Contents

Preface

The second volume, Book 2, of *Introduction to Number Theory in Mathematics Contests* focuses on the most important classical, basically polynomial congruences, and arithmetic functions. We believed that it was important to remind the reader the main concepts covered in Book 1, so we decided to include in Chapter 1 numerous problems to accomplish this goal but also other beautiful problems with unique and interesting results. For example, among these one can find the remarkably beautiful Erdős-Ginzburg-Ziv theorem (stating that among any $2n-1$ integers one can find n whose sum is divisible by n), and also some other classical results arising from the Prime Number Theorem. The important (because of its many applications) "lifting the exponent" lemma can also be found here. We strongly recommend readers to independently try to solve these problems before looking at the solutions provided, since this would help with honing their problem-solving skills and, also, give them the chance to realize how challenging each problem really is.

Chapter 2 is about some of the most important classical theorems in the theory of congruences: Euler's, Fermat's, and Wilson's theorems are cornerstones in this domain – and we present them together with a multitude of applications. Included in this chapter is also the beautiful theorem of Lucas about binomial coefficients modulo a prime, Lagrange's theorem on the number of solutions of a polynomial congruence modulo a prime, along with their interesting and intriguing applications. Chapter 2 culminates with Gauss's theorem about the existence/non-existence of primitive roots modulo an arbitrary positive integer.

Finally, in Chapter 3 we give a short but comprehensive exposition of the arithmetic functions, such as the number of divisors, the sum of divisors, Euler's totient function, and, of course, the ubiquitous Möbius functions. We present their basic properties together with many problems involving and invoking them. At the end of the chapter we use cyclotomic polynomials to prove that any arithmetic progression with its first term 1 contains infinitely many primes – the most important case of the celebrated Dirichlet's theorem (stating the same for an arithmetic progression whose first term and common

difference are relatively prime) for which an elementary proof is known – and this is not the only remarkable result obtained with the help of cyclotomic polynomials.

We gratefully thank Richard Stong for carefully reading the manuscript and for providing truly valuable observations, comments, and new proofs that enlightened the exposition.

Titu Andreescu
Marian Tetiva

Chapter 1

Initial Problem Set

We start this second Book of our *Introduction to Number Theory* with a few problems that will hopefully help the reader to recall the most important results and techniques presented in Book 1. The only criterion that we had in mind for the ordering of the problems is their increasing difficulty (and even this one is subjective). We invite the reader to work carefully on each of the following exercises and problems before reading their solutions, and before studying the expository material starting with Chapter 2.

1. Find the least number of the form $\overline{abaaba}$ that can be written as a product of six distinct primes.

   Proof. Note that

   $$\overline{abaaba} = 1000 \cdot \overline{aba} + \overline{aba} = 1001 \cdot \overline{aba} = 7 \cdot 11 \cdot 13 \cdot \overline{aba},$$

   so we need to find the smallest a for which $\overline{aba}$ is the product of three distinct primes not equal to any of $7, 11$, or 13. Checking $a = 1$ we do not get such a number (101 is a prime, $111 = 3 \cdot 37$, $121 = 11^2$, and so on; check all the possibilities!). Setting $a = 2$ we obtain that $202 = 2 \cdot 101$, $212 = 2^2 \cdot 53$ (with 101 and 53 being primes), and, finally, we get $222 = 2 \cdot 3 \cdot 37$ which has three different prime factors, distinct from any of 7, 11, 13. The answer is therefore $222222 = 2 \cdot 3 \cdot 7 \cdot 11 \cdot 13 \cdot 37$. □

2. Prove that among any three distinct integers we can find two, a and b, such that $a^3b - ab^3$ is divisible by 10.

   Proof. Note that $a^3b - ab^3 \equiv ab - ab = 0 \bmod 2$, hence we only need to ensure that $ab^3 - a^3b = ab(a^2 - b^2)$ is a multiple of 5. If one of the chosen numbers is a multiple of 5, we are done (we let this number

to be, for example, a). Otherwise, their squares give remainders 1 or 4 when divided by 5 (only two possibilities). Hence we can find two numbers a, b among the given three, for which $a^2 \equiv b^2 \bmod 5$. Then $a^3b - ab^3 = ab(a^2 - b^2)$ is a multiple of 10, as desired. □

3. Let a, $b \neq 0$, c, and $n > 0$ be integers such that a is divisible by b, $a \equiv bc \bmod n$, and b is invertible modulo n. Then we have $\frac{a}{b} \equiv c \bmod n$.

