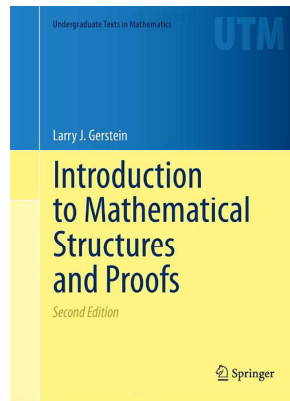


# Mathematical Reasoning

## Chapter 6. Number Theory

### 6.7. More on Prime Numbers—Proofs of Theorems



## Theorem 6.66

**Theorem 6.66.** If  $k \in \mathbb{N}$  and  $n = 2^k + 1$  is prime, then  $k$  is a power of 2.

**Proof.** Suppose  $n = 2^k + 1$  is prime. ASSUME there is a factorization of the exponent  $k = st$  with  $t$  odd and  $t > 1$ . Then  $n = 2^k + 1 = (2^s)^t + 1$ . But for an  $x$  we have (by induction on  $m$  where  $t = 2m + 1$ , or simply by distribution):

$$x^t + 1 = (x + 1)(x^{t-1} - x^{t-2} + \cdots - x + 1) = (x + 1) \left( \sum_{i=0}^{t-1} (-1)^i x^i \right).$$

But then with  $x = 2^s$ , we then see that  $(2^s + 1) \mid n$ , CONTRADICTING the fact that  $n$  is prime. So the assumption that the exponent  $k$  has an odd divisor  $t$  is false, so that  $k$  must be a power of 2, as claimed.  $\square$

## Lemma 6.67

**Lemma 6.67.** For each  $n \geq 1$ ,  $F_n - 2 = F_0 F_1 \cdots F_{n-1}$ .

**Proof.** We give a proof using the Principle of Mathematical Induction. For the basis case, we have  $F_1 - 2 = (5) - 2 = 3 = F_0$ . For the induction hypothesis, we assume the result holds for  $n = k \geq 1$ ; that is,  $F_k - 2 = F_0 F_1 \cdots F_{k-1}$ . Then

$$\begin{aligned} F_{k+1} - 2 &= (2^{2^{k+1}} + 1) - 2 = 2^{2^{k+1}} - 1 = (2^{2^k} + 1) \cdot (2^{2^k} - 1) \\ &= F_k \cdot (F_k - 2) = F_k \cdot (F_0 F_1 \cdots F_{k-1}) = F_0 F_1 \cdots F_k, \end{aligned}$$

so the claim holds for  $n = k + 1$  and the induction step holds. So by the Principle of Mathematical Induction, the claim holds for all  $n \geq 1$ .  $\square$

## Theorem 6.68

**Theorem 6.68.** The Fermat numbers are pairwise relatively prime.

**Proof.** ASSUME that prime number  $p$  divides both  $F_m$  and  $F_n$ , where  $m < n$ . The be Lemma 6.67 we know that  $p \mid (F_n - 2)$  (since  $F_m$  is a factor of  $F_n - 2$ ). But then  $p \mid (F_n - (F_n - 2))$ ; that is,  $p \mid 2$  so that  $p = 2$ . A CONTRADICTION to the fact that  $p$  divides both  $F_m$  and  $F_n$ , and all Fermat numbers are odd. So the assumption that  $F_m$  and  $F_n$  have a common prime divisor is false; that is, any two Fermat numbers are relatively prime, as claimed.  $\square$

## Theorem 6.71

**Theorem 6.71.** There are infinitely many prime numbers.

**Proof.** ASSUME there are finitely many primes, say  $p_1, p_2, \dots, p_k$ . For

$1 \leq i \leq k$  we have by Note 6.7.A(2),  $\sum_{n=0}^{\infty} \frac{1}{p_i^n} = \frac{1}{1 - 1/p_i} \in \mathbb{R}$ . The

product  $\prod_{i=1}^k \frac{1}{1 - 1/p_i}$  is then a real number. By Note 6.7.A(1)

$$\prod_{i=1}^k \frac{1}{1 - 1/p_i} = \prod_{i=1}^k \left( \sum_{n=0}^{\infty} \frac{1}{p_i^n} \right).$$

Now the  $k$  series on the right hand side converge absolutely and so can be rearranged by Note 6.7.A(4). So the right-hand side includes all elements of  $\mathbb{N}$  which are products of powers of the primes  $p_1, p_2, \dots, p_k$  (this is a weak point in our argument; Gerstein makes an argument for this claim when there are only two primes,  $p_1 = 2$  and  $p_2 = 3$ , in his Example 6.70).

## Theorem 6.71 (continued)

**Theorem 6.71.** There are infinitely many prime numbers.

**Proof (continued).** Denote these natural numbers as  $n_1, n_2, \dots$ . Notice that each such  $n_j$  appears only once by the Fundamental Theorem of

Arithmetic (Theorem 6.29). Hence  $\prod_{i=1}^k \frac{1}{1 - 1/p_i} = \sum_{n=0}^{\infty} \frac{1}{n}$ . Now the

left-hand side is some real number, but the right-hand side is a divergent series by Note 6.7.A(3), and this is a CONTRADICTION. So the assumption that there are finitely many primes is false, and hence there are infinitely many primes, as claimed.  $\square$