the proof. ■

Example 1.26 (Bay Area MO 2000 P1)**.** Prove that any integer greater than or equal to 7 can be written as a sum of two relatively prime integers, both greater than 1.

Solution 22. Note that any odd integer can be expressed as the sum of two relatively prime integers. Indeed, for any integer n, the integer $2n+1$ is the sum of the relatively prime integers $n, n+1$.

For any integer k, note that

$$4k = (2k-1) + (2k+1)$$

holds, and the integers $2k-1, 2k+1$ are relatively prime since any of their common divisors is odd and divides $(2k+1) - (2k-1) = 2$.

For any integer ℓ, note that

$$4\ell + 2 = (2\ell - 1) + (2\ell + 3)$$

holds, and the integers $2\ell - 1, 2\ell + 3$ are relatively prime since any of their common divisors is odd and divides $(2\ell+3) - (2\ell-1) = 4$. ■

Example 1.27 (India RMO 2000 P6)**.**

1. Consider two positive integers a and b which are such that $a^a b^b$ is divisible by 2000. What is the least possible value of the product ab?

2. Consider two positive integers a and b which are such that $a^b b^a$ is divisible by 2000. What is the least possible value of the product ab?

Solution 23. Let a, b denote positive integers such that $a^a b^b$ is divisible by 2000 and the product ab is minimum. Note that $2, 5$ divide ab, which shows that 10 divides ab, and hence $ab \geq 10$. Using that 2000 divides $10^{10}1^1$, we obtain $ab = 10$.

Now let a, b denote positive integers such that $a^b b^a$ is divisible by 2000 and the product ab is minimum. Note that $2, 5$ divide ab, and hence 10 divides ab. Moreover, $ab \leq 20$ since 2000 divides $4^5 5^4$. If $ab = 10$, then (a, b) is equal to one of

$$(1, 10), (2, 5), (5, 2), (10, 1),$$

and in each of this cases, 2000 does not divide $a^b b^a$. This shows that $ab \neq 10$, and $ab \leq 20$, and ab is a multiple of 10. Observing that 2000 divides $4^5 5^4$, we conclude that $ab = 20$. ■

Example 1.28 (India RMO 2001 P7)**.** Prove that the product of the first 1000 positive even integers differs from the product of the first 1000 odd integers by a multiple of 2001.

Solution 24. Note that

$$\begin{aligned} &2 \cdot 4 \cdot 6 \cdot \vdots 1998 \cdot 2000 \\ &\quad - 1 \cdot 3 \cdot 5 \cdot \cdots \cdot 1997 \cdot 1999 \\ &= (2001 - 1)(2001 - 3) \cdots (2001 - 1997)(2001 - 1999) \\ &\quad - (2001 - 2)(2001 - 4) \cdots (2001 - 1998)(2001 - 2000) \end{aligned}$$

holds, which yields

$$\begin{aligned} &2 \cdot 4 \cdot 6 \cdots 1998 \cdot 2000 - 1 \cdot 3 \cdot 5 \cdots 1997 \cdot 1999 \\ &\equiv 1 \cdot 3 \cdot 5 \cdots 1997 \cdot 1999 - 2 \cdot 4 \cdot 6 \cdots 1998 \cdot 2000 \bmod 2001. \end{aligned}$$

It follows that

$$2(2 \cdot 4 \cdot 6 \cdots 1998 \cdot 2000 - 1 \cdot 3 \cdot 5 \cdots 1997 \cdot 1999) \equiv 0 \bmod 2001,$$

which implies that

$$2000(2 \cdot 4 \cdot 6 \cdots 1998 \cdot 2000 - 1 \cdot 3 \cdot 5 \cdots 1997 \cdot 1999) \equiv 0 \bmod 2001.$$

This shows that

$$2 \cdot 4 \cdot 6 \cdots 1998 \cdot 2000 - 1 \cdot 3 \cdot 5 \cdots 1997 \cdot 1999 \equiv 0 \bmod 2001,$$

completing the proof. ■

Example 1.29 (India RMO 2002 P3, India RMO 2012d P2, India RMO 2012a P2, India RMO 2012b P2, India RMO 2012c P2)**.**

1. Let a, b, c be positive integers such that a divides b^2, b divides c^2 and c divides a^2. Prove that abc divides $(a+b+c)^7$.
2. Let a, b, c be positive integers such that $a|b^3, b|c^3$ and $c|a^3$. Prove that abc divides $(a+b+c)^{13}$.
3. Let a, b, c be positive integers such that $a|b^4, b|c^4$ and $c|a^4$. Prove that abc divides $(a+b+c)^{21}$.
4. Let a, b, c be positive integers such that $a|b^5, b|c^5$ and $c|a^5$. Prove that abc divides $(a+b+c)^{31}$.

Solution 25. In the following, k denotes one of the integers $2, 3, 4, 5$. Assume that $a \mid b^k, b \mid c^k, c \mid a^k$. Note that if one of a, b, c is equal to 1, then all of them are equal to 1, and then there is nothing to prove. Henceforth, let us assume that a, b, c are larger than 1. The given conditions imply that the set of prime divisors of a, b, c are equal.

Let p be a common prime divisor of a, b, c. Let $p^\alpha, p^\beta, p^\gamma$ denote the highest powers of p dividing a, b, c respectively. The given divisibility conditions imply that

$$\alpha \le k\beta, \beta \le k\gamma, \gamma \le k\alpha.$$

This yields

$$\alpha + \beta + \gamma \le \alpha + k^2\alpha + 2\alpha = (k^2 + k + 1)\alpha,$$

and similarly, $\alpha + \beta + \gamma \le (k^2 + k + 1)\beta$, $\alpha + \beta + \gamma \le (k^2 + k + 1)\gamma$, which shows that

$$\alpha + \beta + \gamma \le (k^2 + k + 1)\min\{\alpha, \beta, \gamma\}.$$

Note that $p^{\min\{\alpha,\beta,\gamma\}}$ divides $a+b+c$. By the above inequality, $p^{\alpha+\beta+\gamma}$ divides $(a+b+c)^{(}k^2+k+1)$. So abc divides $(a+b+c)^7$. Also note that $p^{\alpha+\beta+\gamma}$ is the highest power of p dividing abc. This shows that for each common prime divisor p of a, b, c, the highest power of p that divides abc also divides $(a+b+c)^{k^2+k+1}$. It follows that abc divides $(a+b+c)^{k^2+k+1}$. ■

Solution 26. It suffices to show that abc divides $a^\alpha b^\beta c^\gamma$ for any nonnegative integers α, β, γ such that $\alpha + \beta + \gamma = k^2 + k + 1$. Note that

$$abc \mid ac^{k+1} \mid a^{k^2+k+1}, \quad abc \mid a^{k+1}b \mid b^{k^2+k+1}, \quad abc \mid b^{k+1}c \mid c^{k^2+k+1},$$

which shows that abc divides $a^{k^2+k+1}, b^{k^2+k+1}, c^{k^2+k+1}$. Moreover, abc divides $a^\alpha b^\beta c^\gamma$ when α, β, γ are all positive. It remains to consider the case when exactly one of α, β, γ is zero, which we assume from now on. If $\alpha = 0$, then

$$abc \mid b^{k+1}c \mid b^\beta c^\gamma \text{ if } \beta \geq k+1,$$
$$abc \mid c^{k^2+1}b \mid b^\beta c^\gamma \text{ if } \beta \leq k$$

holds. If $\beta = 0$, then

$$abc \mid c^{k+1}a \mid c^\gamma a^\alpha \text{ if } \gamma \geq k+1,$$
$$abc \mid a^{k^2+1}c \mid c^\gamma a^\alpha \text{ if } \gamma \leq k$$

holds. If $\gamma = 0$, then

$$abc \mid a^{k+1}b \mid a^\alpha b^\beta \text{ if } \alpha \geq k+1,$$
$$abc \mid b^{k^2+1}a \mid a^\alpha b^\beta \text{ if } \alpha \leq k$$

holds. This shows that abc divides $(a+b+c)^{k^2+k+1}$. ■

Example 1.30 (India RMO 2003 P2)**.** If n is an integer greater than 7, prove that $\binom{n}{7} - \left[\frac{n}{7}\right]$ is divisible by 7. [Here $\binom{n}{7}$ denotes the number of ways of choosing 7 objects from among n objects; also for any real number x, $[x]$ denotes the greatest integer not exceeding x.]

Solution 27. If $x_1, x_2, \ldots, x_k$ are real numbers with $k \geq 2$ and $1 \leq \ell \neq k$ is an integer, then we denote by $x_1 \ldots \widehat{x_\ell} \ldots x_k$ the product

$$x_1 \ldots x_{\ell-1} x_{\ell+1} \ldots x_k.$$

Let n be an integer greater than 7. Let q, r be integers with $0 \leq r \leq 6$ and $q \geq 1$ such that n is equal to $7q+r$. We need to show that $\binom{7q+r}{7} - q$ is divisible by 7, which is equivalent to

$$6!\left(\binom{7q+r}{7} - q\right) \equiv 0 \bmod 7 \tag{2}$$

since 6! is coprime to 7. Note that $6!\binom{7q+r}{7}$ is equal to

$$\frac{(7q+r)(7q+r-1)(7q+r-2)(7q+r-3)(7q+r-4)(7q+r-5)(7q+r-6)}{7}.$$

It follows that

$$6!\binom{7q+r}{7} \equiv q \cdot r(r-1)\cdots\widehat{(r-r)}\cdots(r-6) \bmod 7 \equiv q \cdot 6! \bmod 7.$$

This shows that **??** holds, which proves the result. ■

Example 1.31 (India RMO 2005 P2)**.** If x, y are integers and 17 divides both the expressions $x^2 - 2xy + y^2 - 5x + 7y$ and $x^2 - 3xy + 2y^2 + x - y$, then prove that 17 divides $xy - 12x + 15y$.