   Proof. Recall that b is invertible modulo n if there exists an integer b' such that $bb' \equiv 1 \bmod n$, and that this happens if and only if b is relatively prime to n.

   Thus, by hypothesis, we have $a = bc + kn$ for some integer k, and b is relatively prime to n. Since b divides $a - bc = kn$ and $\gcd(b, n) = 1$, it follows that b divides k. Thus we have

   $$\frac{a}{b} = c + \frac{k}{b}n \equiv c \bmod n,$$

   as desired. □

4. Find all integers n such that $4n+17$ and $8n-19$ are not relatively prime.

   Proof. If $4n+17$ and $8n-19$ have a common factor greater than 1, then this must also be a factor of

   $$8(4n + 17) - 4(8n - 19) = 212 = 2^2 \cdot 53.$$

   Since 4 does not divide either of $4n+17$ and $8n-19$, and 53 is a prime, the only chance to have $\gcd(4n + 17, 8n - 19) > 1$ is to actually have $\gcd(4n+17, 8n-19) = 53$. So, the solutions that we are looking for are the solutions of the congruence $4n + 17 \equiv 0 \bmod 53$ — note that they also satisfy $8n - 19 \equiv 0 \bmod 53$, due to the above equality. Since 40 is a multiplicative inverse of 4 modulo 53, the congruence is equivalent to

   $$160n + 680 \equiv 0 \bmod 53 \Leftrightarrow n \equiv 9 \bmod 53,$$

   hence the solutions of the problem are the numbers of the form $9 + 53k$, with integer k (for each of which $4n + 17$ and $8n - 19$ are both divisible by 53 — and actually their greatest common divisor is 53). □

5. Prove that for any positive integer n there exist n consecutive integers $a_1, \ldots, a_n$ (in increasing order) such that a_j can be expressed as the sum of j distinct perfect squares for any $j = 1, \ldots, n$.

Proof. Let $a \geq 2$ be an integer, and let $a_j = 4a^{2^n} + j - 1$ for $j = 1, \ldots, n$. Then, clearly, a_1 is a square, while for $j = 2, \ldots, n$ we have that

$$a_j = 4a^{2^n} + j - 1 = \left(2a^{2^{n-1}} - 1\right)^2 + \left(2a^{2^{n-2}} - 1\right)^2 + \cdots + \left(2a^{2^{n-j+1}} - 1\right)^2 + (2a^{2^{n-j}})^2$$

is a sum of j distinct squares, as desired.

Despite its folkloric flavor, the problem was proposed by Arne Smeets in *Nieuw Archief voor Wiskunde*. This solution is essentially the solution of Thijmen Krebs and Josephine Buskes (from the same magazine). □

6. Show that a positive integer n can be expressed as the sum of at least two consecutive positive integers if and only if n is not a power of 2 with nonnegative exponent.

Proof. The positive integer n can be represented as the sum of k consecutive positive integers if and only if there exist a nonnegative integer m such that

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

Write $n = 2^s(2t+1)$ for some nonnegative integers s and t. For $t = 0$ the above equality turns into

$$k(2m+k+1) = 2^{s+1},$$

thus yielding

$$k = 2^u \text{ and } 2m + k + 1 = 2^v,$$

with nonnegative integers u and v such that $u+v = s+1$ and $u < v$. But k and $2m+k+1$ have different parities, so this forces $u = 0$, and therefore $k = 1$. Thus we have shown that if n is a power of 2 with nonnegative exponent, then its only expression as the sum of consecutive positive integers is as a (trivial) one-term sum.

