Primes

prime. A prime is a natural number that has exactly 2 natural divisors.

composite. A composite number is a natural number that has more than 2 natural divisors.

Note. 1 is neither prime nor composite. It is a **unit**.

Note. 0 is composite as it is divisible by 1, 2, and 3

Theorem: "The fundamental theorem of arithmetic" (existence part). Any integer $\geq$ 1 is the product of some n-tuple of primes.

Such a product is called a **prime decomposition** of a number.

For example. a prime decomposition of 300 is $\langle 2, 2, 3, 5, 5\rangle$ another is $\langle 2, 5, 2, 5, 3\rangle$

If we consider that the product of 0 numbers is 1 , then the theorem applies also to the number 1. A prime decomposition of 1 is the 0-tuple $\langle\rangle$.

We call a prime decomposition "sorted" if the primes are listed in nondescending order.

Theorem: "The fundamental theorem of arithmetic". Each integer ≥ 1 has a unique sorted prime decomposition.

Proof in the book.

Another way to think of a prime decomposition is a finite sequence of exponents for the primes 2, 3, 5, ...

- For example $300 = 2^2 \times 3^1 \times 5^2$ so it corresponds to the sequence $\langle 2, 1, 2 \rangle$
- If we require that the last number in the sequence not be 0, then the sequence is unique.

Question? Suppose that the prime decompositions of two numbers a and b are given by

$a = 2^{a_0} \times 3^{a_1} \times \cdots \times p_n^{a_n}$ and $b = 2^{b_0} \times 3^{b_1} \times \cdots \times p_n^{b_n}$

- How can we quickly find the prime decomposition of the product $a \cdot b$?
- How can we determine whether $b|a$?
- If $b|a$, how do we find the prime decomposition of the quotient of a divided by b?
- How can we determine the $\gcd(a, b)$?
- How many zeros are at the end of $100!$

Here is another proof by contradiction.

Theorem. There is an infinite number of primes.

- Suppose (falsely) that there are a finite number n of primes
- Let $\{p_0, p_1, ..., p_{n-1}\}$ be the set of all n primes
- Let $p = 1 + p_0 \cdot p_1 \cdot ... \cdot p_{n-1}$ be the product of all the primes plus 1.
- Note that p is at least 3, since 2 is a prime and no prime is 0.
- For any k ($0 \leq k < n$) consider dividing p by p_k. We have $p = 1 + qp_k$, where $q = p_0p_1...p_{k-1}p_{k+1}...p_{n-1}$. By the Euclidean Division Algorithm), the remainder 1 is unique; thus p is not divisible by p_k.
- Since p is not divisible by any p_k, its prime decomposition must be

  $$\langle\rangle$$

  and thus $p = 1$, but we know p is at least 3 . This is a contradiction.

□

The Sieve of Erastosthanes

How to find all primes less than N

- Consider a long list of numbers

$$2, 3, 4, 5, 6, 7, 8, 9, 10, 11, 12, 13, .., N - 1$$

- First number is 2. Cross off 2 and every second number

$$\cancel{2}, \cancel{3}, \cancel{4}, 5, \cancel{6}, 7, \cancel{8}, \cancel{9}, \cancel{10}, 11, \cancel{12}, 13, ...$$

- First non-crossed-off number is 3. Cross off 3 and every third number

$$\cancel{2}, \cancel{3}, \cancel{4}, 5, \cancel{6}, 7, \cancel{8}, \cancel{9}, \cancel{10}, 11, \cancel{12}, 13, ...$$

- First non-crossed-off number is 5.
- And so on until all numbers are crossed off.

```
bool b[N] ;
for( int i=2; i < N ; ++i ) b[i] = true ;
for( int i=2 ; i < N ; ++i ) {
        if( b[i] ) {
                cout << i << endl ;
                for( int j = i+i ; j < N ; j += i ) b[j] = false ; } }
```