Solution 28. Let x, y be integers such that 17 divides both the expressions $x^2 - 2xy + y^2 - 5x + 7y$ and $x^2 - 3xy + 2y^2 + x - y$. Note that

$$x^2 - 3xy + 2y^2 + x - y = (x - y)(x - 2y + 1),$$

which is divisible by 17. It follows that

$$x \equiv y \bmod 17, \quad \text{or } x \equiv 2y - 1 \bmod 17$$

holds.

Let us consider the case that $x \equiv y \bmod 17$. It follows that

$$x^2 - 2xy + y^2 - 5x + 7y \equiv (x - y)^2 - 5x + 7y \equiv 2y \bmod 17.$$

Since 17 divides $x^2 - 2xy + y^2 - 5x + 7y$, we get $2y \equiv 0 \bmod 17$, which yields $x \equiv y \equiv 0 \bmod 17$, and hence 17 divides $xy - 12x + 15y$.

Let us consider the case that $x \equiv 2y - 1 \bmod 17$. Using $x^2 - 2xy + y^2 - 5x + 7y \equiv 0 \bmod 17$, we obtain

$$(2y - 1)^2 - 2(2y - 1)y + y^2 - 5(2y - 1) + 7y \equiv 0 \bmod 17,$$

which yields $y^2 - 5y + 6 \equiv 0 \bmod 7$. This implies that $(y-2)(y-3) \equiv 0 \bmod 17$. This shows that either $x \equiv 3 \bmod 17, y \equiv 2 \bmod 17$ holds, or $x \equiv 5 \bmod 17, y \equiv 3 \bmod 17$ holds. If $x \equiv 3 \bmod 17, y \equiv 2 \bmod 17$ holds, then

$$xy - 12x + 15y \equiv 6 - 36 + 30 \equiv 0 \bmod 17$$

holds. If $x \equiv 5 \bmod 17, y \equiv 3 \bmod 17$ holds, then we obtain

$$xy - 12x + 15y \equiv 15 - 60 + 45 \equiv 0 \bmod 17.$$

This proves that 17 divides $xy - 12x + 15y$. ■

Example 1.32 (India RMO 2006 P2)**.** Find the least possible value of $a + b$, where a, b are positive integers such that 11 divides $a + 13b$ and 13 divides $a + 11b$.

Solution 29. Let a, b be positive integers such that 11 divides $a + 13b$ and 13 divides $a + 11b$. It follows that 11 divides $6a + 78b = 6a + b + 77b$, and 13 divides $6a + 66b = 6a + b + 65b$. This shows that $6a + b$ is divisible by 11 and 13. Since the integers $11, 13$ are relatively prime, we obtain that $11 \cdot 13 = 143$ divides $6a + b$.

If $b \geq 4$, then we obtain

$$6a + 6b = 6a + b + 5b \geq 143 + 20 = 163,$$

which implies that

$$a + b \geq 28.$$

If $b = 1$, then $6a + b = 143$ admits no solutions in the integers, and hence $6a + b \geq 3 \cdot 143$ holds, which implies that $a + b \geq (6a + b)/6 > 28$. If $b = 2$, then $6a + b = 143$ admits no solutions in the integers, and hence $6a + b \geq 2 \cdot 143$ holds, which shows that $a + b \geq (6a + b)/6 > 28$. If $b = 3$, then $6a + b = 143$ admits no solutions in the integers, and hence $6a + b \geq 3 \cdot 143$ holds, which implies that $a + b \geq (6a + b)/6 > 28$. Considering these cases, it follows that $a + b \geq 28$.

Note that $a = 23, b = 5$ satisfy the given conditions. This shows that least possible value of $a + b$ accross all positive integers a, b satisfying the given divisibility conditions is 28. ■

Solution 30. Let a, b be positive integers such that 11 divides $a + 13b$, 13 divides $a + 11b$. It follows that $a + 2b$ is equal to $11m$, and $a - 2b$ is equal to $13n$ for some integers m, n with $m \geq 1$. This gives

$$a = \frac{11m + 13n}{2}, b = \frac{11m - 13n}{4}, a + b = \frac{33m + 13n}{4}.$$

Since b is an integer, we obtain $3m \equiv n \bmod 4$. If (m, n) is equal to $(3, 1)$, then note that

$$A := \frac{11m + 13n}{2}, B := \frac{11m - 13n}{4}$$

are positive integers satisfying

$$A + B = 23 + 5 = 28,$$

and 11 divides $A + 2B$ and 13 divides $A - 2B$, or equivalently, 11 divides $A + 13B$ and 13 divides $A + 11B$. This shows that $a + b \leq 28$. Since m is positive, we get

$$\frac{33 + 13n}{4} \leq \frac{33m + 13n}{4} = a + b \leq 28,$$

$$\frac{11 - 13n}{4} \leq \frac{11m - 13n}{4} = b < a + b \leq 28,$$

which gives $-7 \leq n \leq 6$. Note that if n is nonnegative, then we obtain

$$\frac{33m}{4} \leq a + b \leq 28,$$

which gives $m \leq 3$, and when n is negative, we have

$$\frac{33m + 13n}{4} \leq 28,$$

which gives

$$33m \leq 112 - 13n \leq 112 + 13 \cdot 7 = 203,$$

implying $m \leq 6$. Moreover, we have

$$m \geq \frac{13}{11}|n| > |n|.$$

Noting that $m + n \equiv 0 \bmod 4$ holds, it follows that the pair (m, n) is equal to one of $(3, 1), (6, -2), (5, -1)$. If (m, n) is equal to $(6, -2), (5, -1)$, then $b = \frac{11m-13n}{4}$ is larger than 28. Consequently, (m, n) is equal to $(3, 1)$. This shows that the least value of $a + b$ is 28. ■

Example 1.33 (India BMath 2007 P1)**.** Let n be a positive integer. If n has odd number of divisors (other than 1 and n), then show that n is a perfect square.

Example 1.34 (India RMO 2009 P3)**.** Show that $3^{2008} + 4^{2009}$ can be written as product of two positive integers each of which is larger than 2009^{182}.

Solution 31. Note that $3^{2008} + 4^{2009}$ is equal to $4x^4 + y^4$ where $x = 4^{502}, y = 3^{502}$. Also note that

$$3^{2008} + 4^{2009} = (2x^2 + y^2 - 2xy)(2x^2 + y^2 + 2xy)$$

holds. Since $x \neq y$, it follows that the integers $2x^2 + y^2 + 2xy, 2x^2 + y^2 - 2xy$ are strictly larger than x^2. So it suffices to show $x^2 \geq 2009^{182}$, which is equivalent to $x \geq 2009^{91}$, which follows since

$$x = 4^{502} = 2^{1004} > 2^{11 \cdot 91} = 2048^{91} > 2009^{91}$$

holds. ■

Example 1.35 (India RMO 2011a P3)**.** A natural number n is chosen strictly between two consecutive perfect squares. The smaller of these two squares is obtained by subtracting k from n and the larger by adding ℓ to n. Prove that $n - k\ell$ is a perfect square.

Solution 32. Let m be a positive integer such that

$$m^2 = n - k, (m + 1)^2 = n + \ell$$

holds. This yields

$$\begin{aligned} n - k\ell &= n - (n - m^2)((m + 1)^2 - n) \\ &= n + n^2 - n(m^2 + (m + 1)^2) + m^2(m + 1)^2 \\ &= n^2 - n(2m^2 + 2m) + (m^2 + m)^2 \\ &= (n - m^2 - m)^2, \end{aligned}$$

which is a perfect square. ■

Example 1.36 (India Pre-RMO 2012)**.** Let $P(n) = (n+1)(n+3)(n+5)(n+7)$. What is the largest integer that is a divisor of $P(n)$ for all positive even integers n?

Solution 33. Note that

$$\begin{aligned} P(2) &= 3 \cdot 5 \cdot 7 \cdot 9, \\ P(10) &= 11 \cdot 13 \cdot 15 \cdot 17, \\ P(16) &= 17 \cdot 19 \cdot 21 \cdot 23 \end{aligned}$$

holds. Also note that for any integer n, at least one of $n+1, n+3, n+5$ is divisible by 3. It follows that the largest integer that divides $P(n)$ for all positive even integers n is equal to 3. ■

Example 1.37 (India RMO 2012f P2)**.** Let n be a positive integer such that 13 divides $n^2 + 3n + 51$. Show that 169 divides $21n^2 + 89n + 44$.

Solution 34. Note that the polynomial $X^2+3X+51$ is congruent to X^2+3X-1 modulo 13, which vanishes at 5 mod 13, and its discriminant is congruent to 0 modulo 13. This shows that the polynomial $X^2 + 3X + 51$ is congruent to $(X-5)^2$ modulo 13. So n is congruent to 5 mod 13.