On the other hand, assume that $n = 2^s(2t+1)$ is not a power of 2, meaning that $t \geq 1$ (hence $2t+1 \geq 3$). Then the necessary and sufficient equality

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

becomes

$$k(2m+k+1) = 2^{s+1}(2t+1).$$

This equation is satisfied for

$$k = 2^{s+1} \text{ and } m = t - 2^s,$$

and also for

$$k = 2t + 1 \text{ and } m = 2^s - t - 1.$$

Since we need $m \geq 0$, we see that the first solution satisfies all the required conditions if $2^s \leq t$, and the second if $2^s \geq t + 1$. Thus for n not a power of 2, we always get a solution, and the proof is complete.

For instance, for $n = 54$, we get $s = 1$ and $t = 13$, and hence

$$54 = 2(2 \cdot 13 + 1) = 12 + 13 + 14 + 15$$

while for $n = 56$, we get $s = 3$ and $t = 3$, and hence

$$56 = 2^3(2 \cdot 3 + 1) = 5 + 6 + 7 + 8 + 9 + 10 + 11.$$

□

7. Given that

$$34! = \overline{295232799cd960414084761860964 35ab000000},$$

determine the digits a, b, c, d.

Proof. We could of course simply compute 34! and solve this problem, but it is more amusing to use what we know about divisibility to recover a, b, c, d less computationally.

The number of trailing zeros for 34! is

$$\left\lfloor \frac{34}{5} \right\rfloor + \left\lfloor \frac{34}{25} \right\rfloor = 6 + 1 = 7,$$

which implies $b = 0$. We have

$$34! = 2^{32} \cdot 3^{15} \cdot 5^7 \cdot 7^4 \cdot 11^3 \cdot 13^2 \cdot 17^2 \cdot 19 \cdot 23 \cdot 29 \cdot 31$$

and

$$\overline{295232799cd960414084761860964 35a} = \frac{34!}{10^7}$$

$$= 2^{25} \cdot 3^{15} \cdot 7^4 \cdot 11^3 \cdot 13^2 \cdot 17^2 \cdot 19 \cdot 23 \cdot 29 \cdot 31 \equiv 2 \mod 10,$$

hence $a = 2$.

Since 34! is divisible by 9 the sum of its digits $141+c+d$ is divisible by 9, therefore $c+d+6$ is divisible by 9. Also, because 34! is divisible by 11, the alternating sum of its digits $19-c+d$ is divisible by 11, thus $d-c-3$ is divisible by 11. Consequently, $c+d$ could be 3 or 12, while $d-c$ could be -8 or 3. Examining all possibilities we see that $(c,d)=(0,3)$ is the only solution. Thus the required digits of 34! are $a=2$, $b=0$, $c=0$, and $d=3$. □

8. Find all positive integers n for which the number $2\ldots25$ (written with n twos followed by one five in base 10) is a perfect square.

Proof. (Titu Andreescu, *Mathematical Reflections*) Clearly, $n=1$ and $n=2$ are solutions to the problem (as $25=5^2$ and $225=15^2$). We will show that for no other n is $2\ldots25$ (with n twos) a perfect square.

To this purpose let $n\geq 3$ be an integer, and notice first that

$$\underbrace{2\ldots2}_{n\ 2\text{s}}5=\underbrace{2\ldots2}_{n-1\ 2\text{s}}00+25=\underbrace{2\ldots2}_{n-1\ 2\text{s}}\cdot 4\cdot 25+25=\underbrace{8\ldots8}_{n-1\ 8\text{s}}\cdot 25+25=25\cdot\underbrace{8\ldots8}_{n-2\ 8\text{s}}9,$$

thus, if we assume that $2\ldots25$ (with n 2s) is a square, so is $8\ldots89$ (with $n-2$ 8s). We also have (simply by performing the multiplication)

$$\underbrace{8\ldots8}_{n-2\ 8\text{s}}9\cdot 9=8\underbrace{0\ldots0}_{n-2\ 0\text{s}}1,$$

hence, if $8\ldots89$ (with $n-2$ digits of 8) is a perfect square, so is $80\ldots01$ (with $n-2$ digits of 0). Because $80\ldots01$ is odd, there must exist a nonnegative integer k such that

$$8\underbrace{0\ldots0}_{n-2\ 0\text{s}}1=(2k+1)^2\Leftrightarrow 8\cdot 10^{n-1}+1=4k^2+4k+1\Leftrightarrow 2^n\cdot 5^{n-1}=k(k+1).$$

