Composite Numbers, Prime Numbers, and 1

The **natural numbers** are the numbers $1, 2, 3, 4, 5, \ldots$, and so on. Among natural numbers, we distinguish three types of numbers:

1. **Composite numbers:** These are numbers that can be written as a product of two smaller numbers. For example, $6 = 2 \cdot 3$.
2. **Prime numbers:** Everything that isn't a composite, except 1, is a prime number. Thus a prime number cannot be written as a product of smaller numbers. For example, 5 is a prime number.
3. **Numbers that are 1:** There is only one such number. The number 1 is neither prime nor composite.

Starting with a composite number, we know (since it's composite) that we can break it down into smaller pieces, For example, if we take the number 520, we can break it down into the factors 52 and 10. Each of these decomposes further, for example $52 = 4 \cdot 13$ and $10 = 2 \cdot 5$. We can break down 6 a little more, into $6 = 2 \cdot 3$, and then rearrange everything that's left into increasing order:

$$520 = 52 \cdot 10 = 4 \cdot 13 \cdot 2 \cdot 5 = 2 \cdot 2 \cdot 13 \cdot 2 \cdot 5 = 2 \cdot 2 \cdot 2 \cdot 5 \cdot 13.$$

It's clear we can keep going until we can't go anymore. The numbers we are left with are numbers that can't be broken into smaller factors, and we call these prime numbers.

What if we start differently? We could start with $520 = 8 \cdot 65$, and keep going to get

$$520 = 8 \cdot 65 = 2 \cdot 4 \cdot 5 \cdot 13 = 2 \cdot 2 \cdot 2 \cdot 5 \cdot 13.$$

Of course, if we start with a prime number instead of a composite number, there's nothing left to do.

What is **not** clear is that given any number, this process of decomposition, no matter how it is performed, results in a unique answer. This fact deserves a special name:

The Fundamental Theorem of Arithmetic. Any natural number different from 1 can be uniquely represented as a product of primes in increasing order.

Some Divisibility Problems

If a and b are positive integers, then we say that b **divides** a and also that a **is divisible by** b if there is a number q such that $a = qb$. The number q is the **quotient** of a by b. To write "b divides a" with symbols, we write $b \mid a$. When b does not divide a, we write $b \nmid a$.

Examples. $4 \mid 12$, and $13 \mid 91$, but $12 \nmid 25$.

1. Which of the following numbers divides $2^9 \cdot 3$:
   (a) 2 (b) 5 (c) 8 (d) 9
   Why? (Or why not?)

2. Which of the following is true (and why!):

   (a) If a number is divisible by both 3 and 4, then it must be divisible by $3 \cdot 4 = 12$.

   (b) If a number is divisible by 4 and 6, then it must be divisible by $4 \cdot 6 = 24$.

3. (a) If a number N is not divisible by 3, is it possible that $2N$ is divisible by 3?

   (b) The number $15N$ is divisible by 6. Does N have to be divisible by 6?

4. Prove that the product of five consecutive natural numbers is:
   i. ... divisible by 30.
   ii. ... divisible by 120.

5. Check whether the number 24681357975318642 is divisible by:
   (a) 2 (b) 4 (c) 5 (d) 10 (e) 3 (f) 9 (g) 11 (h) 7

6. An agent at an incompetent intelligence agency was using a code where each number is assigned a distinct letter of the alphabet. The agent writes $AB \times CD = EEFF$. Prove that the agent is wrong.

Primes of the form $4k + 3$

We can split the odd primes into two distinct groups: those of the form $4k + 1$ (the first few being $5, 13, 17, 29, 37, \ldots$), and those of the form $4k + 3$ (the first few being $3, 7, 11, 19, 23, \ldots$). Since we know there are infinitely many primes (and only one even prime!), at least one of these two groups must be infinite. Using an argument similar to Euclid's proof for all primes, we can show that there are infinitely many primes of the form $4k + 3$. (In fact there are also infinitely many of the form $4k + 1$, but this is more difficult to show.)

1. Show that if you multiply together any two numbers of the form $4k + 1$ (for instance, $4m + 1$ and $4n + 1$), you get another number of that form.

2. Explain why any number of the form $4k + 3$ has a prime factor of the same form.

3. Now we want to show that there are infinitely many primes of the form $4k+3$. Like in Euclid's proof, we will start by assuming the *opposite*: namely, that there are only finitely many primes of this form–and from this try to reach some impossible conclusion, a contradiction.

   So assume there are only finitely many primes of the form $4k + 3$—call them $p_1, p_2, \ldots, p_r$. Then consider the number $N = 4p_1p_2 \cdots p_r + 3$. What can you say about this number? In particular, which if any of the p_i's is it divisible by?

4. Actually, the number N as defined above *is* divisible by one of the p_i's. Change the definition of N slightly so it's still of the form $4k + 3$, but is no longer divisible by any of the primes p_i of this form. Why is this a contradiction?