Note that the discriminant of $21X^2 + 89X + 44$ satisfies

$$89^2 - 4 \cdot 21 \cdot 44 \equiv (-2)^2 - 4 \cdot (-5) \cdot 5 \equiv 4 \cdot 26 \bmod 13,$$

and hence this polynomial is congruent to $21(X-k)^2$ modulo 13 for some integer k. Observing that

$$21 \cdot 5^2 + 89 \cdot 5 + 44 \equiv (-5) \cdot (-1) - 2 \cdot 5 + 5 \equiv 0 \bmod 13,$$

it follows that k is congruent to 5 mod 13. This implies that $21X^2 + 89X + 44$ is congruent to $21(X-5)^2$ modulo 13. Since n is congruent to 5 mod 13, it follows that 169 divides $21n^2 + 89n + 44$. ■

Example 1.38 (India RMO 2012e P6)**.** A computer program generated 175 positive integers at random, none of which had a prime divisor greater than 10. Prove that there are three numbers among them whose product is the cube of an integer.

Solution 35. Denote these integers by

$$2^{a_1}3^{b_1}5^{c_1}7^{d_1}, 2^{a_2}3^{b_2}5^{c_2}7^{d_2}, \cdots, 2^{a_{175}}3^{b_{175}}5^{c_{175}}7^{d_{175}}.$$

By pigeonhole principle, there exists a subset A of $\{1, 2, \ldots, 175\}$ of size 59 such that the integers a_i, for i in A, are congruent to each other modulo 3. By the same principle, it follows that there exists a subset B of A of size 20 such that

the integers b_i, for i in B, are congruent to each other modulo 3. Applying the same principle, we obtain a subset of C of B of size 7 such that the integers c_i, for i in C, are congruent to each other modulo 3. Using the principle principle once again, we get a subset D of C of size 3 such that the integers d_i, for i in D, are congruent to each other modulo 3. Since $D \subseteq C \subseteq B \subseteq A$ holds, it follows that the product of the three integers

$$2^{a_i}3^{b_i}5^{c_i}7^{d_i}, i \in D$$

is a perfect cube. ■

Example 1.39 (India RMO 2013d P2)**.** Determine the smallest prime that does not divide any five-digit number whose digits are in a strictly increasing order.

Solution 36. Note that 2 divides 12346, 3 and 5 divide 12345, and 7 divides 12348. Hence, the smallest prime satisfying the required condition is at least as large as 11.

Let $(abcde)_{10}$ be a five-digit number in base 10 with $1 \leq a < b < c < d < e \leq 9$. Note that

$$a - b + c - d + e = (a - b) + (c - d) + e \leq e \leq 9$$

holds, and

$$a - b + c - d + e = a + (c - b) + (e - d) \geq a \geq 1$$

holds. This shows that 11 does not divide $a - b + c - d + e$, or equivalently 11 does not divide the integer $(abcde)_{10}$. Since 11 does not divide any five-digit number whose digits are in a strictly increasing order, it follows that the smallest prime satisfying the required condition is at most 11.

We conclude that 11 is the smallest prime satisfying the required condition. ■

Example 1.40 (India RMO 2013e P5)**.** Let a_1, b_1, c_1 be natural numbers. We define

$$a_2 = \gcd(b_1, c_1), \quad b_2 = \gcd(c_1, a_1), \quad c_2 = \gcd(a_1, b_1)$$

and

$$a_3 = \operatorname{lcm}(b_2, c_2), \quad b_3 = \operatorname{lcm}(c_2, a_2), \quad c_3 = \operatorname{lcm}(a_2, b_2).$$

Show that $\gcd(b_3, c_3) = a_2$.

Solution 37. It suffices to show that the highest power of p dividing $\gcd(b_3, c_3)$ and a_2 are equal for any prime p. Fix a prime number p. Let p^x, p^y, p^z denote

the highest powers of p dividing a_1, b_1, c_1 respectively. So the highest exponents of p dividing a_2, b_2, c_2 are

$$\min\{y,z\}, \min\{z,x\}, \min\{x,y\}$$

respectively. Thus the highest exponents of p dividing b_3, c_3 are

$$\max\{\min\{x,y\}, \min\{y,z\}\}, \max\{\min\{y,z\}, \min\{z,x\}\}$$

respectively. So it remains to show that

$$\min\{\max\{\min\{x,y\}, \min\{y,z\}\}, \max\{\min\{y,z\}, \min\{z,x\}\}\} = \min\{y,z\} \tag{3}$$

holds. Note that $\min\{x,y\}, \min\{y,z\}$ are less than or equal to y, which gives

$$\max\{\min\{x,y\}, \min\{y,z\}\} \leq y.$$

Similarly, it follows that

$$\max\{\min\{y,z\}, \min\{z,x\}\} \leq z.$$

This gives that

$$\min\{\max\{\min\{x,y\}, \min\{y,z\}\}, \max\{\min\{y,z\}, \min\{z,x\}\}\} \leq \min\{y,z\}.$$

Note also that

$$\max\{\min\{x,y\}, \min\{y,z\}\} \geq \min\{y,z\},$$
$$\max\{\min\{y,z\}, \min\{z,x\}\} \geq \min\{y,z\}$$

holds, which yields

$$\min\{\max\{\min\{x,y\}, \min\{y,z\}\}, \max\{\min\{y,z\}, \min\{z,x\}\}\} \geq \min\{y,z\}.$$

This proves that **??** holds. ■

Example 1.41 (India RMO 2014c P3)**.** Prove that for any natural number $n < 2310$, $n(2310 - n)$ is not divisible by 2310.

Solution 38. Suppose $n < 2310$ is a positive integer such that $n(2310 - n)$ is equal to $2310k$ for some positive integer k. It follows that there are positive integers a, b such that a divides n, b divides $2310 - n$ and $ab = 2310$. Note that b also divides n. This shows that n is divisible by the least common multiple of the integers a and b, that is, by $ab/\gcd(a,b)$. Note that

$$2310 = 2 \cdot 3 \cdot 5 \cdot 7 \cdot 11$$

holds, and hence 2310 is a square-free integer. Since ab is equal to 2310, it follows that $\gcd(a,b) = 1$. This shows that ab divides n, that is, 2310 divides n, which is impossible. This completes the proof. ■

Example 1.42 (India RMO 2014b P3)**.** Find all pairs of (x, y) of positive integers such that $2x + 7y$ divides $7x + 2y$.

Solution 39. Let (x, y) be a pair of positive integers such that $2x + 7y$ divides $7x+2y$. Let d denote the positive integer such that $7x+2y$ is equal to $(2x+7y)d$. This gives

$$7(x - dy) = 2(dx - y).$$

Since the integers $2, 7$ are relatively prime, it follows that 2 divides $x - dy$ and 7 divides $dx - y$. This shows that

$$\frac{x - dy}{2} = \frac{dx - y}{2} = k$$

holds for some integer k. This shows that

$$x - dy = 2k, \quad dx - y = 7k,$$

which gives

$$(d^2 - 1)x = (7d - 2)k, \quad (d^2 - 1)y = (7 - 2d)k.$$

Since y is positive, we obtain $d \leq 3$. Note that if $d = 1$, then $k = 0$ and hence $x = y$. If $d = 2$, then (x, y) is equal to $(4k, k)$, and if $d = 3$, then (x, y) is equal to $(\frac{19}{8}k, \frac{1}{8}k)$, in which case k is a multiple of 8. So (x, y) is an element of the set

$$\bigcup_{r=1}^{\infty} \{(r, r), (4r, r), (19r, r)\}.$$

Also note that for any element (a, b) of this set, the integer $2a + 7b$ divides $7a + 2b$. This proves that the required pairs form the above set. ■

Example 1.43 (India RMO 2014b P4)**.** For any positive integer $n > 1$, let $P(n)$ denote the largest prime not exceeding n. Let $N(n)$ denote the next prime larger than $P(n)$. (For example $P(10) = 7$ and $N(10) = 11$, while $P(11) = 11$ and $N(11) = 13$.) If $n + 1$ is a prime number, prove that the value of the sum

$$\frac{1}{P(2)N(2)} + \frac{1}{P(3)N(3)} + \frac{1}{P(4)N(4)} + \cdots + \frac{1}{P(n)N(n)} = \frac{n-1}{2n+2}.$$

Solution 40. Let p_n denote the n-th prime for $n \geq 1$. Note that for any integer m with $p_n \leq m \leq p_{n+1} - 1$, the integer $P(m)N(m)$ is equal to $p_n p_{n+1}$. This gives

$$\sum_{m=p_n}^{p_{n+1}-1} \frac{1}{P(m)N(m)} = \frac{p_{n+1} - p_n}{p_n p_{n+1}} = \frac{1}{p_n} - \frac{1}{p_{n+1}}.$$

Let k denote the positive integer such that $n+1$ is equal to p_k. Note that

$$\begin{aligned}
&\frac{1}{P(2)N(2)}+\frac{1}{P(3)N(3)}+\frac{1}{P(4)N(4)}+\cdots+\frac{1}{P(n)N(n)}\\
&=\sum_{m=p_1}^{p_2-1}\frac{1}{P(m)N(m)}+\sum_{m=p_2}^{p_3-1}\frac{1}{P(m)N(m)}+\cdots+\sum_{m=p_{k-1}}^{p_k-1}\frac{1}{P(m)N(m)}\\
&=\left(\frac{1}{p_1}-\frac{1}{p_2}\right)+\left(\frac{1}{p_2}-\frac{1}{p_3}\right)+\cdots+\left(\frac{1}{p_{k-1}}-\frac{1}{p_k}\right)\\
&=\frac{1}{p_1}-\frac{1}{p_k}\\
&=\frac{1}{2}-\frac{1}{n+1}\\
&=\frac{n-1}{2n+2}.
\end{aligned}$$

■

Example 1.44 (India RMO 2014d P3)**.** Determine all pairs $m>n$ of positive integers such that

$$1=\gcd(n+1,m+1)=\gcd(n+2,m+2)=\cdots=\gcd(m,2m-n).$$

Solution 41. Let $m>n$ be positive integers satisfying the given condition. It follows that

$$1=\gcd(n+1,m-n)=\gcd(n+2,m-n)=\cdots=\gcd(m,m-n).$$

Note that the positive integer $m-n$ is relatively prime to the $m-n$ consecutive integers

$$n+1,n+2,\ldots,m.$$

This implies that $m-n=1$.