As k and $k+1$ are relatively prime and each of them must be (according to the above equality and unique factorization) a product of factors equal to either 2, or 5, we infer that we have either

$$k=2^n\ \text{ and }\ k+1=5^{n-1},$$

or

$$k=5^{n-1}\ \text{ and }\ k+1=2^n.$$

It follows that

$$2^n=5^{n-1}\pm 1\geq 5^{n-1}-1,$$

which is false for $n\geq 3$, since

$$2^n=2^{n-2}\cdot 4<5^{n-2}\cdot 4=5^{n-1}-5^{n-2}<5^{n-1}-1.$$ □

Remarks 1.1. 1) The equality

$$9 \cdot \underbrace{2 \ldots 2}_{n \text{ 2s}} 5 = 25 \cdot 8 \underbrace{0 \ldots 0}_{n-2 \text{ 0s}} 1$$

(for $n \geq 2$) is the key for this solution of the problem. It can also be proved by using the decimal representation of the involved numbers, which we invite the reader to do.

2) Again, we invite the reader to show that the number $1 \ldots 16$ (written in base 10 with n digits of 1 followed by a 6) is a perfect square if and only if $n = 1$. Perhaps the equality

$$9 \cdot \underbrace{1 \ldots 1}_{n \text{ 1s}} 6 = 4 \cdot 25 \underbrace{0 \ldots 0}_{n-3 \text{ 0s}} 11$$

($n \geq 3$) will be helpful to achieve this goal (although the last step is not the same as in the proof above). More simply, just divide $1 \ldots 16$ by 4; what do you get, and how do you finish the proof?

9. Let a, b, and c be nonnegative integers such that $ab \geq c^2$. Prove that integers $s \geq 1$ and $x_i \geq 0$, $y_i \geq 0$ for $i = 1, \ldots, s$ exist such that

$$a = \sum_{i=1}^{s} x_i^2, \quad b = \sum_{i=1}^{s} y_i^2, \quad \text{and} \quad c = \sum_{i=1}^{s} x_i y_i.$$

Proof. We use strong induction on c. The result is true for (the base case) $c = 0$, as we can choose

$$s = a + b, \ x_1 = \cdots = x_a = 1, \ x_{a+1} = \cdots = x_{a+b} = 0,$$

$$y_1 = \cdots = y_a = 0, \text{ and } y_{a+1} = \cdots = y_{a+b} = 1.$$

(If $a = b = 0$ we can choose s to be any positive integer, and all x_i and y_i to be 0.)

Assume now that the statement of the problem holds true for any triple (a', b', c'), with nonnegative integers a', b', and c' satisfying $a'b' \geq c'^2$ and $c' < c$, and let us prove it for the triple (a, b, c) of nonnegative integers a, b, and c satisfying $ab \geq c^2$. We can consider that a, b, and c are positive integers, since any of $a = 0$ or $b = 0$ forces $c = 0$, and we already solved this case.

First note that if $a > c$ and $b > c$, we can choose $s = a + b - c$, and

$$x_1 = \cdots = x_a = 1, \ \ x_{a+1} = \cdots = x_{a+b-c} = 0,$$

and

$$y_1 = \cdots = y_{a-c} = 0, \;\; y_{a-c+1} = \cdots = y_{a+b-c} = 1$$

for which

$$a = \sum_{i=1}^{s} x_i^2, \;\; b = \sum_{i=1}^{s} y_i^2, \;\; \text{and} \;\; c = \sum_{i=1}^{s} x_i y_i.$$

Thus we can assume further that $a \leq c$ or $b \leq c$; without loss of generality we may consider $a \leq c$, hence $c - a$ is a nonnegative integer. Also, we have

$$a + b \geq 2\sqrt{ab} \geq 2c,$$

meaning that $a + b - 2c$ is also a nonnegative integer. But we have

$$a(a + b - 2c) - (c - a)^2 = ab - c^2 \geq 0,$$

and $c' = c - a < c$, and therefore the inductive hypothesis applies to the triple (a', b', c'), where $a' = a$, $b' = a + b - 2c$, and $c' = c - a$. This means that we can find nonnegative integers $s \geq 1$ and $x'_1, \ldots, x'_s, y'_1, \ldots, y'_s$ such that

$$a = \sum_{i=1}^{s} x_i'^2, \;\; a + b - 2c = \sum_{i=1}^{s} y_i'^2, \;\; \text{and} \;\; c - a = \sum_{i=1}^{s} x'_i y'_i.$$

