Integers and prime numbers.

Basic notation. Let $\mathbb{N}$ denote the set of natural numbers $\{1, 2, 3, \ldots\}$ and let $\mathbb{Z}$ denote the set of all integers $\{\ldots, -2, -1, 0, 1, 2, \ldots\}$.

Definitions. For two integers a, b, it is said that a *divides* b, and denoted by $a|b$, if $b = ac$ for some integer c. Then a is a *divisor,* or *factor,* of b. A natural number $p > 1$ is *prime* if 1 and p are its only positive divisors. A natural number $n > 1$ that is not prime is said to be *composite.*

Theorem (Euclid). There are infinitely many prime numbers.

Further definitions. If a and b are integers that are not both zero, their *greatest common divisor,* denoted by (a, b) is the largest natural number that divides both a and b. If $(a, b) = 1$, then a and b are said to be *relatively prime.*

The *least common multiple* of a and b, denoted by $LCM(a, b)$, is the smallest natural number that is divisible by both a and b.

The notions of the greatest common divisor and the least common multiple generalize to finite collections of integers.

Euclidean algorithm. If $a > b$, $a, b \in \mathbb{N}$ and a/b yields the quotient q and remainder r:

$$\frac{a}{b} = q + \frac{r}{b}, \qquad 0 \leq r < b,$$

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

Corollary. Let a and b be integers, not both zero. Then

$$\{xa + yb : x, y \in \mathbb{Z}\}$$

is the set of all integral multiples of (a, b).

Euclid's lemma. If $a|bc$ and $(a, b) = 1$, then $a|c$.

Fundamental theorem of arithmetic. Every natural number exceeding 1 can be written uniquely, up to the order of factors, as the product of primes.

Legendre's theorem. The exponent $e_p(n!)$ of a prime p in the prime factorization of $n!$ is

$$e_p(n!) = \sum_{r \geq 1} \lfloor \frac{n}{p^r} \rfloor,$$

where $\lfloor x \rfloor$ denotes the biggest integer not exceeding x.

Euler's totient function theorem. For a natural number n,

$$\#\{k \in \mathbb{N} : k < n,\ (k, n) = 1\} =: \phi(n) = n \prod_{p \text{ prime},\ p|n} \left(1 - \frac{1}{p}\right).$$

Prime number theorem (Chebyshev, improved by Hadamard and de la Vallée Poussin). Let $\pi(x)$ denote the number of primes not exceeding x. Then there exist positive constants A and B such that

$$A\frac{x}{\ln x} < \pi(x) < B\frac{x}{\ln x}.$$

Examples.

1. Find all primes p such that $17p + 1$ is a perfect square.
2. For any two natural numbers a and b, prove that
$$(2^a - 1, 2^b - 1) = 2^{(a,b)} - 1.$$
3. Find a six-digit number that is increased by a factor of 6 if one exchanges (as a block) its first and last three digits.
4. Find the number of terminal zeros in the decimal expansion of 1000!.
5. Prove that $\binom{2n}{n}$ divides $LCM(1, 2, \ldots, 2n)$. Here, as usual,
$$\binom{n}{k} := \frac{n!}{k!(n-k)!}.$$
6. Prove that the product of any n consecutive integers is divisible by $n!$.
7. Prove that, for $n > 1$, the nth harmonic number
$$H_n := 1 + \frac{1}{2} + \frac{1}{3} + \cdots + \frac{1}{n}$$
is not an integer.