Note that if $m-n=1$ holds for two positive integers, then

$$1=\gcd(n+1,m-n)=\gcd(n+2,m-n)=\cdots=\gcd(m,m-n)$$

holds, and which yields

$$1=\gcd(n+1,m+1)=\gcd(n+2,m+2)=\cdots=\gcd(m,2m-n).$$

This proves that the pairs (m,n) satisfying the given condition are precisely of the pairs of the form $(n+1,n)$ as n ranges over the positive integers. ■

Example 1.45 (India RMO 2016d P3)**.** The present ages in years of two brothers A and B, and their father C are three distinct positive integers a, b, and c respectively. Suppose $\frac{b-1}{a-1}$ and $\frac{b+1}{a+1}$ are two consecutive integers, and $\frac{c-1}{b-1}$ and $\frac{c+1}{b+1}$ are two consecutive integers. If $a+b+c\leq 150$ determine a,b and c.

Solution 42. Note that

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

holds, and

$$\frac{c-1}{b-1}-\frac{c+1}{b+1}=\frac{(b+1)(c-1)-(b-1)(c+1)}{b^2-1}=\frac{2(c-b)}{b^2-1}$$

holds. Note that if $a>b$, then

$$\frac{2(a-b)}{a^2-1}=1$$

holds, which yields

$$2-2b=(a-1)^2,$$

which gives $a=2$, and $b=0$, which is impossible since $b\geq 1$. This shows that $a\leq b$. It follows that

$$\frac{2(b-a)}{a^2-1}=1,\quad \frac{2(c-b)}{b^2-1}=1$$

hold. This yields

$$2(b-a)=a^2-1,$$
$$2(c-b)=b^2-1,$$

which implies

$$2b=a^2+2a-1,$$
$$2c=b^2+2b-1.$$

Note that a,b are odd, and

$$2(b+1)=(a+1)^2,$$
$$2(c+1)=(b+1)^2$$

holds. This shows that

$$a+b+c+3=a+1+\frac{(a+1)^2}{2}+\frac{(a+1)^4}{8}.$$

Using the bound $a+b+c\leq 150$, we obtain

$$a+1+\frac{(a+1)^2}{2}+\frac{(a+1)^4}{8}\leq 153,$$

which shows that $a\leq 4$. Since a is odd, it follows that $a=3$. It follows that

$$b=7,\quad c=31.$$

Note that the triple $(a,b,c)=(3,7,31)$ satisfies $a+b+c\le 150$, and $\frac{b-1}{a-1}=3$ and $\frac{b+1}{a+1}=2$ are two consecutive integers, and $\frac{c-1}{b-1}=5$ and $\frac{c+1}{b+1}=4$ are two consecutive integers.

This proves that

$$a=3,\quad b=7,\quad c=31.$$

■

Example 1.46 (India RMO 2016c P3)**.** Let a,b,c,d,e,f be positive integers such that

$$\frac{a}{b}<\frac{c}{d}<\frac{e}{f}.$$

Suppose $af-be=-1$. Show that $d\ge b+f$.

Solution 43. The given conditions yield

$$ad<bc,\quad cf<de.$$

This gives

$$adf\le bcf-f\le bde-b-f,$$

which implies

$$d(be-af)\ge b+f.$$

It follows that $d\ge b+f$. ■

Example 1.47 (India RMO 2016g P3)**.** a,b,c,d are integers such that $ad+bc$ divides each of a,b,c and d. Prove that $ad+bc=\pm 1$.

Remark. What happens when a,b,c,d are equal to zero?

Solution 44. Note that there exist integers p,q,r,s such that

$$\begin{aligned}a&=p(ad+bc),\\ b&=q(ad+bc),\\ c&=r(ad+bc),\\ d&=s(ad+bc)\end{aligned}$$

holds. This yields

$$ad+bc=(ps+qr)(ad+bc)^2.$$

If $ad+bc=0$, then all of the integers a,b,c,d are equal to zero, which is impossible. This shows that $ad+bc$ is nonzero, and hence, we obtain

$$(ps+qr)(ad+bc)=1,$$

which implies

$$ad+bc=\pm 1.$$

■

Example 1.48 (India RMO 2016g P6)**.** Positive integers a, b, c satisfy $\frac{1}{a}+\frac{1}{b}+\frac{1}{c}<1$. Prove that $\frac{1}{a}+\frac{1}{b}+\frac{1}{c} \leq \frac{41}{42}$. Also prove that equality in fact holds in the second inequality.

Solution 45. Let a, b, c be positive integers satisfying

$$\frac{1}{a}+\frac{1}{b}+\frac{1}{c}<1. \tag{4}$$

Since $\frac{1}{a}+\frac{1}{b}+\frac{1}{c}$ is symmetric with respect to a, b, c, by reordering them (if necessary), we may (and do) assume that $a \leq b \leq c$. Using **??**, it follows that $a \geq 2$.

Let us consider the case that $a=3$. Using **??** it follows that one of b, c is greater than 3, and hence

$$\begin{aligned}\frac{1}{3}+\frac{1}{3}+\frac{1}{4} &= \frac{2}{3}+\frac{1}{4}\\ &= \frac{9}{12}\\ &= \frac{3}{4}\\ &< \frac{41}{42}\end{aligned}$$

holds.

Now, let us consider the case that $a=2$. Using **??**, it follows that the integers b, c are greater than or equal to 3. If $b=3$, then using **??**, it follows that $c>6$, which shows that

$$\begin{aligned}\frac{1}{a}+\frac{1}{b}+\frac{1}{c} &= \frac{1}{2}+\frac{1}{3}+\frac{1}{c}\\ &\leq \frac{5}{6}+\frac{1}{7}\\ &= \frac{41}{42}\end{aligned}$$

holds. If $b=4$, then using **??**, it follows that $c>4$, which shows that

$$\begin{aligned}\frac{1}{a}+\frac{1}{b}+\frac{1}{c} &= \frac{1}{2}+\frac{1}{4}+\frac{1}{c}\\ &\leq \frac{3}{4}+\frac{1}{5}\\ &= \frac{19}{20}\\ &\leq \frac{41}{42}\end{aligned}$$

holds. If $b \geq 5$ holds, then using **??**, it follows that

$$\frac{1}{a}+\frac{1}{b}+\frac{1}{c} \leq \frac{1}{2}+\frac{2}{b}$$

$$\begin{aligned} &\leq \frac{1}{2} + \frac{2}{5} \\ &= \frac{9}{10} \\ &\leq \frac{41}{42} \end{aligned}$$

holds. This proves the inequality

$$\frac{1}{a} + \frac{1}{b} + \frac{1}{c} \leq \frac{41}{42}.$$

Observing that

$$\frac{1}{2} + \frac{1}{3} + \frac{1}{7} = \frac{41}{42}$$

holds, it follows that equality holds in the above inequality for some choice of a, b, c. ■

Example 1.49 (India RMO 2016e P2)**.** Consider a sequence $(a_k)_{k\geq 1}$ of natural numbers defined as follows: $a_1 = a$ and $a_2 = b$ with $a, b > 1$ and $\gcd(a, b) = 1$ and for all $k > 0$, $a_{k+2} = a_{k+1} + a_k$. Prove that for all natural numbers n and k, $\gcd(a_n, a_{n+k}) < \frac{a_k}{2}$.

Remark. Note that for the above inequality, it is necessary that $a_1 \geq 3$. In fact, **if $a_1 = 2$, then the above inequality is not strict for $k = 1$.**

Solution 46. Consider the sequence $\{f_n\}_{n\geq 1}$ satisfying the recurrence relation

$$f_{n+2} = f_{n+1} + f_n, \qquad \text{for any } n \geq 1,$$

and $f_1 = 0, f_2 = 1$. Note that

$$a_n = af_{n-1} + bf_n, \qquad \text{for any } n \geq 2.$$

Claim — For any integers $n \geq 2, k \geq 1$,

$$f_{n+k-1} = f_{n-1}f_k + f_nf_{k+1}$$

holds.