From these relations we immediately get

$$a = \sum_{i=1}^{s} x_i'^2, \;\; b = \sum_{i=1}^{s} (x'_i + y'_i)^2, \;\; \text{and} \;\; c = \sum_{i=1}^{s} x'_i (x'_i + y'_i),$$

which is the desired result, since it says that

$$a = \sum_{i=1}^{s} x_i^2, \;\; b = \sum_{i=1}^{s} y_i^2, \;\; \text{and} \;\; c = \sum_{i=1}^{s} x_i y_i,$$

for $x_i = x'_i$ and $y_i = x'_i + y'_i$ $(i = 1, \ldots, s)$.

We invite the reader to notice the similarity between this problem's solution and the solution of the problem presented in section 1.2 from Book 1, and to reformulate that proof in terms of strong induction, as we did here. □

10. Prove that any positive integer can be expressed as the difference of two positive integers having the same number of distinct prime divisors.

Proof. We have $1 = 3 - 2$ and $n = 2n - n$ for any even positive integer (where, clearly, n and $2n$ have the same number of prime divisors), so it remains to prove that the statement holds for any odd integer $n > 1$. Let $q_1 = 3, q_2 = 5, \ldots$ be the sequence of odd primes in increasing order. If n is not divisible by $3 = q_1$, then $n = 4n - 3n$ is the desired expression. Otherwise, let $s \geq 2$ be the smallest integer such that n is not divisible by q_s — thus n *is* divisible by each of $q_1, \ldots, q_{s-1}$, and n *is not* divisible by q_s. Then we finish our proof by writing $n = (q_s + 1)n - q_s n$, where both $(q_s + 1)n$ and $q_s n$ have the same number of distinct prime divisors. (The prime divisors of $(q_s + 1)n$ are $2, q_1, \ldots, q_{s-1}$, and the other odd prime divisors of n, while the prime divisors of $q_s n$ are $q_1, \ldots, q_{s-1}, q_s$ and the other odd prime divisors of n.) □

11. If n is a given positive integer, then there exist distinct positive integers $a_1, \ldots, a_n$ such that all the numbers

$$\sum_{i \in I} a_i$$

with I a nonempty subset of $\{1, \ldots, n\}$ have the same prime factors.

Proof. We use the simple idea that b and $a \cdot b$ have the same prime divisors whenever a and b are positive integers such that a divides b. So, we choose $N = \dfrac{n(n+1)}{2}$, and the numbers $a_i = N!i$ for $i \in \{1, \ldots, n\}$. Then

$$\sum_{i \in I} a_i = N! \sum_{i \in I} i$$

has precisely the same prime factors as $N!$, for every $\emptyset \neq I \subseteq \{1, \ldots, n\}$, because

$$\sum_{i \in I} i \leq 1 + \cdots + n = \frac{n(n+1)}{2} = N,$$

hence $\sum_{i \in I} i$ is a divisor of $N!$ for any such I. □

12. Let m, n, and r be positive integers. Prove that the following statements are equivalent:

(i) There exists an integer x such that $x \equiv r \bmod m$ and x is relatively prime to n.

(ii) We have that $\gcd(m, r)$ and n are relatively prime.

Proof. (i)⇒(ii) If $x = um + r$ (for some integer u) is relatively prime to n, then $\gcd(m, r)$ divides x, hence it is also relatively prime to n.

