A *prime number*, or a *prime*, is a positive integer with exactly two distinct positive divisors. The first few primes: $2, 3, 5, 7, 11, 13, 17, 19, ...$ The largest known prime: $2^{32582657} - 1$ (more than $9.8 \cdot 10^6$ digits, found by GIMPS, September 2006).

Theorem 1 (Fundamental Theorem of Arithmetic)**.** *For each integer $n > 1$ there are primes $p_1 \leq p_2 \leq \ldots \leq p_r$ such that $n = p_1 p_2 \ldots p_r$; this factorisation is unique.*

Proof. Existence – induction step: Assume that each m, $2 \leq m \leq n$, can be factored into primes. If $n+1$ is not a prime, then $n+1 = kl$ where $2 \leq k, l \leq n$. Apply induction hypothesis to k and l and conclude that $n+1$ has a prime factorisation.

Uniqueness – induction step: If $n+1 = p_1 p_2 \ldots p_s = p'_1 p'_2 \ldots p'_t$ where $p_1 \leq p_2 \leq \ldots \leq p_s$ and $p'_1 \leq p'_2 \leq \ldots \leq p'_t$, then (lecture 1) $p_1 = p'_i \geq p'_1$ and $p'_1 = p_j \geq p_1$ for some i, j and hence $p_1 = p'_1$. Apply induction hypothesis to $(n+1)/p_1$. □

Theorem 2. *There are infinitely many prime numbers.*

Proof #1 (Euclid). Let $p_1 < p_2 < \ldots < p_n$ be the list of the first n primes. No prime in the prime factorisation of $p_1 p_2 \ldots p_n + 1$ can be any of $p_1, p_2, \ldots, p_n$. □

Let $\pi(x)$ be the number of primes that are less than or equal to a real number x. The above proof shows that $\pi(x) \geq \log_2 \log_2 x$ and $p_n \leq 2^{2^{n-1}}$, but we will establish much better bounds.

Proof #2 (Ch. Goldbach). The statement is equivalent to existence of an infinite set of pairwise coprime numbers. Example: *Fermat numbers* $F_n = 2^{2^n} + 1$ for $n \geq 0$. The fact that $(F_n, F_m) = 1$ for $n \neq m$ follows from $F_0 F_1 \ldots F_n = F_{n+1} - 2$ or from $F_n | (F_m - 2)$ for $n < m$. □

Proof #3 (L. Euler). Let $M(x)$ be the set of all $m \in N$ such that all prime divisors of m are $\leq x$. For $n \leq x \leq n+1$ we have

$$\log x < \sum_{m \leq n} \frac{1}{m} \leq \sum_{m \in M(x)} \frac{1}{m} = \prod_{p \leq x} (\sum_{j \geq 0} \frac{1}{p^j}) = \prod_{p \leq x} \frac{p}{p-1} = \prod_{k \leq \pi(x)} \frac{p_k}{p_k - 1} \leq \prod_{k \leq \pi(x)} \frac{k+1}{k} = \pi(x) + 1.$$

□

Corollary 3. *For any $n \geq 1$ we have $p_n < e^{n+1}$.* □

Proof #4 (P. Erdös). Let $\{p_n;\ n \in N\}$ be the increasing sequence of all primes. Assume that the series $\sum_n \frac{1}{p_n}$ converges. Then, for some k, $\sum_{i>k} \frac{1}{p_i} < \frac{1}{2}$ and hence $\sum_{i>k} \frac{c}{p_i} < \frac{c}{2}$ for any natural c.

Call a prime p_i small (big) if $i \leq k$ ($i > k$). Let c_b (c_s) denote the number of $n \in N$, $n \leq c$, which are divisible by at least one big prime (by small primes only). Since $\lfloor \frac{c}{p_i} \rfloor$ is the number of $n \in N$, $n \leq c$, which are multiples of p_i, we have $c_b \leq \sum_{i>k} \lfloor \frac{c}{p_i} \rfloor \leq \sum_{i>k} \frac{c}{p_i} < \frac{c}{2}$, so that $c_b < c/2$ for *any* c. To estimate c_s, write any $n \leq c$ that has only small divisors as $n = a_n b_n^2$, where a_n is a product of *distinct* small primes. There are 2^k choices for a_n and since $b_n \leq \sqrt{c}$, we have $c_s \leq 2^k \sqrt{c}$. But if $c \geq 2^{2k+2}$, then $c_s \leq 2^k \sqrt{c} \leq c/2$ and $c = c_b + c_s < c/2 + c/2$, a contradiction. □

Aside: In 1919, Brun proved that the sum of reciprocals of *twin primes* converges.

Exercise 1. Do the above results extend to (a) numbers of the form $4n+1$, (b) complex numbers $s + ti$ where $s, t \in Z$, (c) numbers $s + t\sqrt{2}$ where $s, t \in Z$, (d) polynomials with integer coefficients?

GAP Commands:

`Primes;` lists all primes between 1 and 1000.

`NextPrimeInt(101);` returns the next prime number after 101. `PrevPrimeInt(101);` returns ...

`FactorsInt(24);` gives a list of all prime factors, repeated as appropriate. Also try `DivisorsInt(24);`