Proof of the Claim. It suffices to consider the case $k \geq 2$. Note that

$$\begin{pmatrix} 0 & 1 \\ 1 & 1 \end{pmatrix}^n = \begin{pmatrix} f_n & f_{n+1} \\ f_{n+1} & f_{n+2} \end{pmatrix}$$

holds for $n = 1$, and if it holds for $n = m$ for some integer $m \geq 1$, then it holds for $n = m + 1$ since

$$\begin{aligned}\begin{pmatrix} 0 & 1 \\ 1 & 1 \end{pmatrix}^{m+1} &= \begin{pmatrix} 0 & 1 \\ 1 & 1 \end{pmatrix} \begin{pmatrix} f_m & f_{m+1} \\ f_{m+1} & f_{m+2} \end{pmatrix} \\ &= \begin{pmatrix} f_{m+1} & f_{m+2} \\ f_{m+1} + f_m & f_{m+2} + f_{m+1} \end{pmatrix} \\ &= \begin{pmatrix} f_{m+1} & f_{m+2} \\ f_{m+2} & f_{m+3} \end{pmatrix}\end{aligned}$$

holds. This shows that the above holds for any positive integer n. Consequently, for any integers $n, k \geq 2$, it follows that

$$\begin{pmatrix} f_{n-1} & f_n \\ f_n & f_{n+1} \end{pmatrix} \begin{pmatrix} f_k & f_{k+1} \\ f_{k+1} & f_{k+2} \end{pmatrix} = \begin{pmatrix} 0 & 1 \\ 1 & 1 \end{pmatrix}^{n-1+k} = \begin{pmatrix} f_{n+k-1} & f_{n+k} \\ f_{n+k} & f_{n+k+1} \end{pmatrix},$$

which yields

$$f_{n+k-1} = f_{n-1}f_k + f_n f_{k+1}.$$

□

Let n, k be positive integers. Using the above Claim, we obtain

$$\begin{aligned} a_{n+k} &= af_{n+k-1} + bf_{n+k} \\ &= a(f_{n-1}f_k + f_n f_{k+1}) + b(f_{n-1}f_{k+1} + f_n f_{k+2}) \\ &= a(f_{n-1}f_k + f_n f_{k+1}) + b(f_{n-1}f_{k+1} + f_n f_k + f_n f_{k+1}) \\ &= (af_{n-1} + bf_n)f_k + (af_n + bf_{n-1} + bf_n)f_{k+1} \\ &= a_n f_k + (af_n + bf_{n+1})f_{k+1} \\ &= a_n f_k + a_{n+1}f_{k+1}. \end{aligned}$$

This yields

$$\begin{aligned}\gcd(a_n, a_{n+k}) &= \gcd(a_n, a_n f_k + a_{n+1}f_{k+1}) \\ &= \gcd(a_n, a_{n+1}f_{k+1}).\end{aligned}$$

Note that

$$\gcd(a_n, a_{n+1}) = 1$$

holds for $n = 1$, and if it holds for $n = m$ for some positive integer m, then

$$\begin{aligned}\gcd(a_{m+1}, a_{m+2}) &= \gcd(a_{m+1}, a_{m+1} + a_m) \\ &= \gcd(a_{m+1}, a_m) \\ &= 1,\end{aligned}$$

which shows that the integers a_n, a_{n+1} are relatively prime for any positive integer n. If $a_1 \geq 3$, then it follows that

$$\gcd(a_n, a_{n+1}) = 1 < \frac{a_1}{2},$$

that is, for $k = 1$, the inequality

$$\gcd(a_n, a_{n+k}) < \frac{a_k}{2}$$

holds. Moreover, if $k \geq 2$, then using the above, we obtain

$$\begin{aligned}\gcd(a_n, a_{n+k}) &= \gcd(a_n, f_{k+1}) \\ &\leq f_{k+1} \\ &= f_{k-1} + f_k \\ &< \frac{af_{k-1} + bf_k}{2} \\ &= \frac{a_k}{2}.\end{aligned}$$

This completes the proof. ■

Example 1.50 (India RMO 2017a P2)**.** Show that the equation

$$a^3 + (a+1)^3 + \cdots + (a+6)^3 = b^4 + (b+1)^4$$

has no solutions in integers a, b.

Solution 47. Note that the fourth powers of the integers $0, 1, 2, 3, 4, 5, 6$ are congruent to $0, 1, 2, 4, 4, 2, 1$ modulo 7 respectively. The shows that the sum of the fourth powers of two consecutive integers is congruent to one of

$$0 + 1, 1 + 2, 2 + 4, 4 + 2, 2 + 1, 1 + 0$$

modulo 7. Hence, the sum of the fourth powers of two consecutive integers is not divisible by 7. Also note the cubes of seven consecutive integers is congruent to

$$0^3 + 1^3 + 2^3 + 3^3 + 4^3 + 5^3 + 6^3$$

modulo 7, which is congruent to

$$1^3 + 2^3 + 3^3 + (-3)^3 + (-2) + (-1)^3 = 0$$

modulo 7. This shows that the sum of the cubes of seven consecutive integers is not equal to the sum of the fourth powers of two consecutive integers. This completes the proof. ■

Example 1.51 (India RMO 2017b P2)**.** For any positive integer n, let $d(n)$ denote the number of positive divisors of n; and let $\varphi(n)$ denote the number of elements from the set $\{1, 2, \ldots, n\}$ that are coprime to n. (For example, $d(12) = 6$ and $\varphi(12) = 4$.) Find the smallest positive integer n such that $d(\varphi(n)) = 2017$.

Solution 48. Let n be the least among the positive integers (if any) satisfying $d(\varphi(n)) = 2017$. Observe that $\varphi(n)$ is not equal to 1. Let $\varphi(n) = p_1^{\alpha_1} \ldots p_r^{\alpha_r}$ denote the factorization of $\varphi(n)$ into the product of the powers of distinct primes. We obtain

$$(\alpha_1 + 1) \ldots (\alpha_r + 1) = 2017.$$

Noting that 2017 is a prime, it follows that $r = 1$, and $\alpha_1 = 2016$, that is, $\varphi(n)$ is the 2016-th power of a prime. Since $\varphi(n)$ is larger than 1, it follows that it is an even number, and hence, $\varphi(n)$ is equal to 2^{2016}. Note that if an odd prime q divides n, then q^2 does not divide n, and $q - 1$ is a power of 2. It follows that n is equal to $2^k p_1 \ldots p_m$ where k, m are nonnegative integers, and $p_1 < \cdots < p_m$ are distinct odd primes, and $p_i - 1$ is a power of 2 for any $1 \leq i \leq m$.

> **Claim —** If p is an odd prime such that $p - 1$ is a power of 2, then p is equal to $2^{2^i} + 1$ for some integer $i \geq 0$.

Proof of the Claim. It suffices to consider the case $p \geq 5$. Write $p = 2^a + 1$. Note that $a \geq 2$. If a is odd, then p is divisible by 3, and $p > 3$, which is a contradiction to the primality of p. This shows that a is even. If a is not a power of 2, then writing $a = 2^b c$ for some positive integers b, c, with c an odd integer, it follows that p is divisible by $2^{2^b} + 1$, which shows that c is equal to 1. This completes the proof. □

Note that the above Claim shows that for any $1 \leq i \leq m$, p_i is equal to $2^{2^{a_i}} + 1$ for some nonnegative integer a_i.

> **Claim —** For no integer $1 \leq i \leq m$, the prime p_i is equal to $2^{2^5} + 1$.

Proof of the Claim. Note that $641 = 5 \cdot 2^7 + 1$ is a prime. This gives $5 \cdot 2^7 \equiv -1 \bmod 641$, which yields $5^4 \cdot 2^{28} \equiv 1 \bmod 641$. Using $641 = 2^4 + 5^4$, it follows that $2^{32} + 1$ is divisible by 641. Since $2^{32} + 1$ is larger than $5 \cdot 2^7 + 1 = 641$, the Claim follows. □

Let us first consider the case that $k = 0$. Since $\varphi(n) = 2^{2016} < 2^{2^{11}}$ holds, it follows that

$$p_m \leq 2^{2^{10}} + 1.$$

The first Claim shows that $\{p_1, \ldots, p_m\}$ is a subset of

$$\left\{2^{2^i} + 1 \,|\, 0 \leq i \leq 10\right\}.$$

This shows that

$$\begin{aligned} 2^{2016} &= \varphi(p_1 \dots p_m) \\ &\le \prod_{0\le i\le 10, i\ne 5} 2^{2^i} \quad \text{(using the second Claim)} \\ &= 2^{1+2+4+8+16+64+128+256+512+1024} \\ &= 2^{2015}, \end{aligned}$$

which is impossible.

Let us consider the case that $k \ge 1$. If $m \ge 1$, then note that

$$n > 2^k(p_1 - 1)(p_2 - 1)\dots(p_m - 1)$$

and

$$\varphi(n) = \varphi(2^k(p_1 - 1)(p_2 - 1)\dots(p_m - 1))$$

hold, which contradicts the minimality of n. This shows that $m = 0$, that is, n is a power of 2, and hence, $n = 2^{2017}$.

Noting that

$$d(\varphi(2^{2017})) = d(2^{2016}) = 2017$$

holds, it follows that the smallest positive integer n satisfying $d(\varphi(n)) = 2017$ is 2^{2017}. ■

Example 1.52 (India RMO 2018a P5)**.** Find all natural numbers n such that $1 + [\sqrt{2n}]$ divides $2n$. (For any real number x, $[x]$ denotes the largest integer not exceeding x.)

Solution 49. Let n be a positive integer such that $1 + [\sqrt{2n}]$ divides $2n$. Write

$$2n = m^2 + k$$

where m is a positive integer, and k is an integer satisfying $0 \le k \le 2m$. Note that

$$1 + [\sqrt{2n}] = m + 1$$

holds. Since $1 + [\sqrt{2n}]$ divides $2n$, it follows that

$$\begin{aligned} \frac{2n}{1 + [\sqrt{2n}]} &= \frac{m^2 + k}{m + 1} \\ &= \frac{(m + 1)^2 - 2(m + 1) + k + 1}{m + 1} \\ &= m - 1 + \frac{k + 1}{m + 1} \end{aligned}$$

is an integer, which shows that $m+1$ divides $k+1$. Using $0 \le k \le 2m$, we obtain $k = m$, which yields

$$n = \frac{m(m+1)}{2}.$$

Conversely, if n is equal to

$$\frac{m(m+1)}{2}$$

for some positive integer m, then $1 + [\sqrt{2n}]$ divides $2n$.