(ii)⇒(i) Suppose that $\gcd(m, r)$ and n are relatively prime. Let $p_1, \ldots, p_s$ be all the distinct primes that divide n, but do not divide r and let $P = p_1 \cdots p_s$ be their product. Take $x = mP + r = mp_1 \cdots p_s + r$. Since $p_1, \ldots, p_s$ do not divide r, they also do not divide x. Thus any common prime factor p of x and n must also divide r. But then it follows that $p \mid x - r = mP$. Since p divides r, it cannot be one of the prime factors of P, so this implies $p \mid m$. This would make p a common factor of $\gcd(m, r)$ and n, contrary to (ii). Thus x is relatively prime to n. Since it is clear that $x \equiv r \pmod{m}$, (i) follows. □

Remark 1.2. Dirichlet's theorem about primes in arithmetic progressions immediately solves the second implication. Indeed, the arithmetic progression

$$\frac{m}{\gcd(m, r)}u + \frac{r}{\gcd(m, r)}, \quad u = 1, 2, \ldots$$

contains infinitely many primes, so we can choose one of them, say q, which is greater than all the prime factors of n. Then $x = q \gcd(m, r)$ is congruent to r modulo m, and also relatively prime to n.

13. Find all positive integers n such that any integer x relatively prime to n satisfies $x^2 \equiv 1 \bmod n$.

Proof. The required values of n are 1, 2, 3, 4, 6, 8, 12, 24 (all the positive divisors of 24). Suppose n is a positive integer for which $x \in \mathbb{Z}$ and $\gcd(x, n) = 1$ imply $x^2 \equiv 1 \bmod n$.

We first show that 5 cannot divide n. Suppose, on the contrary, that 5 is a divisor of n. By the result of the previous exercise (for $m = 5$ and $r = 2$), we can find some $x \equiv 2 \bmod 5$ such that x and n are relatively prime. According to the hypothesis, we must have $x^2 \equiv 1 \bmod n$, and, since 5 divides n, this implies $x^2 \equiv 1 \bmod 5$, which is clearly false (we have $x^2 \equiv 4 \not\equiv 1 \bmod 5$).

Thus 5 does not divide n, hence 5 is relatively prime to n. Again the hypothesis implies $5^2 \equiv 1 \bmod n$, that is, n is a divisor of 24.

It is easy to verify that all these values of n work, based on two simple observations that we already made a few times: first, if x is an integer relatively prime to 3, then $x^2 \equiv 1 \bmod 3$ (as x is congruent to either 1, or -1 modulo 3), and second: if x is an odd integer, then $x^2 \equiv 1 \bmod 8$ (remember why!). We leave it to the reader to complete the details. □

Proof. For another approach, let us denote by Q the property of an integer n that $x^2 \equiv 1 \bmod n$ whenever $\gcd(x, n) = 1$. We show first that n has property Q if and only if each power of a prime $p^{v_p(n)}$ from the prime factorization of n has property Q.

Indeed, suppose that n has property Q, and let $p^{v_p(n)}$ be such a prime power. Assume that an integer x is relatively prime to $p^{v_p(n)}$, and consider the product r of the (distinct) primes that divide n, but not x. Then $x+p^{v_p(n)}r$ is relatively prime to n, hence $(x+p^{v_p(n)}r)^2 \equiv 1 \bmod n$, by hypothesis. Therefore $(x + p^{v_p(n)}r)^2 \equiv 1 \bmod p^{v_p(n)}$, which clearly leads to $x^2 \equiv (x + p^{v_p(n)}r)^2 \equiv 1 \bmod p^{v_p(n)}$. Conversely, if every prime power dividing n has property Q, and x is relatively prime to n, then x is also relatively prime to each such prime power, so $x^2 - 1$ is divisible by each such prime power, and, consequently, $x^2 - 1$ is divisible by n, so $x^2 \equiv 1 \bmod n$.

Considering this, we see that no prime p greater than 3 can appear in the factorization of n, since 2 is relatively prime to p, but $2^2 = 4 \not\equiv 1 \bmod p$. Also since 3 is relatively prime to 2^k, but $3^2 = 9 \not\equiv 1 \bmod 2^k$ for $k \geq 4$, we see that $v_2(n) \leq 3$ (the exponent of 2 in the factorization of n is at most 3). Similarly, because 2 is relatively prime to 3^k and $2^2 = 4 \not\equiv 1 \bmod 3^k$ for $k \geq 2$, we must have $v_3(n) \leq 1$. We conclude that $n = 2^a 3^b$ with natural numbers $a \leq 3$, and $b \leq 1$, leading to the same values of n as in the first proof. (Checking them completely is still left to the reader!) □

14. Find all pairs of positive integers (a, b) such that both $a! + b$ and $a + b!$ are powers of 5 with a natural exponent.

