Theorem 11.6 (Euclid). *There are infinitely many primes.*

Proof Suppose that there are a finite number r of primes $p_1, p_2, \ldots, p_r$. Take

$$N = \left(\prod_{i=1}^{r} p_i\right) + 1.$$

Then $N > p_i \quad \forall i \in \{1, 2, \ldots, r\}$. Hence, by assumption, N is composite.

Considering the (unique) prime factorization of N gives that for some $j \in \{1, 2, \ldots, r\}$, $p_j \mid N$. Assume, by reordering the primes $p_1, p_2, \ldots, p_r$ if necessary, that $p_1 \mid N$. Then

$$p_1 \mid \left(\prod_{i=1}^{r} p_i\right) + 1.$$

Furthermore, $p_1 \mid \prod_{i=1}^{r} p_i$.

Hence $p_1 \mid 1$, a contradiction. □

Remark 11.7. Suppose that we denote by $\pi(x)$ the number of primes which are $< x$. Then $\pi(x) \sim \frac{x}{\log x}$ in the sense that

$$\lim_{x \to \infty} \frac{\pi(x)}{x/\log x} = 1.$$

Theorem 11.8. *There are arbitrarily large gaps in the sequences of primes.*

Proof Pick $n \in \mathbb{N}$. Consider the n successive integers

$$(n+1)! + 2,\ (n+1)! + 3,\ (n+1)! + 4,\ \ldots,\ (n+1)! + (n+1).$$

The first of these is divisible by 2, the second by 3, etc. In fact, the i^{th} one is divisible by $i + 1$. Hence none of the above n successive integers is prime. □

Definition 11.9. A *Fermat prime* is a prime of the form $2^r + 1$.

Remark 11.10. If $r > 0$ and $2^r + 1$ is a prime, then $r = 2^n$ for some $n \in \overline{\mathbb{N}}$.

For $n \in \mathbb{N}$, take $F_n = 2^{2^n} + 1$. Then

$$F_0 = 3, \quad F_1 = 5, \quad F_2 = 17, \quad F_3 = 257, \quad F_4 = 65537,$$
$$F_5 = 4294967297 = 641 \cdot 6700417 \text{ (countering a Fermat conjecture).}$$

Definition 11.11. A *Mersenne prime* is a prime of the form $2^r - 1$.

Remark 11.12. If $r > 1$ and $a^r - 1$ is a prime, then $a = 2$ and r is prime.

For primes p, take $M_p = 2^p - 1$. Then

$$M_2 = 3, \quad M_3 = 7, \quad M_5 = 31, \quad M_7 = 127, \quad M_{11} = 2047 = 23 \cdot 89.$$