This proves that the positive integers satisfying the given condition are precisely the integers of the form

$$\frac{m(m+1)}{2}$$

for some positive integer m. ■

Example 1.53 (India RMO 2018a P3)**.** For a rational number r, its *period* is the length of the smallest repeating block in its decimal expansion, for example, the number $r = 0.123123123\ldots$ has period 3. If S denotes the set of all rational numbers of the form $r = 0.\overline{abcdefgh}$ having period 8, find the sum of all elements in S.

Solution 50. The sum of all rational numbers of the form $0.\overline{abcdefgh}$ is equal to

$$\sum_{0 \le i_1, i_2, \ldots, i_8 \le 9} \left(\frac{i_1}{10} + \frac{i_2}{10^2} + \cdots + \frac{i_8}{10^8} \right) \frac{1}{1 - \frac{1}{10^8}}.$$

Note that the rational numbers of the form $0.\overline{abcdefgh}$ which have period less than 8, are of period 1 or 2 or 4, and hence, they are of the form $0.\overline{abcd}$. The sum of such rational numbers is equal to

$$\sum_{0 \le i_1, i_2, i_3, i_4 \le 9} \left(\frac{i_1}{10} + \frac{i_2}{10^2} + \cdots + \frac{i_4}{10^4} \right) \frac{1}{1 - \frac{1}{10^4}}.$$

It follows that the sum of the rational numbers of the given form having period 8 is equal to

$$\begin{aligned}
&\sum_{0 \le i_1, i_2, \ldots, i_8 \le 9} \left(\frac{i_1}{10} + \frac{i_2}{10^2} + \cdots + \frac{i_8}{10^8} \right) \frac{1}{1 - \frac{1}{10^8}} \\
&- \sum_{0 \le i_1, i_2, i_3, i_4 \le 9} \left(\frac{i_1}{10} + \frac{i_2}{10^2} + \cdots + \frac{i_4}{10^4} \right) \frac{1}{1 - \frac{1}{10^4}} \\
&= 10^7 \left(\sum_{i=0}^{9} i \right) \left(\frac{1}{10} + \frac{1}{10^2} + \cdots + \frac{1}{10^8} \right) \frac{1}{1 - \frac{1}{10^8}}
\end{aligned}$$

$$
\begin{aligned}
&- 10^3 \left(\sum_{i=0}^{9} i\right) \left(\frac{1}{10} + \frac{1}{10^2} + \cdots + \frac{1}{10^4}\right) \frac{1}{1 - \frac{1}{10^4}} \\
&= \frac{10^7}{9} \left(\sum_{i=0}^{9} i\right) - \frac{10^3}{9} \left(\sum_{i=0}^{9} i\right) \\
&= 5 \times 10^7 - 5 \times 10^3 \\
&= (50000 - 5) \times 10^3 \\
&= 49995000.
\end{aligned}
$$

■

Solution 51. Note that the rational numbers of the form $0.\overline{abcdefgh}$, not having period 8, have period 1 or 2 or 4, and hence, are of the form $0.\overline{abcd}$. This shows that there are precisely $10^8 - 10^4$ rational numbers of the form $0.\overline{abcdefgh}$, having period 8.

Observe that

$$0.\overline{abcdefgh} \mapsto 0.\overline{\mathsf{abcdefgh}},$$

where $\mathsf{x} = 9 - x$ for any $x \in \{a, b, c, d, e, f, g, h\}$, defines a map of order two from S to S, and this map has no fixed points. This shows that each element of S can be paired with its image under this map, and it produces $\frac{1}{2}|S|$ many pairs. Note that the sum of the elements of any such pair is equal to

$$0.\overline{999999} = 1.$$

Consequently, the sum of the elements of S is equal to

$$\frac{1}{2}|S| = \frac{10^8 - 10^4}{2} = 49995000.$$

■

Example 1.54 (India RMO 2019b P1)**.** For each $n \in \mathbb{N}$ let d_n denote the gcd of n and $(2019 - n)$. Find value of $d_1 + d_2 + \cdots + d_{2018} + d_{2019}$.

Solution 52. Note that for a positive integer n, the greatest common divisor of n and $2019 - n$ divides $n + (2019 - n) = 2019 = 3 \cdot 673$. Observe that $3, 673$ are primes. This shows that for an integer n satisfying $1 \leq n < 2019$, the greatest common divisor of n and $2019 - n$ is equal to

$$
\begin{cases}
1 & \text{if } n \text{ is relatively prime to 3 and to 673,} \\
3 & \text{if 3 divides } n, \\
673 & \text{if 673 divides } n.
\end{cases}
$$

This yields

$$d_1 + d_2 + \cdots + d_{2018} + d_{2019}$$

$$
\begin{aligned}
&= \sum_{\substack{1\le n<2019,\\ \gcd(n,2019)=1}} 1 + \sum_{\substack{1\le n<2019,\\ 3\mid n}} 3 + \sum_{\substack{1\le n<2019,\\ 673\mid n}} 673 + 2019 \\
&= 2019 - \frac{2019}{3} - \frac{2019}{673} + \frac{2019}{3\cdot 673} + 3\cdot 672 + 673\cdot 2 + 3\cdot 673 \\
&= 2\cdot 672 + 3\cdot 672 + 5\cdot 673 \\
&= 5\cdot 1345 \\
&= 6725.
\end{aligned}
$$

■

Example 1.55 (India RMO 2023a P2)**.** Given a prime number p such that $2p$ is equal to the sum of the squares of some four consecutive positive integers. Prove that $p-7$ is divisible by 36.

Solution 53. Let p be a prime satisfying the given condition. Write

$$2p = x^2 + (x+1)^2 + (x+2)^2 + (x+3)^2$$

where x is a positive integer. Note that

$$
\begin{aligned}
x^2 + (x+1)^2 + (x+2)^2 + (x+3)^2 &= 4x^2 + 12x + 14 \\
&\equiv 4x(x+1) + 6 \bmod 8 \\
&\equiv 6 \bmod 8
\end{aligned}
$$

holds. It follows that $2p$ is congruent to 6 modulo 8, which shows that p is congruent to 3 modulo 4.

Note that if $x \equiv \pm 1 \bmod 3$, then

$$
\begin{aligned}
x^2 + (x+1)^2 + (x+2)^2 + (x+3)^2 &= 4x^2 + 12x + 14 \\
&\equiv x^2 + 2 \bmod 3 \\
&\equiv 0 \bmod 3
\end{aligned}
$$

holds, which shows that 3 divides $2p$, and hence $p = 3$. However, 6 cannot be expressed as the sum of four consecutive positive integers since $3^2 > 6$. This shows that x is divisible by 3. It follows that

$$
\begin{aligned}
x^2 + (x+1)^2 + (x+2)^2 + (x+3)^2 &= 4x^2 + 12x + 14 \\
&\equiv 14 \bmod 9.
\end{aligned}
$$

So, $2p - 14$ is a multiple of 9, and hence, it is an even multiple of 9, implying that $p-7$ is a multiple of 9. Since $p \equiv 3 \bmod 4$, we obtain $p \equiv 7 \bmod 36$. ■

Example 1.56 (India RMO 2023b P1)**.** Let $\mathbb{N}$ be the set of all positive integers and

$$S = \left\{(a,b,c,d) \in \mathbb{N}^4 : a^2+b^2+c^2 = d^2\right\}.$$

Find the largest positive integer m such that m divides $abcd$ for all $(a,b,c,d) \in S$.

Solution 54. Let m denote the largest positive integer such that it divides $abcd$ for all (a,b,c,d) in S. Note that $1^2+2^2+2^2 = 3^2$ holds, which shows that $(1,2,2,3)$ lies in S. This shows that m divides 12.

Let (a,b,c,d) be an element of S. Note that at least one of a,b,c,d is divisible by 3 since

$$(\pm 1)^2+(\pm 1)^2+(\pm 1)^2 \not\equiv (\pm 1)^2 \bmod 3.$$

Also note that if all of a,b,c,d are odd, then we obtain

$$(\pm 1)^2+(\pm 1)^2+(\pm 1)^2 \equiv (\pm 1)^2 \bmod 4,$$

which is impossible. It follows that at least one of a,b,c,d is even.

If d is even, then at least one of a,b,c is even because the sum of squares of three odd integers is congruent to 3 modulo 4. If d is odd, then at least one of a,b,c is even. Note that $0+(\pm 1)^2+(\pm 1)^2 \not\equiv (\pm 1)^2 \bmod 4$, which shows that if d is odd, then at least two of a,b,c are even. This implies that at least two of a,b,c,d are even. Hence, m is divisible by $2\cdot 2\cdot 3 = 12$.

This proves that $m = 12$. ■

Example 1.57 (India RMO 2024a P1)**.** Find all positive integers x,y such that $202x+4x^2 = y^2$.

Solution 55. Let x,y be positive integers satisfying $202x+4x^2 = y^2$. Note that y^2 is even, and hence, so is y. This shows that 4 divides $y^2-4x^2 = 202x$. It follows that x is even.