Proof. (Junior Balkan Mathematical Olympiad 2023) The solutions are $(1, 4)$, $(4, 1)$, and $(5, 5)$.

First, if (a, b) is a solution with $a = b$, then we must have that $a! + a$ is a power of 5, so $(a - 1)! + 1$ is also a power of 5 (as a divisor of a power of 5). Since $(a - 1)! + 1 \geq 2$, it must be a multiple of 5, yielding that $(a-1)! = ((a-1)!+1) - 1$ is *not* a multiple of 5. This implies $a-1 \leq 4$, and, by checking all the possibilities, we find the solution $(a, b) = (5, 5)$, for which $5! + 5 = 5^3$ is a power of 5, as required. We further search for the solutions of the problem with distinct a and b.

Suppose, without loss of generality, that we have a solution with $b < a$. Then b is one of the factors in $a!$ and hence $b \mid a!$. Since b divides $a! + b$ which is a power of 5, it follows that b is a power of 5 and

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

is also a power of 5. Since $\frac{a!}{b}+1 \geq 2$, this forces $\frac{a!}{b}+1$ to be a multiple of 5, and, consequently, $\frac{a!}{b} = \left(\frac{a!}{b}+1\right) - 1$ is *not* a multiple of 5. Thus

$$\frac{a!}{b} = 1 \cdot \ldots \cdot (b-1) \cdot (b+1) \cdot \ldots \cdot a$$

is not a multiple of 5, implying that $b \leq 5$ and $a \leq 4$ (otherwise there is a multiple of 5 among $1, \ldots, b-1, b+1, \ldots, a$). So, actually, $1 \leq b < a \leq 4$, and a quick inspection shows that among all these six possible pairs only $(a, b) = (4, 1)$ satisfies the requirements of the problem (we have $4! + 1 = 5^2$ and $4 + 1! = 5$). By symmetry, we also get the solution $(a, b) = (1, 4)$. □

Proof. For a second approach, let us start by reminding a few things.

First recall that, given a positive integer n and a prime p, the exponent of p in the factorization of $n!$ is (by a theorem of Legendre)

$$v_p(n!) = \sum_{j \geq 1} \left\lfloor \frac{n}{p^j} \right\rfloor.$$

Consequently, if $v_p(n) \geq s$ for some $s \geq 0$ (meaning that $n = p^s t$ for some positive integer t), then

$$v_p(n!) = v_p((p^s t)!) \geq (p^{s-1} + \cdots + 1)t \geq \frac{p^s - 1}{p-1}.$$

For $t = 1$ the above inequality becomes an equality:

$$v_p((p^s)!) = \frac{p^s - 1}{p-1}.$$

Also recall that for integers m, n and a prime p we have

$$v_p(m \pm n) \geq \min\{v_p(m), v_p(n)\},$$

while for nonnegative integers s and t and an odd prime p

$$v_p(p^s \pm p^t) = \min\{s, t\}$$

holds, except for the case when the sign is minus and $s = t$.

Moreover, we will use Bernoulli's inequality

$$(1+u)^n \geq 1 + nu, \quad u > -1, \quad n \in \mathbb{N}$$

which follows by induction on n. For $u \geq 0$ the inequality is an immediate consequence of the binomial expansion:

$$(1+u)^n = 1 + nu + \binom{n}{2}u^2 + \cdots + \binom{n}{n}u^n \geq 1 + nu.$$

We invite the reader to exercise the inductive proof and to observe that the equality

$$(1+u)^n = 1 + nu$$

holds if and only if either $u = 0$, or $n \in \{0, 1\}$ (so, only for $n \in \{0, 1\}$ whenever $u > 0$). In particular

$$5^n \geq 1 + 4n \Leftrightarrow \frac{5^n - 1}{4} \geq n$$

for any nonnegative integer n, with equality only for $n = 0$ or $n = 1$.

