1. Verify that 8 always divides the difference of the squares of two odd numbers.

2. True or false?
(a) $(a \mid b \text{ and } a \mid c) \Longrightarrow a \mid 3b-5c$; (b) $a \mid b+c \Longrightarrow (a \mid b \text{ and } a \mid c)$;
(c) $ab \mid c \Longrightarrow (a \mid c \text{ and } b \mid c)$; (d) $(a \mid c \text{ and } b \mid c) \Longrightarrow ab \mid c$;
(e) $(a \mid b \text{ or } a \mid c) \Longrightarrow a \mid bc$; (f) $a \mid bc \Longrightarrow (a \mid b \text{ or } a \mid c)$;
(g) $(a \mid b+c \text{ and } a \mid b-c) \Longrightarrow (a \mid b \text{ and } a \mid c)$;
(h) $(a \mid 2b+3c \text{ and } a \mid 3b+5c) \Longrightarrow (a \mid b \text{ and } a \mid c)$.

3. Verify the following divisibilities:
(i) $a-b \mid a^n - b^n$; (ii) $a+b \mid a^{2k+1}+b^{2k+1}$; (iii) $a+b \mid a^{2k}-b^{2k}$.

4. If $m \mid a-b$, i.e. a and b give the same remainder upon division by m, then we say that "a is *congruent* to b modulo m" and denote it by $a \equiv b \pmod m$. E.g. $-5 \equiv 7 \pmod 4$, but $3 \not\equiv 10 \pmod 5$. Verify: If $a \equiv b$ and $c \equiv d \pmod m$, then $a \pm c \equiv b \pm d$ and $ac \equiv bd \pmod m$. What about a/c and b/d?

5. (Digits are understood in decimal system.)
(a) Prove that 9 divides n iff 9 divides the sum of its digits.
(b) Prove that 11 divides n iff 11 divides the alternating sum of its digits.
(c) We add the digits of 2^{2019}, then add the digits of the number obtained, etc. until we get a one-digit number. Determine this final number.
(d) Prove that $43 \mid 6^{n+2} + 7^{2n+1}$ holds for every $n \geq 0$.

6. True or false? ($[k,n]$ denotes the least common multiple of k and n.)
(a) $k \mid n,\ a \equiv b \pmod n \Longrightarrow a \equiv b \pmod k$;
(b) $k \mid n,\ a \equiv b \pmod k \Longrightarrow a \equiv b \pmod n$;
(c) $a \equiv b \pmod n,\ a \equiv b \pmod k \iff a \equiv b \pmod{kn}$;
(d) $a \equiv b \pmod n,\ a \equiv b \pmod k \iff a \equiv b \pmod{[k,n]}$;
(e) $a \equiv b \pmod n \iff ka \equiv kb \pmod{kn}$;
(f) $a \equiv b \pmod n,\ c \equiv d \pmod k \Longrightarrow ac \equiv bd \pmod{kn}$;
(g) $a^2 \equiv b^2 \pmod n \Longrightarrow a \equiv \pm b \pmod n$;
(h) $a^2 \equiv b^2 \pmod{101} \Longrightarrow a \equiv \pm b \pmod{101}$.

7. Consider any infinite integer sequence $a_1, a_2, a_3, \ldots$ Prove that there are infinitely many a_i such that the difference of any two of them is divisible by 2019.

8. We take a maximal set of integers where any two give distinct remainders upon division by n. What is the remainder of their sum?

9. In a fun run with n participants we added the serial and ranking numbers for each runner (e.g. if a contestant wore 7 on her T-shirt and was the 2nd quickest, then we considered the sum $7+2=9$). We noted that the n sums obtained give distinct remainders upon division by n. Is this possible if n is (a) 99; (b) 100?

10. (a) There are m trees around a circular clearing with a squirrel on each tree. The squirrels want to get together on one tree, but they are allowed to move only the following way: In every minute, any two squirrels may jump to an adjacent tree. For which values of m can they gather on one tree?

(b) What happens if we modify the admissible step so that the two squirrels must jump to the adjacent trees in opposite directions (i.e. one of them clockwise, and the other counter-clockwise).

11. Euler's function $\varphi(n)$ is defined as the number of integers coprime to n in $\{1, 2, \ldots, n\}$. E.g. $\varphi(10) = 4$. If the standard form of n is $n = p_1^{k_1} \ldots p_r^{k_r}$ where p_j are distinct primes and $k_j > 0$, then $\varphi(n) = p_1^{k_1-1}(p_1 - 1) \ldots p_r^{k_r-1}(p_r - 1)$.

(a) Prove this formula if n is a prime power.

(b) For which values of n is $\varphi(n)$ odd?

12. *Euler–Fermat Theorem*: If c and m are coprime, then $c^{\varphi(m)} \equiv 1 \pmod{m}$. (There are elementary proofs, but we shall prove it using group theory.)

(a) Formulate the special case when m is a prime (this is *Fermat's Little Theorem*).

(b) What are the last two digits of 1357^{8642}?

*(c) Prove that a square number plus one cannot have a prime divisor of the form $4k - 1$.

13. A *linear congruence* $ax \equiv b \pmod{m}$ is solvable (for x) iff $(a, m) \mid b$. The number of pairwise incongruent solutions is (a, m) (where (a, m) denotes the greatest common divisor of a and m).

(a) Prove the special case when a and m are coprime.

(b) Solve the congruence $8x \equiv 13 \pmod{11}$.

14. A *linear Diophantine equation* (in two variables) is $Ax + By = C$ where A, B, C are given integers, A and B are not both zero, and we are looking for integer solutions in x and y.

(a) Transform the equation into a linear congruence and derive the condition for solvability from the result stated in the previous exercise.

(b) Show that if solvable, the equation has infinitely many solutions.

(c) There are two types of dragons on an island, some have 7 heads, the others have 11 heads. Find the number of dragons if the total number of their heads is 118?

15. (a) For which values of n can you design n (not necessarily uniform) squares from which you can assemble a (bigger) square?

(b)* Investigate the similar question for cubes. (This problem is partly unsolved!)

***16.** I thought of 100 positive integers $x_1, \ldots, x_{100}$. You may ask any expression formed from these, using addition and subtraction (e.g. $6x_1 - 13x_2$). What is the minimal number of questions you need to guess all x_i-s? And if the questions may use also multiplication (i.e. you may ask e.g. $3x_1x_3 + 7x_5^6$)?

freud@caesar.elte.hu