Note that

$$4y^2 = (4x)^2 + 2\cdot 101\cdot(4x)$$

holds, which gives

$$101^2 = (4x+101-2y)(4x+101+2y). \tag{5}$$

Since x,y are positive integers, it follows that $4x+101-2y < 4x+101+2y$. This shows that

$$4x+101-2y = 1, \quad 4x+101+2y = 101^2, \tag{6}$$

which yields

$$x = 1250, \quad y = 2550.$$

Also note that if $x = 1250$ and $y = 2550$, then **??** holds, which yields **??**, which implies $202x + 4x^2 = y^2$. Hence, the solution to the given equation in the positive integers is precisely

$$x = 1250, \quad y = 2550.$$

■

Example 1.58 (India RMO 2024a P4)**.** Let $n > 1$ be a positive integer. Call a rearrangement $a_1, a_2, \ldots, a_n$ of $1, 2, \ldots, n$ *nice* if for every $k = 2, 3, \ldots, n$, we have that $a_1^2 + a_2^2 + \cdots + a_k^2$ is not divisible by k. Determine which positive integers $n > 1$ have a nice arrangement.

Solution 56. If n is an odd positive integer and is not divisible by 3, then the sum of the squares of $1, 2, \ldots, n$, that is, the integer

$$\frac{n(n+1)(2n+1)}{6}$$

is a multiple of n. This shows that if $n > 1$ is an integer relatively prime to 6, then $1, 2, \ldots, n$ do not admit any nice rearrangement.

Claim — For any positive integer k, the following rearrangement of $1, 2, \ldots, 6k$ (to be read accross the rows)

$$\begin{array}{cccccc} 2 & 1 & 3 & 4 & 6 & 5 \\ 8 & 7 & 9 & 10 & 12 & 11 \\ 14 & 13 & 15 & 16 & 18 & 17 \\ \vdots & \vdots & \vdots & \vdots & \vdots & \vdots \\ 6k-4 & 6k-5 & 6k-3 & 6k-2 & 6k & 6k-1 \end{array}$$

is nice.

Proof of the Claim. Note that

$$\begin{aligned} \frac{2^2+1^2}{2} &= \frac{(2+1)(2\cdot 2+1)}{6} \\ \frac{2^2+1^2+3^2}{3} &= \frac{(3+1)(2\cdot 3+1)}{6} \\ \frac{2^2+1^2+3^2+4^2}{4} &= \frac{(4+1)(2\cdot 4+1)}{6} \\ \frac{2^2+1^2+3^2+4^2+6^2}{5} &= \frac{(5+1)(2\cdot 5+1)}{6} + \frac{6^2-5^2}{5} \\ \frac{2^2+1^2+3^2+4^2+6^2+5^2}{6} &= \frac{(6+1)(2\cdot 6+1)}{6} \end{aligned}$$

are not integers. This proves the Claim for $k = 1$. Let k be a positive integer such that the Claim holds. Consider the rearrangement (to be read accross the rows)

$$\begin{array}{cccccc} 2 & 1 & 3 & 4 & 6 & 5 \\ 8 & 7 & 9 & 10 & 12 & 11 \\ 14 & 13 & 15 & 16 & 18 & 17 \\ \vdots & \vdots & \vdots & \vdots & \vdots & \vdots \\ 6k-4 & 6k-5 & 6k-3 & 6k-2 & 6k & 6k-1 \\ 6k+2 & 6k+1 & 6k+3 & 6k+4 & 6k+6 & 6k+5 \end{array}$$

of $1, 2, \ldots, 6k+6$. Note that

$$\frac{\sum_{i=1}^{6k} i^2 + (6k+2)^2}{6k+1} = \frac{6k(12k+1)}{6} + \frac{(6k+2)^2}{6k+1}$$

is not an integer since the integers $6k+1, 6k+2$ are relatively prime and $6k+1$ is larger than 1. Observe that

$$\frac{\sum_{i=1}^{6k} i^2 + (6k+2)^2 + (6k+1)^2}{6k+2} = \frac{(6k+3)(12k+5)}{6}$$

is not an integer since the integers $6k+3, 12k+5$ are odd. Also note that

$$\frac{\sum_{i=1}^{6k} i^2 + (6k+2)^2 + (6k+1)^2 + (6k+3)^2}{6k+3} = \frac{(6k+4)(12k+7)}{6}$$

since 3 does not divide any of $6k+4, 12k+7$. Notice that

$$\frac{\sum_{i=1}^{6k} i^2 + (6k+2)^2 + (6k+1)^2 + (6k+3)^2 + (6k+4)^2}{6k+4} = \frac{(6k+5)(12k+9)}{6}$$

is not an integer since $6k+5, 12k+9$ are odd integers. Observe that

$$\begin{aligned} &\frac{\sum_{i=1}^{6k} i^2 + (6k+2)^2 + (6k+1)^2 + (6k+3)^2 + (6k+4)^2 + (6k+6)^2}{6k+5} \\ &= \frac{(6k+6)(12k+11)}{6} + \frac{(6k+6)^2 - (6k+5)^2}{6k+5} \end{aligned}$$

is not an integer since the integers $6k+5, 6k+6$ are relatively prime and $6k+5$ is larger than 1. Also note that

$$\begin{aligned} &\frac{\sum_{i=1}^{6k} i^2 + (6k+2)^2 + (6k+1)^2 + (6k+3)^2 + (6k+4)^2 + (6k+6)^2 + (6k+5)^2}{6k+6} \\ &= \frac{(6k+7)(12k+13)}{6} \end{aligned}$$

is not an integer since the integers $6k+7, 12k+13$ are relatively prime to 6. By induction, the Claim holds for any positive integer k. □

By the above Claim, it follows that if n is a positive integer and n is not relatively prime to 6, then the integers $1, 2, \ldots, n$ admit a nice rearrangement.

This proves that the positive integers $n > 1$, admitting a nice rearrangement, are precisely those which are not relatively prime to 6. ■

Example 1.59 (India RMO 2024b P1)**.** Let $n > 1$ be a positive integer. Call a rearrangement $a_1, a_2, \ldots, a_n$ of $1, 2, \ldots, n$ *nice* if for every $k = 2, 3, \ldots, n$, we have that $a_1 + a_2 + \cdots + a_k$ is not divisible by k.

1. If $n > 1$ is odd, prove that there is no nice arrangement of $1, 2, \ldots, n$.
2. If n is even, find a nice arrangement of $1, 2, \ldots, n$.

Solution 57. Note that if $n > 1$ is an odd positive integer, then for any rearrangement $a_1, a_2, \ldots, a_n$ of $1, 2, \ldots, n$, the integer

$$a_1 + \cdots + a_n = 1 + 2 + \cdots + n = n \times \frac{n+1}{2}$$

is divisible by n. This proves the first part.

For any even positive integer n, a nice rearrangement of $1, 2, \ldots, n$ is provided by the Claim below.

> **Claim —** For any even positive integer n,
>
> $$2, 1, 4, 3, 6, 5, 8, 7, \ldots, n, n-1$$
>
> is a nice rearrangement of $1, 2, \ldots, n$.

Proof of the Claim. Note that the Claim holds for $n = 2$. Let n be an even positive integer satisfying the Claim. Consider the rearrangement

$$2, 1, 4, 3, 6, 5, 8, 7, \ldots, n, n-1, n+2, n+1$$

of $1, 2, \ldots, n+2$. Note that the sum of its first $n+1$ terms is equal to

$$(n+1) \times \frac{n+2}{2} + 1,$$

which is not a multiple of $n+1$. Also note that the sum of the integers $1, 2, \ldots, n+2$ is equal to

$$(n+2) \times \frac{n+3}{2},$$

which is not a multiple of $n+2$. By the induction hypothesis, it follows that the rearrangement

$$2, 1, 4, 3, 6, 5, 8, 7, \ldots, n, n-1, n+2, n+1$$

of $1, 2, \ldots, n+2$ is nice. This proves the Claim. □

■

Example 1.60 (India RMO 2024b P2)**.** For a positive integer n, let $R(n)$ be the sum of the remainders when n is divided by $1, 2, \ldots, n$. For example, $R(4) = 0+0+1+0 = 1$, $R(7) = 0+1+1+3+2+1+0 = 8$. Find all positive integers such that $R(n) = n-1$.

Walkthrough —

(a) Note that

$$\begin{aligned}
R(1) &= 0,\\
R(2) &= 0,\\
R(3) &= 0+1+0\\
&= 1,\\
R(4) &= 0+0+1+0\\
&= 1,\\
R(5) &= 0+1+2+1+0\\
&= 4,\\
R(6) &= 0+0+0+2+1+0\\
&= 3,\\
R(7) &= 0+1+1+3+2+1+0\\
&= 8,\\
R(8) &= 0+0+2+0+3+2+1+0\\
&= 8,\\
R(9) &= 0+1+0+1+4+3+2+1+0\\
&= 12,\\
R(10) &= 0+0+1+2+0+4+3+2+1+0\\
&= 13
\end{aligned}$$

holds.

(b) Does the above help?

Solution 58. For positive integers n and k, denote by $r(n,k)$ the remainder obtained upon dividing n by k. Note that any integer $k \geq 4$,

$$\begin{aligned}
R(2k) &\geq r(2k,k-1) + r(2k,k+1) + r(2k,k+2) + \cdots + r(2k,2k-1)\\
&= 2 + (k-1) + (k-2) + \cdots + 1\\
&= 2 + \frac{k(k-1)}{2}\\
&\geq 2k
\end{aligned}$$

holds. Also note that any integer $k \geq 3$,

$$\begin{aligned} R(2k+1) &\geq r(2k+1,k) + r(2k+1,k+1) \\ &\quad + r(2k+1,k+2) + \cdots + r(2k+1,2k-1) + r(2k+1,2k) \\ &= 1 + k + (k-1) + \cdots + 2 + 1 \\ &= 1 + \frac{k(k+1)}{2} \\ &\geq 2k+1 \end{aligned}$$

holds. Note that

$$\begin{aligned} R(1) &= 0, \\ R(2) &= 0, \\ R(3) &= 0+1+0 \\ &= 1, \\ R(4) &= 0+0+1+0 \\ &= 1, \\ R(5) &= 0+1+2+1+0 \\ &= 4, \\ R(6) &= 0+0+0+2+1+0 \\ &= 3 \end{aligned}$$

holds. This proves that the positive integers n satisfying $R(n) = n-1$ are precisely $1, 5$. ■

§1.2 More on congruences

Theorem 1 (Wilson)

For any prime p, the congruence

$$(p-1)! \equiv -1 \pmod{p}$$

holds.