Now we solve the problem. We have $a! + b = 5^u$ and $a + b! = 5^v$ for some natural numbers (actually positive integers) u and v, and, by symmetry, we can assume that $a \geq b$. Then b is a divisor of $a! + b = 5^u$, hence $b = 5^x$ for some natural number x. Then

$$v_5(b!) = v_5((5^x)!) = \frac{5^x - 1}{4},$$

thus

$$v_5(a) = v_5(5^v - b!) \geq \min\{v, v_5(b!)\} = v_5(b!) = \frac{5^x - 1}{4}$$

(the minimum is so because $5^v > b! \geq 5^{v_5(b!)}$). We get

$$v_5(a!) \geq \frac{5^{v_5(a)} - 1}{4} \geq \frac{5^{\frac{5^x - 1}{4}} - 1}{4} \geq \frac{5^x - 1}{4} \geq x.$$

On the other hand,

$$v_5(a!) = v_5(5^u - 5^x) = x,$$

therefore all the above inequalities must be equalities. This gives either $x = 0$, or $x = 1$.

For $x = 0$ we have $b = 5^0 = 1$ and the equations $a! + 1 = 5^u$, $a + 1 = 5^v$. Clearly, for $a \geq 5$ the first equation does not hold modulo 5, so we only have to check a from $\{1, 2, 3, 4\}$. We find that only 4 works ($4! + 1 = 5^2$, $4 + 1! = 5$), and we thus obtain the solutions $(1, 4)$ and $(4, 1)$.

For $x = 1$ we get $b = 5$ and the equations $a! + 5 = 5^u$ and $a + 120 = 5^v$. From the second equation we see that a is a multiple of 5, and the first one does not hold modulo 25 for $a \geq 10$. Thus we must have $a = 5$, which indeed satisfies both equations (which are, in this case, the same). Thus this case gives the solution $(5, 5)$. □

Remarks 1.3. 1) We leave it to the reader to check that, if a and b are allowed to be nonnegative integers, we get the additional solution $(0, 0)$. Also, we invite the reader to notice the similarities, but also the differences between the two solutions.

2) The same proof works for 2, or 3, instead of 5. More precisely, we invite the reader to prove that the only pairs (a, b) of positive integers for which both $a! + b$ and $a + b!$ are powers of 2 are $(1, 1)$ and $(2, 2)$, while the only pairs (a, b) of positive integers for which both $a! + b$ and $a + b!$ are powers of 3 are $(1, 2)$, $(2, 1)$, and $(3, 3)$.

Actually, one can show (exactly as in the previous proof), that if both $a! + b$ and $a + b!$ are powers of a prime p, then the smaller of a and b is either 1, or p. Unfortunately, to find all the solutions for an arbitrary prime $p > 5$ seems unachievable with only elementary tools.

15. Let a, b, c, and d be integers. Find necessary and sufficient conditions for $an + b$ and $cn + d$ to be relatively prime for any integer n.

Proof. An obvious necessary condition to have $\gcd(an + b, cn + d) = 1$ for any integer n is $\gcd(b, d) = 1$ — and assume this is the case. Then note that the equality

$$a(cn + d) - c(an + b) = ad - bc$$

holds for any n, and suppose that a prime p divides $ad-bc$, but it does not divide a. Since a is relatively prime to p, the congruence $ax+b \equiv 0 \bmod p$ is solvable, hence we can find an integer n satisfying it, that is, such that

$$an + b \equiv 0 \bmod p.$$

Multiplying this by d, and using the divisibility of $ad - bc$ by p, we get

$$b(cn + d) \equiv bcn + bd \equiv adn + bd \equiv 0 \bmod p,$$

Now, if p divides b, since it also divides $ad - bc$, it follows that p divides ad; but p does not divide a, hence we get $p \mid d$, and the assumption that b and d are relatively prime is contradicted. So p does not divide b, hence $b(cn + d) \equiv 0 \bmod p$ implies $cn + d \equiv 0 \bmod p$. We summarize: when $\gcd(b, d) = 1$, if a prime p exists such that p divides $ad-bc$, but p does not divide a, then we can find an integer n such that $\gcd(an + b, cn + d) > 1$ (p divides both $an + b$ and $cn + d$). Similarly, the existence of a prime that divides $ad - bc$, but does not divide c leads to the same conclusion. Thus, for $\gcd(an + b, cn + d) = 1$ to hold for all integers n it is necessary