Example 1.61. Let $n \geq 5$ be an integer. Show that n is composite if and only if n divides $(n-1)!$.

Solution 59. If n is a prime, then by Wilson's theorem, it follows that n does not divide $(n-1)!$. This proves the "if part".

To prove the "only if part", note that if n is composite, then the highest power of any of its prime divisors is at most $n-1$, and hence divides $(n-1)!$, and since these powers are pairwise coprime, it follows that n divides $(n-1)!$. ■

Theorem 2 (Fermat's little theorem)
If p is prime, and a is an integer not divisible by p, then

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

holds.

Example 1.62 (IMOSL 1984 P2)**.** Prove that if m, n are positive integers, then $4mn - m - n$ cannot be a perfect square.

Solution 60. Let m, n be positive integers such that $4mn - m - n = k^2$ holds for some positive integer k^2. This yields

$$(4m-1)(4n-1) = 4k^2 + 1.$$

Since $4m - 1$ is a positive integer and it is congruent to 3 modulo 4, it admits a prime divisor p satisfying $p \equiv 3 \bmod 4$. Note that p divides $4k^2 + 1$, and p does not divide $2k$. Applying Fermat's little theorem, it follows that

$$(-1)^{\frac{p-1}{2}} \equiv ((2k)^2)^{\frac{p-1}{2}} \equiv 1 \bmod p,$$

which is impossible since $p \equiv 3 \bmod 4$. ■

Example 1.63 (India RMO 1990 P4)**.** Find the remainder when 2^{1990} is divided by 1990.

Solution 61. Since 199 is a prime, by Fermat's little theorem, we obtain

$$2^{198} \equiv 1 \bmod 199,$$

which yields

$$2^{1990} \equiv 2^{1980} \cdot 2^{10} \bmod 199 \equiv 29 \bmod 199.$$

Using $2^4 \equiv 1 \bmod 5$, we get

$$2^{1990} \equiv 4 \bmod 5 \equiv 29 \bmod 5.$$

Since $5, 199$ are coprime, this shows that

$$2^{1990} \equiv 29 \bmod 199 \cdot 5.$$

Observe that

$$2^{1990} - (29 + 199 \cdot 5)$$

is divisible by $199 \cdot 5$, and also by 2. Since $2, 199 \cdot 5$ are coprime, it follows that

$$2^{1990} \equiv 29 + 199 \cdot 5 \bmod 2 \cdot 199 \cdot 5,$$

which implies that

$$2^{1990} \equiv 1024 \bmod 1990.$$

So, one obtains 1024 as the remainder upon dividing 2^{1990} by 1990. ■

Example 1.64 (India RMO 1990 P6)**.** N is a 50 digit number (in the decimal scale). All digits except the 26th digit (from the left) are 1. If N is divisible by 13, find the 26th digit.

Solution 62. Let a denote the 26-th digit of N. The given condition yields

$$N = 1 + 10 + 10^2 + \cdots + 10^{49} + (a-1)10^{50-26}.$$

Assume that N is divisible by 13. This gives

$$1 + 10 + 10^2 + \cdots + 10^{49} + (a-1)10^{24} \equiv 0 \bmod 13.$$

Applying Fermat's little theorem, we obtain $10^{12} \equiv 1 \bmod 13$, and this shows that

$$10^{24} \equiv 1 \bmod 13, \quad 10^{50} - 1 \equiv 10^2 - 1 \bmod 13.$$

Note that

$$9(1 + 10 + 10^2 + \cdots + 10^{49}) + 9(a-1)10^{24} \equiv 0 \bmod 13$$

holds, which shows that

$$10^{50} - 1 + 9(a-1)10^{24} \equiv 0 \bmod 13,$$

and this implies that

$$10^2 - 1 + 9(a-1) \equiv 0 \bmod 13.$$

Since the integers $9, 13$ are relatively prime, we obtain

$$11 + a - 1 \equiv 0 \bmod 13.$$

It follows that $a = 3$. ■

Theorem 3 (Euler)

Let n be a positive integer, and $\varphi(n)$ denote the number of integers lying between 1 and n which are relatively prime to n. If a is an integer relatively prime to n, then

$$a^{\varphi(n)} \equiv 1 \pmod{n}$$

holds.

Example 1.65 (India RMO 1993 P5)**.** Show that $19^{93} - 13^{99}$ is a positive integer divisible by 162.

Solution 63. Note that the congruences

$$\begin{aligned} 19^{93} &\equiv (1+18)^{93} \bmod 9^2 \\ &\equiv 1 + 93 \cdot 18 \bmod 9^2 \\ &\equiv 1 + 12 \cdot 18 \bmod 9^2 \\ &\equiv 1 + 8 \cdot 27 \bmod 9^2 \\ &\equiv 1 - 27 \bmod 9^2 \\ &\equiv -26 \bmod 9^2 \\ &\equiv 55 \bmod 9^2, \\ 13^{99} &\equiv (4+9)^{99} \bmod 9^2 \\ &\equiv 4^{99} + 99 \cdot 4^{98} \cdot 9 \bmod 9^2 \\ &\equiv 4^{99} \bmod 9^2 \end{aligned}$$

hold. Also note that

$$\begin{aligned} 4^{81} &\equiv 1 + 81 \cdot 3 + \binom{81}{2} 3^2 + \binom{81}{3} 3^3 \bmod 9^2 \\ &\equiv 1 \bmod 9^2 \end{aligned}$$

holds, which yields

$$\begin{aligned} 4^{99} &\equiv 4^{81} \cdot 4^{18} \bmod 81 \\ &\equiv 4^{18} \bmod 81 \\ &\equiv (1+3)^{18} \bmod 81 \\ &\equiv 1 + 18 \cdot 3 + \frac{18 \cdot 17}{2} 3^2 + \frac{18 \cdot 17 \cdot 16}{6} 3^3 \bmod 81 \\ &\equiv 1 + 18 \cdot 3 \bmod 81 \\ &\equiv 55 \bmod 81. \end{aligned}$$

It follows that $19^{93} - 4^{99}$ is divisible by 81, and hence, $19^{93} - 13^{99}$ is divisible by 81. Since $19^{93} - 13^{99}$ is an even number, and $2, 81$ are coprime, we conclude that $19^{93} - 13^{99}$ is divisible by 162. ■

Example 1.66 (India RMO 2015f P3)**.** Let

$$N = 2^5 + 2^{5^2} + 2^{5^3} + \cdots + 2^{5^{2015}},$$

written in the usual decimal form, find the last two digits of the number N.

Solution 64. Applying Euler's theorem, we obtain [1]

$$2^{20} \equiv 2^{\varphi(25)} \equiv 1 \bmod 25.$$

[1] Alternatively, one may observe that $2^{10} = 1024 \equiv -1 \bmod 25$, which yields $2^{20} \equiv 2^{\varphi(25)} \equiv 1 \bmod 25$.

Note that for any integer $n \geq 1$,

$$5^n - 5 = 5(5^{n-1} - 1) = 5((1+4)^{n-1} - 1)$$

holds, and hence we obtain $5^n \equiv 5 \bmod 20$. This yields

$$N = 2^5 \left(\sum_{i=1}^{2015} 2^{5^i - 5} \right) = 2^5 \left(\sum_{i=1}^{2015} (2^{20})^{\frac{5^i - 5}{20}} \right),$$

and consequently, we obtain

$$N \equiv 2^5 \cdot 2015 \equiv 7 \cdot 15 \equiv 5 \bmod 25.$$

Also note that $N \equiv 0 \bmod 4$ holds. It follows that $N - 80$ is divisible by the relatively prime integers $4, 25$, which shows that 100 divides $N - 80$. Hence, the last two digits of N are $8, 0$. ■

References

[**AE11**] Titu Andreescu and Bogdan Enescu. *Mathematical Olympiad treasures*. Second. Birkhäuser/Springer, New York, 2011, pp. viii+253. ISBN: 978-0-8176-8252-1; 978-0-8176-8253-8

[**Che25**] Evan Chen. *The OTIS Excerpts*. Available at https://web.evanchen.cc/excerpts.html. 2025, pp. vi+289

[**Eng98**] Arthur Engel. *Problem-solving strategies*. Problem Books in Mathematics. Springer-Verlag, New York, 1998, pp. x+403. ISBN: 0-387-98219-1

[**FGI96**] Dmitri Fomin, Sergey Genkin, and Ilia Itenberg. *Mathematical circles (Russian experience)*. Vol. 7. Mathematical World. Translated from the Russian and with a foreword by Mark Saul. American Mathematical Society, Providence, RI, 1996, pp. xii+272. ISBN: 0-8218-0430-8

[**Tao06**] Terence Tao. *Solving mathematical problems*. A personal perspective. Oxford University Press, Oxford, 2006, pp. xii+103. ISBN: 978-0-19-920560-8; 0-19-920560-4